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

Pablo Andrés Díaz Alvear – Pablo Hidalgo Lascano
pabloandresepnd@yahoo.com
Escuela Politécnica Nacional
Facultad de Ingeniería Eléctrica y Electrónica
Campus Politécnico "Rubén Orellana" / Ladrón de Guevara E11-253, Quito - Ecuador

Resumen **- La Empresa Eléctrica Quito S.A. (E.E.Q.S.A.) se encuentra modernizando su red de datos, y dentro de este proceso se halla mejorando y manteniendo en constante evolución los sistemas de seguridad y protección de su red.**
Con este propósito y como una alternativa segura para acceder a la red privada de la E.E.Q.S.A. se diseña Redes Privadas Virtuales incluyendo el dimensionamiento de su equipamiento necesario, partiendo del análisis de la red de datos existente.
La implementación contempla la adquisición, instalación, configuración de equipos y pruebas de tráfico con los sistemas informáticos requeridos, con lo cual la VPN queda a disposición de los usuarios para la etapa final de producción.

I. Redes Privadas Virtuales Y Sus Aplicaciones

La evolución de las VPNs ha estado marcada por la necesidad de garantizar seguridad y confiabilidad en la información, esto en el pasado ha implicado costos que solo empresas con altos presupuestos podían contratarlos. Con el despliegue de redes públicas como *Frame Relay* y ATM mejoraba el panorama de las redes privadas, ya que estas tecnologías permiten a partir de un medio físico crear canales virtuales a través de la configuración soportada por el equipo concentrador de *Frame Relay* o ATM de cada extremo del enlace. Cada canal virtual podría considerarse como una VPN.

Al llegar el Internet y éste a su vez al ser abierto a la libre comercialización ha llegado a tener un gran despliegue hasta la actualidad, lo cual permite una comunicación a gran escala a precios relativamente bajos y al alcance de más usuarios. Esto ha permitido que sobre esta red se desarrollen e implementen varios protocolos de comunicación y servicios, entre los cuales se pueden mencionar los correspondientes a VPNs.

A. Conceptos y protocolos de VPNs

Las VPNs se conciben como redes virtuales que se forman sobre una infraestructura de red pública como el Internet; estas redes pueden presentar tres tipos de topologías, en la Fig. 1 se puede observar las topologías típicas de conexiones VPN.

Dentro de estas topologías, las VPNs deben cumplir con requerimientos de seguridad como Privacidad, Integridad,

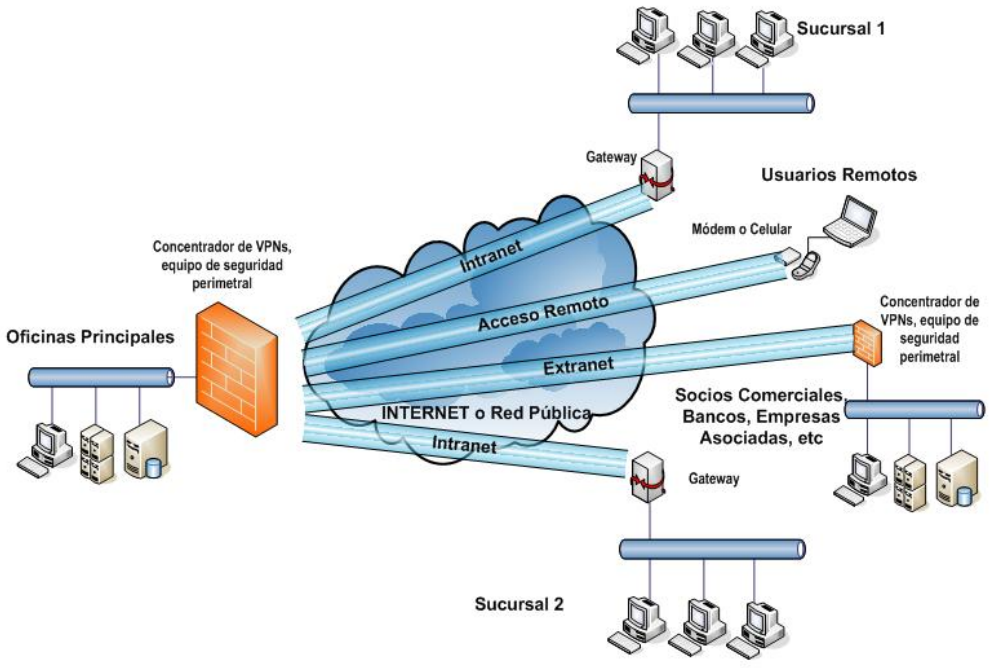

Fig. 1. Diferentes esquemas para la formación de VPNs [1]

autenticación, autorización y contabilidad; a la seguridad se le suma la calidad en la transmisión de la información, una fácil administración y por supuesto una interoperabilidad que permita a los equipos de diferentes fabricantes, que forman las VPN, manejar protocolos comunes y así garantizar la comunicación deseada.

Dentro de los protocolos que los equipos deben soportar, existe un grupo de tecnologías VPN que tienen mucho tiempo desde su desarrollo, las mismas que han sido adoptadas por la mayor parte de fabricantes de equipos de seguridad para redes de datos. IPSec, PPTP, SSL y L2TP son las tecnologías más comunes para la formación de VPNs. Cada una de ellas ha ido evolucionando para mejorar su funcionamiento.

B. Seguridad en las redes de datos

A través de la experiencia se ha podido determinar que los tipos de amenazas atacan las vulnerabilidades de las infraestructuras informáticas, siendo éstas tan comunes como mensajes y archivos infectados con virus informáticos, equipos de conectividad mal configurados, alteración en páginas y sitios web, sistemas operativos desactualizados, denegación de servicio, etc.; lo que ha permitido establecer mecanismos de seguridad tradicionales, como: *Firewalls*, Antivirus, Anti-Spams, control de contenido Web, etc.

Los sistemas de seguridad deben evolucionar ante los métodos de fraude a través de una red de datos y su entorno que lo compone. En la actualidad los sistemas tradicionales de seguridad no son los suficientemente efectivos cuando se trata de nuevos métodos de ataques informáticos. Los equipos que antes eran reactivos ahora deben ser proactivos, como proactivos deberán ser quienes administren las comunicaciones y seguridades informáticas de determinada entidad.

Dentro de la nueva tendencia en sistemas de seguridad, los fabricantes de equipos de conectividad y seguridad ofrecen al mercado soluciones que variarán dependiendo de la naturaleza de las infraestructuras que necesiten ser protegidas. Lo más común es encontrar infraestructuras de redes heterogéneas es decir que los equipos de conectividad son de diferentes fabricantes, lo cual implica un sistema de seguridad que se adapte a lo que está implementado. Por lo general el sistema de seguridad tradicional se ha compuesto de un *firewall*, un antivirus y un antispam y que esté implementado sobre servidores de propósito general.

