ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO DE INGENIERÍA

"DISEÑO E IMPLEMENTACIÓN DEL SISTEMA INTEGRADO DE COMUNICACIONES PARA LA RED CORPORATIVA INTERTRADING ARDILA."

MARCO FERNANDO MORENO BRITO

SANGOLQUÍ – ECUADOR

2008

CERTIFICACIÓN

Certificamos que el siguiente proyecto de grado, “Diseño e Implementación del sistema integrado de comunicaciones para la red corporativa Intertrading Ardila.”, fue desarrollado en su totalidad por el señor Marco Fernando Moreno Brito, bajo nuestra dirección.

Atentamente,

_____	_____
Ing. Carlos Romero	Ing. Fabian Saenz
DIRECTOR	CODIRECTOR

RESUMEN

El presente proyecto es para satisfacer la necesidad de la corporación Intertrading Ardila, la cual al ser una empresa que posee 2 sucursales, una en Bogota – Colombia y la otra en Quito – Ecuador, se ven en la obligación de encontrar la forma de abaratar costos en las llamadas internacionales y en compartir archivos. Para lo cual pensaron en la solución de voz sobre ip y formación de VPN entre los sitios para el efecto, ya que en ambos sitios poseen Internet y porque no explotar este recurso al máximo. Como adicional, el gerente requirió que desde su casa también pueda tener acceso a las computadoras de las oficinas de Quito.

Para la realización del proyecto se estudio las redes con las que venían trabajando, para poder aprovechar de estas, los recursos que se requiera, como el ancho de banda de Internet y equipos con los que ya estén trabajando. Se hizo un análisis de que equipos, (Routers y Gateways de VoIP) que convendría colocarlos en la red, así como, el análisis de costos correspondientes, para comprobar que la inversión se justifica.

Con los equipos escogidos, se crearon las reglas correspondientes para vpn, firewall, dnat y administración de ancho de banda, este último pensando en que se necesita una calidad de servicio para la comunicación, por ello tengan canales dedicados para VoIP, para VPN y para Internet.

Finalmente, se procedió a la instalación de los equipos y las pruebas correspondientes para comprobar que todas las configuraciones requeridas estén funcionando, así como la comunicación sea entendible, sin retardo y comparable con la comunicación por líneas convencionales.

DEDICATORIA

Dedico este trabajo, principalmente a mis padres, forjadores y orientadores para culminar mi carrera, por sus palabras y consejos que día a día me supieron dar. A mis hermanos, primos, abuelitos y tíos que supieron aportar con su granito de arena. Y a mi novia que sin su amor, hubiese dejado de soñar.

AGRADECIMIENTO

Agradezco a Dios por cada día de vida, por la fe, constancia y la dicha que me da, por haber culminado un peldaño más de la vida. A mis padres que sin su apoyo nada de esto fuese posible, gracias a su esfuerzo a su ejemplo de vida estoy terminando mi carrera universitaria. A mis hermanos, tías, primos, y familiares, por sus palabras de aliento cuando me hicieron falta. A mis profesores que con su guía y orientación puedo ser un excelente profesional. Y a mis amigos y compañeros que dieron su aporte para terminar esta etapa mas de la vida.

PROLOGO

Las llamadas Internacionales tiene un costo muy elevado, y la tecnología a avanzado para poder transportar Voz y Datos a través de Internet, es por esto que la empresa vio la necesidad de aminorar sus costos en llamadas internacionales pudiendo hacer una inversión inicial y recuperando este gasto en pocos meses.

De igual manera el manejo de redes privadas virtuales a través de Internet les permite que la información de la empresa pueda estar compartida y obtener archivos, información de manera mas fácil entre Bogota y Quito, a su vez, le da un valor agregado al poder ver los equipos de los empleados con herramientas como escritorio remoto originario de Windows o Remote Admin.