En la actualidad se han desarrollado equipos de Gestión Unificada de Amenazas o UTM (*Unified Threat Management*). Este tipo de equipos de tipo *appliance* permite mitigar las amenazas íntegramente desde un solo equipo, a través de las funcionalidades de *firewall*, antivirus, IPS e IPSec-VPN, todos éstos ejecutados en tiempo real. Básicamente la ubicación de este tipo de equipos debe ser en las zonas perimetrales de las redes de datos.

Soluciones semejantes pueden ser también a través de *software* sobre plataformas Linux. Para redes que no exigen mucha carga de tráfico puede ser una solución adecuada, pero al tratarse de redes corporativas donde el número hosts en su red llega a alcanzar los 1000 equipos, los dispositivos dedicados o *appliances* son los más adecuados.

C. Aplicaciones Multimedia sobre VPN y el futuro de las VPNs

Un reto dentro de las transmisiones sobre enlaces VPN son las relacionadas con aplicaciones de voz y video. Para este tipo de aplicaciones se debe tomar en cuenta que los protocolos que ayudan a formar las VPNs agregan más información en las unidades de datos de protocolo (PDU); esto implica que se necesite más capacidad de canal que el habitual, además de esto si se utilizan métodos de encripción la latencia aumenta ya que los extremos finales realizan un procesamiento adicional correspondiente al cifrado.

A más de necesitar un incremento en la capacidad del canal, los enlaces VPN deben proveer calidad de servicio (QoS), garantizando de esta manera que las aplicaciones que no son tolerantes a retardos puedan ejecutarse de una manera confiable.

Para las aplicaciones de voz se tiene una amplia gama de códecs que pueden ser soportados por los equipos que generan las transmisiones de voz como Voz sobre IP, telefonía, radio en línea, etc. Dependiendo de la naturaleza y estado del enlace, se puede escoger un códec adecuado.

Las aplicaciones de video son más exigentes ya que están compuestas por audio y una gran cantidad de imágenes que podrían ser transmitidas en tiempo real, esto conlleva a un gran aumento en la capacidad del canal. Por lo general se recomienda que este tipo de aplicaciones se ejecute sobre redes de gran capacidad como canales de banda ancha o redes MPLS.

D. Futuro de las VPN

El futuro de las VPNs estará marcado por tecnologías como VPN SSL y MPLS. VPN SSL ha tenido un gran despliegue en el desarrollo de su tecnología, ya que los clientes que un inicio podían acceder a sitios seguros por medio de páginas web HTTPS y ejecutar aplicaciones sencillas de tipo web, debido a las exigencias de múltiples aplicaciones a corto plazo, requerían de un servicio cada vez más completo; es así que protocolos como TELNET y FTP se integraron a las páginas HTTPS como objetos embebidos. Actualmente VPN SSL soporta más protocolos como VNC, RDP, SSH y para quienes necesitan ejecutar todo tipo de aplicaciones, se ha desarrollado el túnel VPN SSL.

Las VPNs con MPLS tienen su campo de acción sobre redes donde se encuentra instalada una base de enlaces de fibra óptica o redes de alta velocidad. Estas redes por lo general pertenecen a los ISPs y empresas que entregan el servicio de transmisión de datos. MPLS permite que Ethernet despliegue todas sus características de tecnología de redes LAN hacia redes metropolitanas o MAN con el debido equipamiento. Esta evolución de MPLS se denomina VPLS y que también soporta direccionamiento IPv4 o IPv6 para formar VPNs seguras.

Como se ha indicado las redes han evolucionado en infraestructura física lo que ha permito que la información viaje en diferentes formas, ya sea escrita, en audio o de manera visual y con una amplia gama de calidad. Paralelamente a esta evolución, las redes y los sistemas han requerido seguridad, confiabilidad e integridad, estas características son propias de medios seguros como las VPNs

que sin duda son de gran ayuda para solucionar problemas de conectividad segura a bajos costos.

II. Análisis Del Estado Actual De La Red De Datos De La Empresa Eléctrica Quito S.A.

La E.E.Q.S.A. cuenta con un área de concesión muy amplia que abarca casi en su totalidad la provincia de Pichincha y algunos sectores de las provincias de Imbabura, Cotopaxi y Napo, lo que ha originado que las red de datos se extienda a través de diferentes medios de comunicación y en los cuales se diferencien el tipo de usuarios internos y externos.

A. Componentes de la red de datos

La red de datos de la E.E.Q.S.A. está compuesta por tres tipos de usuarios que son los Administradores o de la División de Tecnología de la Información y Comunicaciones (DTICs), usuarios locales y remotos; estos usuarios se diferencian por la localización y la naturaleza de sus necesidades informáticas.

Dentro los componentes de la red de datos de la E.E.Q.S.A. se tienen aplicaciones que se ejecutan y que sirven para la actividad normal del funcionamiento de la empresa. Las aplicaciones en su mayoría se ejecutan sobre servidores de virtualización CITRIX, otra gran parte a través de aplicaciones web y muy pocas en el modo cliente servidor.

La mayoría de computadores de escritorio y portátiles funcionan con el sistema operativo Microsoft Windows XP. Los principales servidores son de la marca IBM, y cuentan con sistemas operativos servidores como AIX, Windows Server 2003 y Red Hat Linux. El sistema de base de datos es ORACLE y principalmente sirve para los sistemas de Comercialización, Financiero, GIS, Sistema de Información de Distribución, y otros menores.

B. Enlaces y redes de datos

En cuanto a los enlaces de datos se puede mencionar que la E.E.Q.S.A. tienen que cubrir una amplia zona y lo hace mediante enlaces de cobre, fibra óptica y enlaces inalámbricos que son de su propiedad; además en aquellos lugares donde la infraestructura de red propia no ha llegado se tiene contratados enlaces dedicados con las empresas CNT y Telconet. Para los usuarios móviles la E.E.Q.S.A. cuenta con módems provisto por una operadora local de telefonía celular, la cual mediante un contrato de servicio ha dotado de Internet banda ancha, lo que ha permitido una comunicación de tipo móvil.

La E.E.Q.S.A. cuenta dentro de sus edificaciones con un sistema de cableado estructurado Categoría 5e; la comunicación entre las principales edificaciones es a través de fibra óptica a velocidades de hasta 1 Gbps con el centro de cómputo ubicado en el edificio matriz Las Casas.

Se cuenta con un servicio de Internet corporativo que es provisto por la empresa Telconet, a través de un enlace de última milla de 3.5 Mbps.

Los enlaces exteriores se consideran a aquellos que atraviesan redes públicas o si el medio no es muy confiable como los enlaces inalámbricos; para estos enlaces incluyendo el acceso al Internet, se realiza un análisis de la capacidad.

Los enlaces inalámbricos tienen la base instalada en el edificio Matriz Las Casas y a través de repetidoras ubicadas en sitios estratégicos como Cruz Loma, Pichincha, Miravalle y Collaloma que permiten que los sistemas informáticos lleguen a las agencias de recaudación, centrales de generación y subestaciones en los cuales no ha sido posible llegar con algún medio de comunicación guiado. Estos enlaces operan en las bandas no licenciadas de 2.4 Ghz y 5 Ghz con velocidades de entre 1 Mbps y 12 Mbps en condiciones técnicamente adecuadas.

Los enlaces contratados a la empresa CNT (antes ANDINATEL S.A.) tienen capacidades entre 128 kbps para agencias con un número de usuarios internos menor a 20 como Machachi y 512 kbps para agencias con un número de usuarios internos mayor a 20 como El Inca o Zona Sur.

Los enlaces contratados a la empresa TELCONET son de 1 Mbps en cada agencia sin distinción del número de usuarios. En muchas agencias de recaudación el enlace de TELCONET es el enlace principal y el de respaldo pasa a ser el enlace inalámbrico o de CNT.

Los enlaces son interconectados con *switches*, *routers*, *access points*, *gateways* de telefonía IP y otros dispositivos que se pueden integrar a la red Ethernet de la empresa.

El porcentaje de utilización de los canales antes señalados son relativamente bajos respecto a la capacidad de éstos. La Tabla 1 toma como referencia algunos sitios para la toma de datos que corresponden a la utilización de los diferentes enlaces incluido el acceso a Internet, el cual es el de mayor consumo respecto a la capacidad de su canal.

El equipo de *core*, por el cual pasa la mayor parte de tráfico de datos de la empresa y sirve como puerta de enlace hacia el Internet, es un *switch* multicapa que en su configuración tiene los accesos a las diferentes subredes, a través de enlaces punto a punto, VLANs y configuraciones de rutas estáticas y dinámicas.

La zona perimetral de la red tiene una seguridad instalada por medio de un *firewall* de tipo Software el cual se ejecuta sobre una plataforma AIX en un servidor IBM. Este *firewall* ha dejado de ofrecer una disponibilidad y seguridad adecuada que en la actualidad necesita la red de datos de la E.E.Q.S.A. Las razones por las que el *firewall* ha bajado su nivel de disponibilidad y seguridad y por las que también debe ser reemplazado, son las siguientes:

- *Manejo de Políticas*. Ambiente no muy amigable hace que el administrador sea propenso a fallas en el establecimiento de políticas.
- *Protocolos Antiguos*. Protocolos para formación de VPN no actualizados ocasionan incompatibilidad entre equipos.
- *Recursos de Hardware*. Disco duro y memoria son insuficientes ante el crecimiento de usuarios.
- *Lentitud en el acceso a sitios WEB.* Poca capacidad para los actuales niveles de crecimiento en el número de nuevas sesiones por segundo.

TABLA 1

CAPACIDAD Y UTILIZACIÓN DE LOS ENLACES EXTERIORES A LA E.E.Q.S.A. [1]

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%

– *Administración Compleja*. *Software* para la configuración y manejo del firewall muy complejo, pérdida de tiempo.
– *Sistema fuera de servicio*. El sistema ya presentaba deficiencias al tener una carga considerable de usuarios. Paralización frecuente de los procesos relacionados a las políticas de acceso y control, como consecuencia, usuarios fuera del acceso al Internet.

III. Diseño De La Red Privada Virtual

Para iniciar con el diseño de la VPN es necesario identificar claramente los usuarios y aplicaciones que necesitan acceder de manera remota a los servidores de base de datos y aplicaciones. Los CARs (Centros Autorizados de Recaudación), Operadores y revisores del servicio eléctrico, Administradores de Sistemas, funcionarios y ejecutivos, son los usuarios que potencialmente requieren un acceso a la red de la E.E.Q.S.A. desde un sitio externo a la empresa.

A. Aplicaciones requeridas

Las aplicaciones que los usuarios antes mencionados necesitan son los siguientes: SIDECOM, WEB-SDI y WEB-GIS, consolas de administración de los sistemas informáticos (HTTP, HTTPS, TELNET, SSH, SNMP y FTP).

Uno de los principales objetivos es dotar de acceso hacia el sistema comercial o SIDECOM a los CARs. Uno de los modos de acceso al SIDECOM es por medio del sistema de virtualización CITRIX. Para acceder a través del sistema CITRIX, es necesario que los clientes adquieran las licencias que tienen un costo. Las aplicaciones que se ejecutan por medio de CITRIX están implementadas sobre la red LAN de alta velocidad de la E.E.Q.S.A.

B. Metodología para determinar la capacidad del canal VPN IPSec requerido

Dentro del ambiente LAN se analiza la capacidad del canal de comunicaciones. Para esto se ha tomado un equipo que es parte de la red del edificio Matriz Las Casas, el mismo que tiene instalado y configurado un cliente CITRIX. Para analizar la capacidad ocupada durante la ejecución de la aplicación se ha puesto en escucha el analizador de protocolos WireShark (antes Ethereal), el cual permitirá observar la conversación (de datos) entre el cliente y el servidor.

El método para determinar la capacidad utilizada en el canal, es observar cuanta información atraviesa hasta la capa de red del modelo OSI utilizando el protocolo IP. Con este dato se podrá analizar la capacidad que necesitaría para transportar adecuadamente la información que sería la aplicación CITRIX y el encapsulamiento que realizaría IPSec en modo túnel con el protocolo ESP.

De la prueba realizada se han obtenido datos que arrojan los siguientes resultados resumidos en las Tablas 2 y 3, y que permiten considerar la capacidad necesaria para implementar la VPN para los CARs.

TABLA 2

RESUMEN DEL DIMENSIONAMIENTO PARA UN TÚNEL VPN CON IPSEC ESP [1]

Tasa de transferencia	Aplicaciones		
	VoIP (G.729)	GSM	Citrix
Capa 3 Protocolo IP (kbps)	24.00	28.40	10.00
Capa 2 Protocolo PPP (kbps)	27.20	31.60	11.59
IP + IPSec	45.60	48.80	21.32
IP + IPSec + PPP (kbps)	48.80	52.00	22.91
Porcentaje de Incremento de Capa3 a encapsulamiento IPSec (%)	90.00	71.83	113.20

El equipo de seguridad perimetral permitirá una protección robusta a través de nuevos sistemas de seguridad en conjunto con las herramientas tradicionales de seguridad como el firewall, Antivirus, Anti-SPAM, etc. Para esto se ha considerado establecer tres niveles de seguridad:

TABLA 3
CAPACIDAD DEL CANAL DE COMUNICACIONES PARA VPN IPSEC CON APLICACIONES SIMULTÁNEAS [1]

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

- *Primer nivel de seguridad*, que determina los equipos, puertos y servicios autorizados que son permitidos para el acceso externo.
- *Segundo nivel de seguridad*, al tener los sistemas que pueden ser accedidos desde el exterior se complementa la seguridad al poder inspeccionar si la información tiene software malintencionado como virus, troyanos o spam.
- *Tercer nivel de seguridad*, implica un servicio de proactividad en el cual las amenazas no identificadas pueden ser inspeccionadas por medio de un IPS (Sistema de Prevención de Intrusos) que tomará la decisión adecuada (según el administrador del equipo) para detener un posible ataque.