Es por esto, que en primer capitulo se explica cuales son los requerimientos y necesidades de la empresa, como esta confirmada la empresa, y las herramientas que ya poseen y que sirvan para la realización del proyecto.

En el segundo capitulo, se analiza la teoría que corresponde a la Voz sobre Ip y a la formación de VPN. Los protocolos, los algoritmos de encriptación, las codificaciones que puedan existir, para ver las seguridades que se puedan dar a la VPN, y a la compresión de la voz que podemos implementar. Añadiendo un poco de la legalidad de implementar este proyecto en el Ecuador.

En el tercer capitulo, se toma todas las necesidades de la empresa y todos los equipos que nos puedan servir para el diseño, tomando en cuanta los requerimientos de seguridad, de firewall de nat y manejo de ancho de banda, realizando una comparación entre distintas marcas que existen en el mercado para escoger el que cumpla con los requerimientos y su costo sea accesible para la empresa.

En el cuarto capitulo se realiza un análisis de costos, viendo el costo de inversión, los gatos corrientes, y los beneficios, que para este caso es el ahorro en llamadas internacionales. Para con estos datos hacer un flujo de caja, y de esta manera obtener valores del TIR y el VAN que son herramientas de costos que nos ayudan a comprobar que tan buena es una inversión poniéndole a un tiempo de plazo para compensar el gasto inicial.

En el capitulo cinco, se explica paso a paso la implementación del proyecto, con la configuración de cada unos de los equipos que se van a instalar en los diferentes sitios. Basados en el diseño que se realizo en el capitulo tres, indicando características adicionales que los equipos poseen y pueden servir en este proyecto. Aquí también se realiza las pruebas correspondientes para verificación de que las configuraciones y reglas implementadas se cumplan, así como, la comunicación de voz sobre ip tenga una buena aceptación con calidad de servicio.

Finalmente en el capitulo seis se presentan las conclusiones y recomendaciones que se han obtenido con la presente implementación.

ÍNDICE DE CONTENIDO

CAPITULO I

1. INTRODUCCIÓN **1**

1.1 Introducción 1

1.2 Situación actual de la red 3

CAPITULO II

2. COMUNICACIÓN VOIP Y VPN **7**

2.1 Tecnología 7

2.2 Definición de VoIP 9

2.3 Protocolos H323 y SIP 10

2.3.1 Protocolo H323 10

2.3.2 Protocolo SIP 11

2.3.3 SIP vs. H323 12

2.4 Protocolos de VPN 18

2.4.1 Definición de VPN 18

2.4.2 Necesidades y surgimiento de las VPNs 19

2.4.3 Estructura de las VPNs 20

2.4.4 Protocolos utilizados en las VPNs 23

2.5 Aspectos de Regulación de VoIP 30

CAPITULO III

3. DISEÑO DE LA NUEVA RED **32**

3.1 Diseño 32

3.2 Estructura física 34

3.2.1 Características del Router 34

3.2.2 Características del equipo de VoIP 34

3.2.3 Características del Switch 35

3.2.4 Características de las Cámaras 35

3.2.5 Comparación de Routers existentes en el mercado 35
3.2.6 Cuadro comparativo para mejor selección de router 39
3.2.7 Equipos de Voz sobre IP del mercado 40
3.2.8 Cuadro comparativos de equipos de VoIP para seleccionar el adecuado 44
3.3 Diseño Lógico 44
3.3.1 Diseño para la Red 1 45
3.3.2 Diseño para la Red 2 46
3.3.3 Diseño para la Red 3 46
3.4 Configuración para los equipos y protocolos a emplearse 48
3.4.1 Las reglas para oficinas de Ardila en QUITO 48
3.4.2 Las reglas para la oficina de Ardila en BOGOTA 51
3.4.3 Las reglas para la casa de Sr. Ardila en BOGOTA 52