Estos niveles de seguridad no deben generar una alta degradación en la latencia del equipo, por lo que se hace necesario contar con un equipo que realice estas funciones en tiempo real y a una alta velocidad (velocidad de *hardware*).

C. Diseño de la zona perimetral

El equipo de seguridad perimetral físicamente debe cubrir los siguientes segmentos de red: Enlace Internet corporativo, DMZ, Red Interna corporativa y Extranet; la configuración es la que está actualmente operativa con el *firewall* antiguo.

En la parte de extranet se realizará un cambio, el diseño contempla que para el acceso de las diferentes empresas se lo haga independientemente a través de canales claramente diferenciados para definir los permisos y el tráfico permitido. Esta parte es posible realizarla a través de un *switch* de capa 2 que soporte IEEE 802.1q; el equipo de seguridad debe también soportar esta funcionalidad en el puerto requerido para que entre los equipos se pueda establecer un enlace de *trunk* o enlace troncal, donde se pueda transmitir varias VLANs. Cada VLAN pertenecerá a una empresa en particular donde dependiendo del requerimiento se le otorgará los permisos correspondientes (ver Fig. 2).

El direccionamiento IP que se implementará será con la red 172.16.20.0/24 para los enlaces de tipo Acceso Remoto. Para el modo de conexión LAN - LAN se podrá utilizar el mismo direccionamiento del sitio remoto o empresa externa, si hay una duplicación en la red interna de la E.E.Q.S.A. se utilizará NAT para evitar el problema. El equipo de seguridad y otros equipos y servidores que complementan el servicio de seguridad perimetral, tendrán direccionamiento de la red 132.147.160.0/22 que es la red IP principal interna. Para la administración del *switch* de la extranet se asignará a la VLAN de administración de ese segmento el direccionamiento de red 192.168.10.0/28.

D. Adquisición del equipo de seguridad perimetral

A través de empresas que ofrecen soluciones de seguridad perimetral y tomando en cuenta el estudio realizado para la E.E.Q. S.A. se ha podido realizar 4 presentaciones en las cuales se ha expuesto los productos: FORTINET FortiGate, CISCO ASA, ASTARO Security Gateway y Tipping Point.

Las tres primeras soluciones cubren en gran medida los

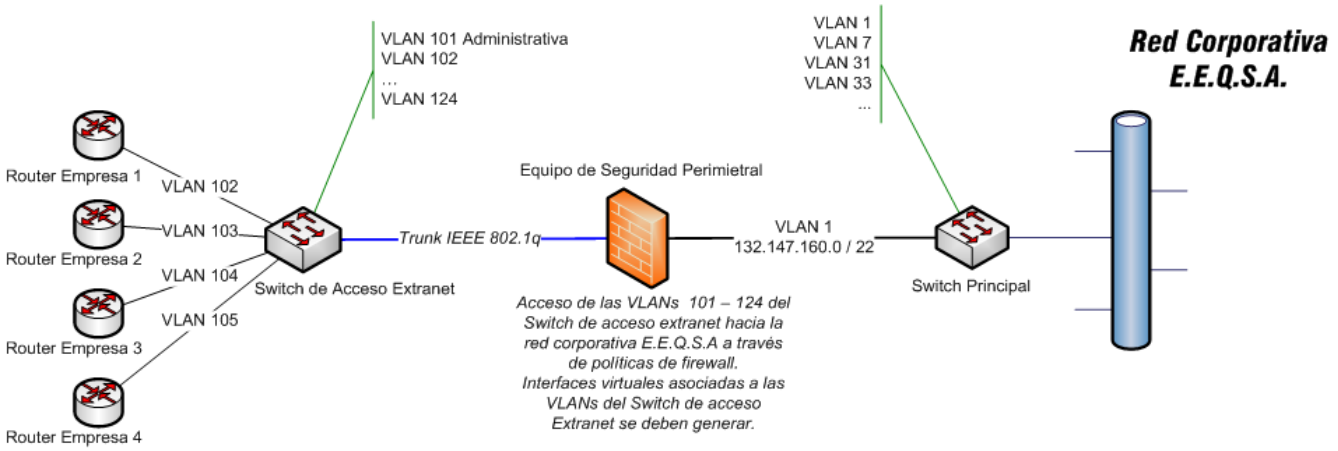

Fig. 2. Diseño de la zona perimetral de la red corporativa de la E.E.Q.S.A. [1]

requerimientos solicitados, la última presentación se trata de un equipo netamente IPS el cual no cubre la funcionalidad de *firewall*.

Al haber analizado estos productos y los requerimientos de la E.E.Q.S.A. se ha llegado a determinar un listado en el cual se exponen las necesidades en el ámbito de seguridad y también que la garantía del producto que se vaya a ofertar sea de alta calidad y un eficiente soporte.

Una vez realizadas las especificaciones técnicas se ha procedido a lanzar a concurso la adquisición del equipo seguridad perimetral, para el cual se han tenido tres ofertas de las cuales se ha escogido la que mejor se ajusta técnicamente a los requerimientos en base al diseño desarrollado y mejor oferta económica.

La oferta ganadora pertenece a la firma EVOLUTIONET que ha ofertado el equipo FortiGate FG300A del fabricante FORTINET el cual permitirá realizar las configuraciones necesarias e implementar los modernos mecanismos de seguridad así como la implantación de las VPNs, razón fundamental del este proyecto.

IV. Implementación De La Red Privada Virtual, Configuración De Equipos Y Pruebas Del Diseño Implementado

La implementación se inicia con la instalación del equipamiento en el centro de cómputo del edificio matriz. Los equipos a instalar son:

- Equipo de seguridad perimetral
- *Switch* administrable de capa 2
- Analizador de *logs*, eventos y generador de reportes del equipo de seguridad perimetral.

Una vez instalados y puestos en funcionamiento se procede a las configuraciones iniciales.

La configuración del *switch* es básicamente la asignación y funcionalidad de un puerto de *trunk* IEEE 802.1q y dependiendo de los requerimientos cada interfaz será parte de una VLAN. Según el diseño se iniciará la numeración de VLANs desde la 101 en adelante.

Para el equipo de seguridad perimetral, se inicia con la activación de un puerto que pertenezca o sea parte de la red local interna, el mismo que temporalmente estará en modo transparente para realizar un análisis previo de la carga de sesiones que existe en el *firewall* antiguo. Con este monitoreo se podrá saber qué día y en qué horario será conveniente la implementación definitiva del FortiGate 300A que en adelante se lo denominará como FG300A.

Según el diseño se designa las funcionalidades de cada una de las interfaces. Luego se configura los parámetros de red respectivos en cada interfaz. Toda esta configuración se la podrá hacer a través de consola de tipo línea de comandos, en la cual se habilitará el acceso desde puerto 3 (LAN INTERNA) de tipo HTTPS. Esta consola de tipo HTTPS permite una configuración de tipo gráfica y más amigable, sin embargo existen algunos comandos no tan comunes que no están en el modo gráfico, que de ser necesario se tendrá que ingresar vía consola RS-232 o SSH para la respectiva configuración por CLI (Línea de comandos).

El plan de configuración estará dado por la siguiente metodología: Configuración de redes y enrutamiento, Configuración de usuarios y grupo de usuarios y Configuración de seguridad.

- *Configuración de redes y enrutamiento*. Para iniciar es necesario que el FG300A conozca cuáles son las redes que van a ser interconectadas a través de sus interfaces. Se declara la red, la interfaz física de donde se puede alcanzar dicha red, una puerta de enlace y la distancia administrativa. Una vez que las redes son agregadas es posible que desde el FG300A se pueda realizar pruebas de conectividad para verificar la respuesta remota.
- *Configuración de usuarios y grupo de usuarios*. Los usuarios en el FG300A pueden ser de los siguientes tipos: Locales, LDAP, RADIUS y *Active Directory*. FG300A tiene control absoluto de los usuarios Locales; para los otros tipos de usuarios se debe especificar las referencias hacia los servidores de autenticación que tienen el control completo de las cuentas de usuarios. En el caso de usuarios de tipo RADIUS, se necesita configurar el acceso hacia un servidor RADIUS desde el FG300A especificando el nombre de *host* o dirección IP y una contraseña que es común entre el FG300A y el servidor RADIUS que en conjunto permitirán el acceso de los usuarios. El grupo de usuarios permitirá que aquellas cuentas que tengan requerimientos en común se los agrupen y puedan ser identificados al momento de aplicar determinada configuración de acceso. Por medio de estos grupos se podrá aplicar perfiles de usuario, al momento de aplicar políticas en la parte que corresponde al *firewall* del FG300A.
- *Configuración de seguridad*. Esta configuración implica otras como políticas del *firewall*, filtrado de contenido, operación del IPS, aplicación de perfiles de usuario, etc. La concentración de la mayoría de las configuraciones está en las políticas del *firewall* del FG300A. Básicamente aplicar políticas necesita la creación de objetos como: direcciones de red, grupo de direcciones, servicios, grupo de servicios y el debido enrutamiento de las redes. En el FG300A las políticas se las agrupa según la dirección que toma el tráfico entre un par de interfaces, por ejemplo al aplicar el acceso desde el Internet hacia el servidor web de la E.E.Q.S.A. (www.eeq.com.ec), la política estará dentro del grupo de políticas del puerto 1 (Acceso Internet) hacia puerto 2 (DMZ) (*port 1 → port 3*).

Las políticas necesitan cumplir con un orden en un listado de tipo vertical. El orden debe ser ascendente respecto a la generalidad de la política, es decir que, cuando una política tenga un ámbito más genérico que otra del mismo grupo, deberá ir más abajo. Cada vez que las políticas incrementen su restricción, la ubicación de determinada política se hace más compleja.

A. Implementación de Redes Privadas Virtuales, pruebas de tráfico y control de seguridad

La formación de VPNs será a través de IPSec, PPTP y SSL, todas serán utilizadas para la modalidad de acceso remoto a excepción de IPSec que será utilizada también para la modalidad LAN – LAN.

Para todas las opciones de conexión VPN se tendrá asignada la red IP 172.16.20.0/24 tal como se ha especificado en el diseño, además la asignación de la dirección para el cliente será de forma dinámica.

1) Configuración VPN PPTP:

Para el servidor de conexiones VPN PPTP la configuración se basa en habilitar el servicio y asignar un rango de direcciones así como un grupo de usuarios definido previamente en el FG300A.

La siguiente fase para habilitar este servicio es la configuración de la política que permite el paso de este tipo de tráfico. La política requerirá que se definan tanto las interfaces como las direcciones de origen y destino. En el formulario de la política también es importante indicar el tipo de servicio o protocolos permitidos, así como la acción asociada a la política. Parámetros opcionales como NAT, Perfil de protección, autenticación, y *Traffic Shaping* pueden ser definidos si es necesario; en el caso particular de esta política se definirá solo el *Traffic Shaping* o limitante de capacidad de canal en un valor de 128 KBytes/s. Por último se verifica la ubicación de la política en el listado.

2) Configuración VPN SSL:

En el formulario correspondiente a la configuración del servidor VPN SSL, se deben configurar los siguientes parámetros: activación del servicio, puerto de login, rango de direcciones para la opción de túnel VPN, clave de algoritmo de encripción y las direcciones de DNS y WINS.

Una segunda instancia que define este tipo de VPN es el grupo de usuarios ya que éstos son del tipo específico SSL VPN, y esto se debe a que este grupo tiene una configuración en particular que es vinculada a las opciones del portal web seguro donde se pueden habilitar accesos de tipo HTTP, TELNET, VNC, FTP, Samba y RDP.

La tercera instancia es referida a la política donde el parámetro *Action* es diferente al visto en VPN PPTP; aquí se especifica el valor de SSL-VPN, el cual genera otros campos en el formulario de la política y que indican básicamente el grupo de usuarios de tipo SSL VPN que serán asignados a la política. Al final del formulario de la política los parámetros no cambian, en el cual también se fijará el valor de 128 KBytes/s en el control de ancho de banda o *traffic shapping*, finalmente se verifica la ubicación de la política.

3) Configuración VPN IPSec:

Para habilitar este servicio se debe tomar en cuenta que con IPSec se permitirá las conexiones de tipo Acceso Remoto y LAN – LAN.

- *Conexión tipo Acceso Remoto*. Para el primer tipo de servicio se debe tomar en cuenta que los usuarios no son de tipo local, sino que la autenticación es a través de un servidor de autenticación RADIUS sobre una plataforma Linux CentOS 5.2. La asignación dinámica de las direcciones de clientes se la realizará por medio del servidor DHCP con el que cuenta el FG300A. La política es muy similar a la vista en VPN PPTP con la diferencia que la acción es de tipo IPSEC y este tipo de acción solicita que se especifique una conexión túnel previamente configurada en VPN IPSec.