CAPITULO IV

4. ANÁLISIS ECONÓMICO 54

4.1 Costos de equipos e instalación 54
4.1.1 Costo de equipos e instalación 54
4.1.2 Gastos corrientes 55
4.1.3 Beneficios 55
4.2 Flujo de caja y obtención de costos de la inversión 56

CAPITULO V

5. IMPLEMENTACIÓN DEL PROYECTO 58

5.1 Configuración de routers 58
5.1.1 Configuración Zywall 2 Plus Oficina Quito 60
5.1.2 Configuración Zywall 2 Plus Oficina Bogotá: 74
5.1.3 Configuración Zywall 2 Casa Bogotá: 83
5.2 Configuración de equipos de voz sobre IP 87
5.2.1 Plan de marcación 88
5.2.2 Configuración de Gateway de voz Quito: 89
5.2.3 Configuración de Gateway de voz Bogotá: 93

5.3 Pruebas de acceso a cámaras, a routers y formación de VPN 96
5.4 Pruebas de comunicación de voz 97

CAPITULO VI
6. CONCLUSIONES Y RECOMENDACIONES 99
6.1 Conclusiones 99
6.2 Recomendaciones 100

ANEXOS
Anexo 1. Regulación en el Ecuador para VoIP 102
Anexo 2. Análisis de Costos 109
Anexo 3. Prueba de funcionamiento de Firewall, Nat y VPN 113
Anexo 4. Encueste de calidad de servicio de la comunicación VoIP 121

BIBLIOGRAFÍA 122

ÍNDICE DE TABLAS

CAPITULO I INTRODUCCIÓN

CAPITULO II COMUNICACIÓN VOIP Y VPN

Tabla 2.1. Disponibilidad de servicios en SIP y H323 16

CAPITULO III DISEÑO DE LA NUEVA RED

Tabla 3.1 Comparación entre routers 39

Tabla 3.2 Comparación entre gateways de VoIP 44

CAPITULO IV ANÁLISIS DE COSTOS

Tabla 4.1 Costo de equipos e instalación 54

Tabla 4.2 Gastos Corrientes 55

Tabla 4.3 Beneficios Económicos 56

CAPITULO V IMPLEMENTACIÓN DE PROYECTO

CAPITULO VI CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE FIGURAS

CAPITULO I INTRODUCCIÓN

Figura 1.1 Esquema red actual 6

CAPITULO II COMUNICACIÓN VOIP Y VPN

Figura 2.1. Componente de un sistema H323 11
Figura 2.2 Red VPN 20
Figura 2.3 Capas de encapsulamiento PPTP 24
Figura 2.4 Paquete AH en modo túnel 27
Figura 2.5 Paquete AH en modo transporte 27
Figura 2.6 Combinación AH y ESP 27
Figura 2.7 Paquete de entunelamiento 27
Figura 2.8 Escenario L2TP 28
Figura 2.9 Relación entre PPP y L2TP 29

CAPITULO III DISEÑO DE LA NUEVA RED

Figura 3.1 Esquema de nueva red 33
Figura 3.2 Router Netgear 35
Figura 3.3 Router Cisco 1711R 36
Figura 3.4 Router Zywall 2 38
Figura 3.5 Gateway Linksys 40
Figura 3.6 Gateway de VoIP Multitech 41
Figura 3.7 Gateway de VoIP Microñes 42
Figura 3.8 Diseño de nueva red 47

CAPITULO IV ANÁLISIS DE COSTOS

CAPITULO V IMPLEMENTACIÓN DE PROYECTO

Figura 5.1 Esquema de Red a implementarse 59
Figura 5.2 Pantalla principal zywall 2 uio 60
Figura 5.3 Interfase LAN zywall uio 61
Figura 5.4 Interfaz IP Alias zywall uio 61
Figura 5.5 Interfase WAN zywall uio 62
Figura 5.6 Pantalla de configuración DNS del zywall 63
Figura 5.7 Interfaz de Firewall de zywall 2 uio 63
Figura 5.8 Reglas de port forwarding 64
Figura 5.9 Reglas de firewall para cámaras 65
Figura 5.10 Reglas de acceso remoto al zywall uio 65
Figura 5.11 Reglas de Firewall para acceso remoto al zywall uio 66
Figura 5.12 Regla general de administración de ancho de banda 67
Figura 5.13 Configuración de servicios de BW Lan 68
Figura 5.14 Configuración de servicios de BW Wan 68
Figura 5.15 Formación de 2 VPN 69
Figura 5.16 Regla General VPN oficinas UIO – BGT 70
Figura 5.17 Regla especifica VPN oficinas UIO – BGT 71
Figura 5.18 Regla general VPN UIO – casa Ardila 72
Figura 5.19 Regla especifica VPN UIO – casa Ardila 73
Figura 5.20 Pagina home de zywall BGT 74
Figura 5.21 Interfase Lan Zywall BGT 75
Figura 5.22 DCHP estático zywall BGT 75
Figura 5.23 Interfase Wan Zywall BGT 76
Figura 5.24 Reglas de DNAT Zywall BGT 77
Figura 5.25 Reglas de firewall para la cámara y equipo VoIP 77
Figura 5.26 Administración remota zywall BGT 78
Figura 5.27 Regla de firewall para administración remota zywall BGT 78
Figura 5.28 Administración de BW Lan 79
Figura 5.29 Administración de BW Wan 80
Figura 5.30 Vpn entre oficina BGT y UIO 80

Figura 5.31 Regla general VPN de oficina BGT y UIO 81
Figura 5.32 Regla especifica de VPN BGT a UIO 82
Figura 5.33 Estado de zywall casa Ardila 83
Figura 5.34 Interfaz LAN zywall casa Ardila 84
Figura 5.35 Interfaz WAN zywall casa Ardila 84
Figura 5.36 Administración remota de zywall casa Ardila 85
Figura 5.37 Regla de VPN en zywall casa Ardila 85
Figura 5.38 Regla de formación de VPN casa Ardila 86
Figura 5.39 Reglas de encriptación para VPN casa Ardila 87
Figura 5.40 Plan de marcación VoIP 88
Figura 5.41 Ip de gateway de voz UIO 89
Figura 5.42 Configuración de parámetros equipo VoIP UIO 90
Figura 5.43 Configuración de autollamada equipo de VoIP UIO 91
Figura 5.44 Parámetros de Interfase MVP130 UIO 91
Figura 5.45 Outbound phonebook MVP130 UIO 92
Figura 5.46 Indbound phonebook MVP130 UIO 92
Figura 5.47 IP de equipo VoIP BGT 93
Figura 5.48 Parámetros de la voz MVP130 BGT 94
Figura 5.49 Parámetros de la interfase MVP130 BGT 95
Figura 5.50 Outbound MVP130 BGT 95
Figura 5.51 Indbound MVP130 BGT 96
Figura 5.52 Formación de llamada desde UIO a BGT 97

CAPITULO VI CONCLUSIONES Y RECOMENDACIONES

GLOSARIO

VoIP : Voz sobre IP

IP : Internet Protocol

PSTN: Public Switch Telephony Network

VPN : Virtual Private Network

LAN : Local Area Network

WAN : Wide Area Network

RDSI: Red Digital de Servicios Integrados (RDSI o ISDN en inglés

NAT: Network Address Translation

ADSL: Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica

CPE: Customer-premises equipment or customer-provided equipment (CPE)

SIP: Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones)

3DES: Norma de triple encriptación de datos

AES: Norma de encriptación avanzada

FXS: Foreign Exchange Station

FXO: Foreign Exchange Office

ICMP: Internet Control Message Protocol El Protocolo de Mensajes de Control de Internet

BW: Bandwidth ancho de banda

http: HyperText Transfer Protocol El protocolo de transferencia de hipertexto

Https: Hypertext Transfer Protocol Secure , Protocolo seguro de transferencia de hipertexto