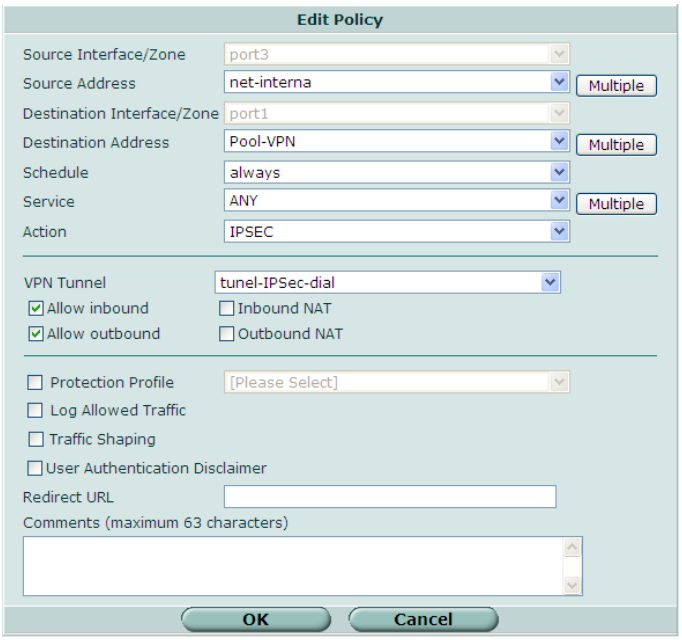

Fig. 3. Configuración de la política del *firewall* para VPN IPSec de Acceso Remoto E.E.Q.S.A. [1]

Para configurar el servidor VPN IPSec se debe definir si la generación de claves se lo hace automáticamente por medio de IKE o de forma manual. En este caso se lo realizará según IKE, donde se definen dos fases: autenticación y el establecimiento del túnel propiamente. En la fase 1 de autenticación se debe fijar los valores de identificación del túnel IPSec, el tipo de equipo remoto que para este caso debe ser *Dialup User*, la interfaz local, el modo de conexión, método de autenticación entre los equipos finales, como los más importantes.

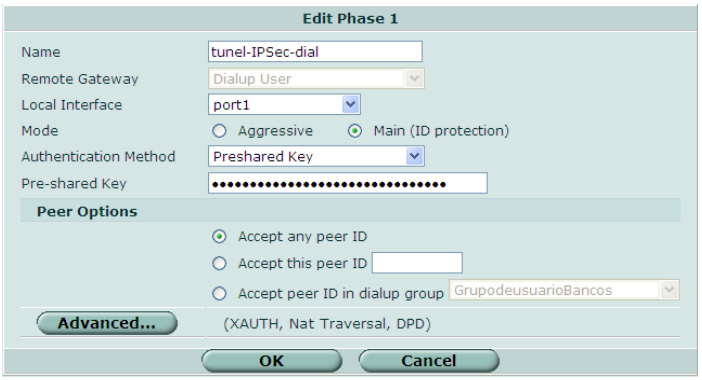

Fig. 4. Configuración IPSec para Acceso Remoto Fase 1 E.E.Q.S.A. [1]

Las opciones avanzadas permiten especificar valores como: el modo de interfaz, algoritmos de encripción y autenticación, el tiempo de vida de la llave o clave. Se puede especificar el tipo de autenticación extendida o XAuth la cual permite especificar un grupo de usuarios el cual será de tipo RADIUS. Como otras opciones se tiene *NAT-Traversal* para la detección de *firewalls* intermedios y la detección de pérdida de conexión del extremo o *Dead Peer Detection*.

La fase 2 de establecimiento del túnel es similar al formulario de la fase 1 y se diferencia en que, al tener establecida la autenticación solo se detallarán aspectos como los algoritmos de cifrado (confidencialidad de la información) y autenticación (para la integridad de la información), el tiempo de vida de las llaves de cifrado y tipo de autenticación. Aquí se define la conexión extremo – extremo, por lo que se debe especificar un servidor DHCP y las direcciones de origen y destino, las cuales corresponden a las direcciones LANs internas de los extremos de la VPN.

– *Conexión tipo LAN – LAN*. Según el diseño de este proyecto indica que para las extranets se necesita un *switch* da capa 2 que soporte IEEE 802.1q o VLANs y también que sea administrable. Los accesos de tipo IPSec LAN – LAN, serán categorizados como enlaces que pertenecen al grupo de extranets.

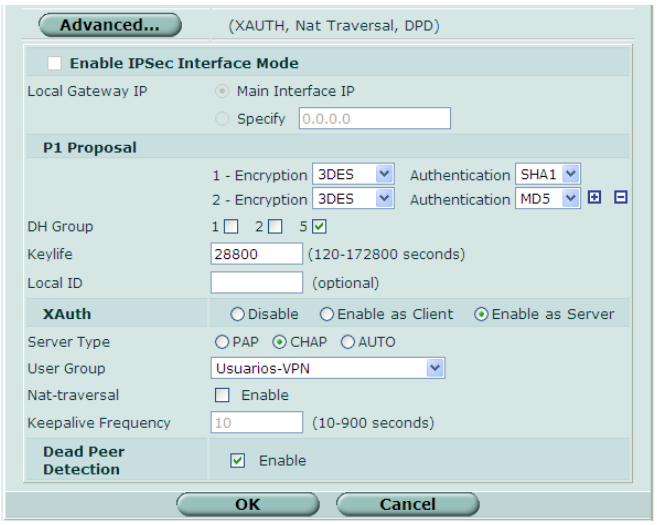

Fig. 5. Configuración IPSec para Acceso Remoto Fase 1 (Avanzado) [1]

El *switch* designado es un Cisco modelo Express 500 (CE500) de 24 puertos Ethernet a 10/100 Mbps y 2 puertos *gigabit-ethernet* de cobre a 10/100/1000 Mbps. Un puerto *gigabit-ethernet* es configurado como puerto de *trunk* IEEE 802.1q con el puerto 5 del FG300A, con lo cual la comunicación de las diferentes VLANs configuradas en el CE500 está garantizada. En el FG300A se configuran sobre la interfaz *port 5* las subinterfaces o interfaces virtuales asociadas a las VLANs configuradas en el CE500.

En la configuración del extremo del enlace IPSec no se realizan grandes cambios, como en el valor del parámetro *Remote Gateway* el cual se debe fijar en *Static IP address*, con lo cual se habilita el campo de *IP Address* y es donde se coloca la dirección remota de la interfaz local, que por ejemplo podría ser una dirección pública de Internet. Otro valor que debe ser cambiado es el *XAuth* el cual se lo deshabilita ya que se trata de conexiones con extremos fijos y confiables para los cuales no es práctico definir usuario y contraseña de tipo alguno. Un último cambio en la configuración avanzada, indica que se debe habilitar el modo de IPSec interfaz, con lo cual se crea automáticamente una nueva interfaz en la lista de interfaces locales del FG300A de tipo IPSec. La metodología en la fase 2 no cambia en relación a la configuración para el Acceso Remoto.

En el *firewall* se deben configurar dos tipos de políticas. Primeramente los asociados a las VLANs definidas en el CE500, las cuales permitirán en primera instancia el paso del tráfico de tipo público. Una vez configuradas las primeras políticas se puede seguir con las políticas asociadas a la interfaz virtual de tipo IPSec y la interfaz local de la red LAN del FG300A. Al tener interfaces virtuales de tipo IPSec las políticas asociadas a estas interfaces no requieren de que en la acción se fije el valor de IPSEC ya que serán tratadas como políticas comunes, a este tipo de configuración se le denomina LAN – LAN IPSec de modo ruteo.