DHCP: Dynamic Host Configuration Protocol Protocolo de Configuración Dinámica de Máquinas

UDP: User Datagram Protocol

QoS Quality of Service Calidad de Servicio

AH Encabezamiento de autentificación

ESP Carga útil de seguridad de encapsulación

IKE Intercambio de claves por Internet

MD5 Condensado de mensaje 5

SHA Algoritmo de troceo seguro

DH Acuerdo sobre clave Diffie-Hellman

DES Norma de encriptación de datos

TCP (Transmission Control Protocol, en español Protocolo de Control de Transmisión

DNS domain name server

CAPITULO I

INTRODUCCIÓN

1.1 Introducción

Desde hace un par de años atrás, dentro de las industrias de telecomunicaciones, se presentaron cambios rápidos en las comunicaciones de las empresas y personas. Muchos de estos cambios surgieron desde el crecimiento rápido de la Internet y de aplicaciones basadas en el protocolo Internet (IP). La Internet ha llegado ser un significado omnipresente de la comunicación, y la cantidad total de tráfico de red basado en paquetes ha superado rápidamente al tráfico de red de voz tradicional (PSTN).

"En el despertar de estos adelantos tecnológicos, es claro para los portadores de telecomunicaciones, compañías y vendedores que los servicios y tráfico de voz será uno de las mayores aplicaciones para tomar ventaja completa de IP. Esta esperanza esta basada en el impacto de un nuevo grupo de tecnologías generalmente referidas como Voz sobre IP (VoIP) o Telefonía IP." [1]

VoIP suministra muchas capacidades únicas a los portadores y clientes quienes dependen en IP o en otra red basada en paquetes. Los beneficios más importantes incluyen lo siguientes:

- Ahorros de costos: moviendo tráfico de voz sobre redes IP, las compañías pueden reducir o eliminar los cargos asociados con el transporte de llamadas sobre la red telefónica publica conmutada (PSTN). Los proveedores de servicios y los usuarios

- finales pueden aun conservar ancho de banda invirtiendo una capacidad adicional solo cuando es necesario. Esto es posible por la naturaleza distribuida de VoIP y por los costos de operación reducida según las compañías combinen tráficos de voz y datos dentro de una red.

- Estándares abiertos e Interoperabilidad: adoptando estándares abiertos, ambos los negocios y proveedores de servicios pueden comprar equipos de múltiples fabricantes y eliminar su dependencia en soluciones propietarias.

- Redes integradas de voz y datos: haciendo la voz como otra aplicación IP, las compañías pueden construir verdaderamente redes integradas para voz y datos. Estas redes integradas no solo proveen la calidad y confianza de las actuales PSTN's, también estas redes habilitan a las compañías para tomar rápidamente ventaja de nuevas oportunidades dentro del mundo cambiante de las comunicaciones.

"En estos días, la telefonía Ip esta ligada a la transferencia de archivos por Internet de forma segura. Es decir, que todo paquete debe viajar encriptado y con seguridades para que no puedan obtener información de empresas o personas, es por esto, que es una ventaja la formación de las VPN a través de la Internet, cuando el usuario no posee un enlace dedicado."[1]

"La nueva economía exige, no como un lujo sino más bien como una necesidad, una cobertura global entre oficinas locales y remotas de una misma organización. Una red privada virtual (RPV o VPN, *Virtual Private Network*) es la interconexión de varias redes locales (LAN, *Local Area Network*) que están separadas físicamente (remotas) y que realizan una transmisión de datos entre ellas de un volumen considerable. De forma habitual, lo que se pretende es que dicho grupo de redes locales se comporten como si se trataran de una única red local, aunque por diversos motivos, fundamentalmente de índole económica, la interconexión entre dichas redes LAN se efectúa a través de medios potencialmente hostiles o

inseguros (Internet, Red telefónica conmutada o RTC a través de módem, Líneas alquiladas, RDSI o ISDN, X.25, *Frame Relay*, ATM,...), de forma que hay que articular diversos mecanismos, especialmente de encriptación y de firma digital, para garantizar la seguridad de los sistemas" [2].