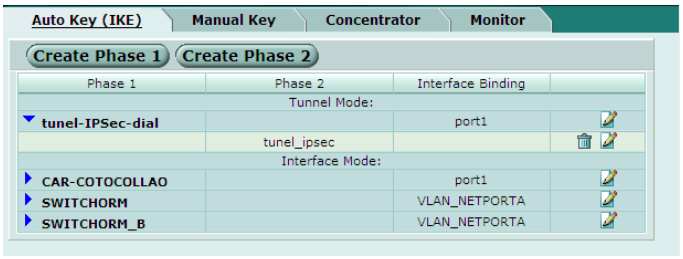

Fig. 6. Listado de túneles VPN IPSec configurados [1]

B. Servicio telefonía IP con SIP

Además del tráfico de datos, el tráfico de VoIP también puede ser transmitido por un canal VPN; es así que preliminarmente se ha configurado un sistema de telefonía IP con el propósito de realizar pruebas sobre el canal VPN ya sea éste PPTP, SSL o IPSec.

El objetivo consiste en montar un servidor de telefonía IP bajo el protocolo SIP y realizar llamadas de extremo a extremo sobre un canal virtual, en el cual se analizará el consumo de ancho de banda y la calidad de voz. El equipamiento consiste en un servidor en el cual se le instalará el servicio 3CX Phone System 7.0. El servidor está ubicado en la red LAN de la E.E.Q.S.A. el cual a través del canal virtual los clientes podrán acceder lo que les posibilita registrarse y realizar las llamadas con las extensiones internas del mismo sistema. El cliente cuenta con las opciones de configuración donde se puede especificar la dirección del servidor al cual debe registrase, el número de extensión y códec a utilizarse. En el presente caso la dirección del servidor es 132.147.163.55/22 las extensiones se han definido en el servidor y van desde la extensión con número 1000 hasta la 1010, tiene dos tipos de codec: PCM y

GSM; PCM genera sin encapsular 64 kbps a diferencia de los 28.4 kbps que genera GSM por lo tanto se utilizará GSM ya que los enlaces de datos a una red pública son menores a los de una red LAN.

C. Puesta a punto de equipos clientes finales y pruebas de tráfico y seguridades

Los equipos remotos finales pueden ser PCs de escritorio o portátiles en los que debe estar instalado el sistema operativo Windows XP SP2 para la conexión de tipo VPN con el FG300A. Para el caso de los enlaces LAN – LAN los equipos que forman la VPN en el extremo opuesto del FG300A deberán cumplir con el estándar IPSec actualizado.

1) Clientes PPTP y SSL:

En Windows XP SP2 se tiene el asistente de configuración para conexiones nuevas el cual soporta PPTP, en el cual se deberá especificar la dirección pública del FG300A.

El cliente SSL es básicamente un navegador web que soporte al menos 128 bits de cifrado como Internet Explorer 7 y Mozilla Firefox 3.0. Para ingresar al sitio seguro se debe dirigir a la dirección pública del FG300A a través de un URL de tipo HTTPS por el puerto 10443 (https://200.93.231.242:10443), el cual desplegará el formulario de ingreso usuario y contraseña autorizados a este servicio. El portal es una página muy intuitiva en la que se puede acceder a varios servicios de la red interna, sin embargo la herramienta más poderosa de este portal es un Control ActiveX, con el que cuenta el FG300A para una instalación automatizada de una interfaz virtual sobre el computador cliente y que hereda las configuraciones de red establecidas en el FG300A cuando se realizó la respectiva configuración del servidor VPN SSL. Esto permite la formación del túnel y por consiguiente el acceso a los recursos de la red interna.

2) Cliente IPSec Acceso Remoto:

Para el modo de acceso remoto IPSec, el fabricante del FG300A Fortinet ha desarrollado un cliente que permite crear una conexión VPN IPSec donde se configuran valores de conexión de red y sobre todo los algoritmos de cifrado y autenticación de las dos fases. Este cliente denominado FortiClient garantiza la conectividad y compatibilidad con el FG300A para canales IPSec.

D. Pruebas de tráfico y seguridades

Una vez iniciada la sesión se ha procedido a ingresar a un servidor de archivos el cual ha iniciado la descarga de archivos de considerable volumen (308 MB) a través de una conexión a Internet de banda ancha (3 Mbps). En la descarga se comprobó que la VPN utiliza toda la capacidad para el canal, sin embargo esto supone un gran riesgo para el acceso a Internet corporativo de la E.E.Q.S.A., por lo que se fija el valor de *traffic shapping* en la política del *firewall* respectiva a 128 kbps (14 KBytes/s).

Se inicializó una llamada utilizando el sistema de telefonía IP 3CX en el cual se mantuvo una conversación clara en la que se generó un ancho de banda de alrededor de 90 kbps, lo que indica que sobre un canal de 128 kbps es posible mantener una conversación clara con SIP y el codec GSM, y a su vez tener activa una sesión del sistema de comercialización SIDECOM sobre un cliente CITRIX.

Además de estas pruebas fueron también posibles las pruebas de seguridad en las que básicamente se referían al control de acceso por medio de un servidor RADIUS, en el cual se recolecta la actividad de acceso de determinado usuario. Otras pruebas de seguridad se refieren a la funcionalidad de control de contenido al navegar por sitios web bloqueados en el FG300A. Otra función implementada es el IPS, donde se ha bloqueado el flujo de tráfico de video bajo demanda y descarga de archivos multimedia como mp3, mp4,