Todas estas tendencia llevan a que las empresas, en este caso Intertrading Ardila Corp. De un paso más hacia el futuro tanto para su comunicación, así como, la compartición de archivos, que son un medio indispensable para que ahora se desarrolle una empresa, ahorrado recursos, y trabajando con tecnología de punta, en especial si tiene locales remotos.

La corporación INTERTRADING ARDILA, esta conformada por dos empresas que trabajan en las mismas oficinas, tanto en Quito, como en Bogota, estas son: Vanderpet y Pertel. Vanderpet es una empresa dedicada a la venta de artículos para mascotas, y la empresa Pertel, a la venta e instalación de equipos e infraestructura para cabinas telefónicas.

Las dos oficinas al estar ubicadas en diferentes países, el costo de comunicación entre ellas viene a representar un valor muy alto al final de cada mes, así como el envió de fax, la impresión de las hojas, todo suma un costo que se puede invertir en equipos de telecomunicaciones que reduzcan estos costos y se recupere muy fácilmente en pocos meses.

1.2 Situación actual de la red

La infraestructura que posee Intertrading Ardila en Quito, esta basada en un enlace de Internet de 320Kbps, entregados vía radio y un router que esta haciendo NAT. En la empresa, trabajan unas 14 personas y todas poseen acceso a Internet sin ningún tipo de restricción o algún proxy. Atrás de del router se encuentra un *switch* de 24 puertos no administrable que une todos los equipos terminales a la red. Poseen dos cámaras IP, con IP públicas cada una, con las cuales desde Colombia pueden chequear el trabajo de los empleados en Quito. En la

red están hechas dos subredes para que se manejen indistintamente la empresa Vanderpet de Pertel por motivo de cruce de información lo manejan de esta manera.

Las centrales telefónicas que poseen tanto en Quito como en Bogota son de marca PANASONIC, y poseen extensiones libres en ambos lugares, por lo que el equipo de voz se conectara a las extensiones de la central para cualquier persona pueda tomar esta extensión y comunicarse con Bogota o viceversa. Por lo que se formara un esquema FXO – FXO. Hay que tomar en cuenta que este esquema en general con cualquier equipo *gateway* de voz se va a tener conflictos en cuanto al cerrado de la línea. Es decir, se marca normalmente, se conversa, pero al momento de cerrar el teléfono la extensión se queda tomada porque no envía las cadencia correspondientes a la terminación de la comunicación, es por esto que se debe saber las cadencias de la central para poder configurarlas en el *gateway* de voz como tono de que ha terminado la conversación y se cierren las líneas.

Al momento no tienen ningún equipo, como un servidor ftp, que les permita compartir archivos de Ecuador a Colombia, ni ningún tipo de comunicación IP hacia Colombia, utilizan las líneas de abonado publico normal para comunicarse, es por esto, que ven la necesidad de implementar una solución que reduzca costos, tanto en llamadas como en la compartición de carpetas o archivos.

En las oficinas ubicadas en Bogota - Colombia, tienen un enlace de Internet tipo ADSL, con un router que es el mismo CPE que les entrega su proveedor como equipo terminal del adsl. El enlace es de 600Kbps, y existen unas 8 personas trabajando en la empresa y que tienen acceso al Internet, igual que en Quito sin ningún tipo de restricción. Todas las CPU se conectan a través de un *switch* no administrable de 24 puertos.

El otro punto donde se debe establecer la VPN para compartición de archivos, es la casa del gerente en Bogota - Colombia. En este lugar no existe ningún enlace de Internet, por lo

que se solicita la contratación de Internet con un ancho de banda no mayor a 128Kbps que será suficiente para levantar la VPN y poder navegar en Internet.