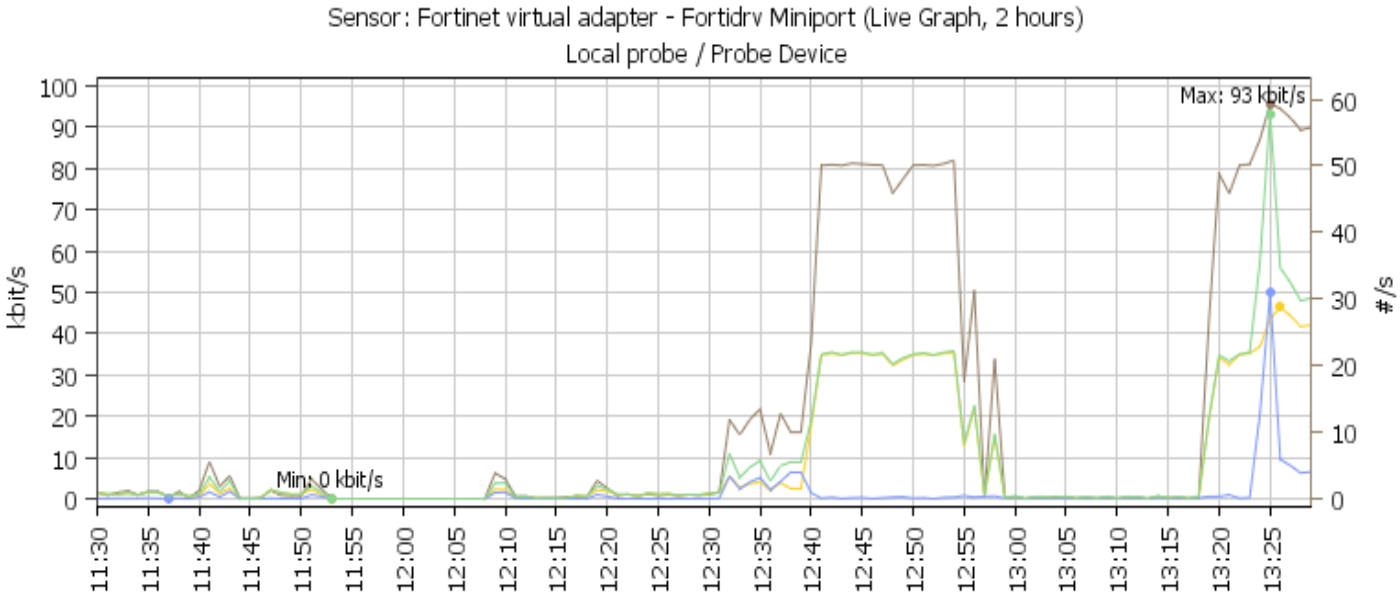

Fig. 7. Ocupación del canal generado por la llamada de tipo SIP sobre el canal VPN [1]

avi, etc. de sitios web que no tienen restricciones en la política del *firewall*, con lo cual se mejora, tanto la utilización del acceso a Internet como la seguridad al usuario final.

V. CONCLUSIONES

Las políticas de modernización han llevado a mejorar el equipamiento de seguridad perimetral de la red corporativa de la E.E.Q.S.A., en la que se ha añadido un nuevo servicio que es la VPN, lo que abrirá sin duda otras opciones de conectividad para el acceso a los servicios de la LAN Interna.

Los CARs podrán acceder a la recaudación en línea, aunque el *software* de aplicación aun no está definido formalmente, la VPN provee una versatilidad en el transporte de datos sobre varios protocolos; así que si no se lo realiza por CITRIX, este proceso se lo podrá realizar a través de otros protocolos que podrán ser de menor consumo de ancho de banda como el acceso directo a la base de datos por medio del puerto 1521 de ORACLE el cual es muy liviano.

EL UTM Fortigate 300A permite a más de la funcionalidad de *firewall* convencional, la posibilidad de controlar amenazas por medio de su IPS incorporado, el filtrado de contenido, antivirus y antispam que mejoran la seguridad perimetral de la red corporativa, sin embargo esta seguridad será complementada principalmente con políticas de seguridad que impliquen una colaboración responsable entre quienes administran los sistemas informáticos y sus respectivos usuarios.

Se espera mejorar la zona perimetral a través de un sistema de redundancia en línea y un acceso a Internet con otro proveedor para así tener un sistema altamente confiable.

FG300A es un equipo robusto el cual para su efectivo funcionamiento requerirá de las respectivas actualizaciones del *firmware* así como de las definiciones del antivirus e IPS, con lo cual se podrá prolongar la vida útil del equipo de seguridad.

VI. BIBLIOGRAFÍA

[1] Díaz, P., *"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 de Titulación, Escuela Politécnica Nacional, Quito, Ecuador. Feb. 2010.

[2] M. Mampaey. O. Paridaens. (2005). Alcatel Vision for Secured Next Generation Networks. Alcatel – Lucent. [Online]. Disponible: 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

[3] J. Witters, J. De Clercq, S. Khandekar. (4to. Trimestre 2004). TUTORIAL TÉCNICO DEL VPLS: Introducción técnica a los servicios Ethernet multipunto sobre MPLS. [Online]. Disponible: http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/pdf/ATR2004Q4/T0411-VPLS-ES.pdf

[4] Y. El Mghazli, J. De Clercq. (4to. Trimestre 2004) VPNS BGP/MPLS: TUTORIAL Y CONSIDERACIONES DE ESCALAMIENTO. Revista de Telecomunicaciones de Alcatel. Alcatel – Lucent. [Online]. Disponible: http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/pdf /ATR2004Q4/ T0411-MPLS-VPN-ES.pdf

[5] *FortiGate IPSec VPN User Guide*, Fortinet Version 3.0, 01-30005-0065-20081015, Oct. 2008. [Online]. Disponible: http://docs.fortinet.com/fgt/archives/3.0/techdocs/FortiGate_IPSec_VPN_User_Guide_01-30005-0065-20081015.pdf

[6] *FortiGate v3.0 MR7 SSL VPN User Guide*, Fortinet Version 3.0, 01-30007-0348-20080718, Jul. 2008. [Online]. Disponible: http://docs.fortinet.com/fgt/archives/3.0/techdocs/FortiGate_SSL_VPN_User_Guide_01-30007-0348-20080718.pdf

VII. BIOGRAFÍA

Pablo Andrés Díaz Alvear, nacido en Pichincha - Ecuador el 4 de mayo de 1979 estudió la primaria en la Unidad Educativa Darío Figueroa Larco, realiza sus estudios secundarios en el colegio Nacional Juan de Salinas de la ciudad de Sangolquí. Los estudios superiores los desarrolla y culmina en la Escuela Politécnica Nacional en la facultad de Ingeniería Eléctrica y Electrónica en la Carrera de Ingeniería en Electrónica y Redes de Información. Incursiona laboralmente en empresas que se dedican al negocio de las telecomunicaciones y redes de datos y desde el año 2005 hasta la actualidad es parte del personal técnico del área de Comunicaciones y Redes de la Empresa Eléctrica Quito S.A.

Pablo Hidalgo Lascano. Nació en Ambato en 1959. Obtuvo el título de Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional (1985) siendo declarado el mejor graduado de su promoción. Becado por el Gobierno Alemán y auspiciado por la E.P.N. realizó estudio de postgrado en Telecomunicaciones en el Deutsche Bundespost (1988 - 1990) y en la Maestría de Conectividad y Redes de Telecomunicaciones en la E.P.N. (2000 - 2002) Actualmente se desempeña como profesor principal del Departamento de Electrónica, Telecomunicaciones y Redes de Información de la E.P.N. Fue promotor y Coordinador de la Carrera de Ingeniería en Electrónica y Redes de Información de la E.P.N. (2000 – 2007). Ha dirigido más de 60 tesis de grado y proyectos de titulación. Se ha desempeñado como consultor y asesor para algunas entidades públicas y privadas. Sus áreas de interés actuales son: Redes de Información, Comunicaciones Inalámbricas y Transmisión de Datos. Es miembro de la Association for Computing Machinery (ACM) y el Institute of Electrical and Electronics Engineers (IEEE).