Dado que el uso del Internet no esta restringido por ningún servidor en ningún sitio, se ve la necesidad de poder administrar el ancho de banda, es decir, separar los servicios que se va a ofrecer, y esto manejarlo con priorización, por ejemplo, la voz debe tener un canal dedicado y los paquetes de este deben tener prioridad al atravesar la red, para que la comunicación de voz no se vea afectada, cuando exista inundación del canal por estar navegando en internet.

Esquema de la red:

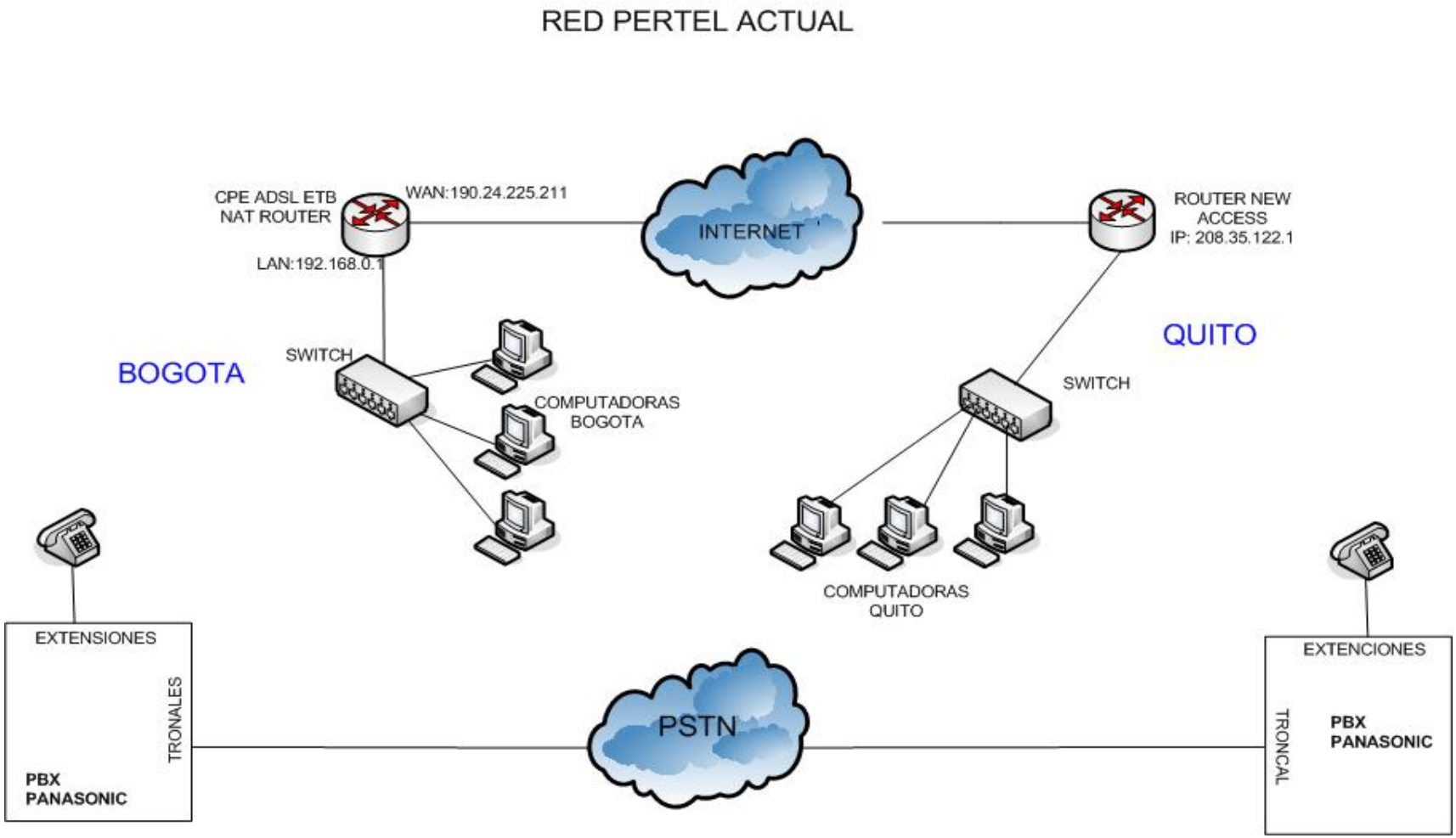


Figura 1.1 Esquema de red actual

CAPITULO 2

COMUNICACIÓN DE VOZ SOBRE IP Y VPN

2.1 Tecnología

"Las redes de voz y las redes de datos presentan tecnologías muy disímiles. Por un lado, la transmisión de voz, con una historia de más de 100 años, se basa en el establecimiento de vínculos permanentes entre dos puntos, diseñados para transmitir un tipo de señal específico: la voz humana, típica señal analógica, de ancho de banda acotado, que debe llegar a destino "inmediatamente" y ser lo más inteligible posible. Por otro lado, la transmisión de datos, con una relativa reciente historia, se basa en la transmisión de información digital, sin establecer vínculos permanentes, y donde los retardos no son generalmente importantes.

La integración de estas dos tecnologías no parece algo sencilla, y cabe preguntarse si existe alguna ventaja en realizar el intento. Las ventajas aparecen al analizar por los menos los siguientes tres aspectos:

El primero aspecto es económico: es posible ahorrar dinero al integrar las tecnologías. El segundo aspecto es de administración: es más sencillo administrar un único sistema que dos independientes. Ambos aspectos son importantes, y las Empresas, tanto desarrolladoras, como consumidoras de tecnología están haciendo una fuerte apuesta a esta integración. El tercer aspecto, y quizás a nivel del usuario presente las ventajas más relevantes, tiene que ver con la mejora en las aplicaciones. Las nuevas tecnologías de unificación de redes permitirán a los

usuarios disponer de facilidades que hasta hace un tiempo no eran posibles. La primera etapa en la integración se ha dado, no casualmente, en la transmisión a distancia. La transmisión a distancia está directamente relacionada con gastos mensuales, ya sean fijos, o por utilización. Bajar estos costos, incide directamente en los costos operativos de las Empresas.

La primera “integración” de estas redes, existe desde hace muchos años: Los MODEM (Moduladores / Demoduladores) utilizan las redes telefónicas para la transmisión de datos a distancia. Dado que las redes telefónicas existen desde mucho antes que las de datos, resulta entendible que las primeras transmisiones de datos a distancia utilizaran como soporte estas redes. Para ello se diseñaron los módems, encargados de adaptar la información “de datos” al medio telefónico. Como éste último esta diseñado para señales analógicas, de hasta 3.4 kHz de ancho de banda, los módems utilizan “tonos" dentro de esta banda para enviar los datos que desean transmitir. De esta manera, se utilizan los enlaces telefónicos, generalmente disponibles y ya amortizados, para transmitir esporádicamente datos.

Con el incremento de la cantidad computadoras y la baja de sus precios, vino aparejado la creciente necesidad de intercambio de información (“datos”), y la comunicación vía módem está limitada por las propias características de la red telefónica: el teorema de Shannon limita la cantidad de “información por segundo” que se puede transitar por un enlace de este tipo, a menos de 60 kb/s.

Luego de algún tiempo, con el crecimiento de la necesidad de transmitir datos, surgieron las primeras redes a distancia de transmisión de datos. Estas redes, inicialmente “punto a punto”, permitieron aumentar la velocidad en la transmisión de datos, con un costo fijo mensual para las empresas. En este caso, los “enlaces de datos”, no están limitados por el bajo ancho de banda de los “enlaces telefónicos”. Con la creciente demanda de transmisión de datos, estos enlaces se incrementaron, ofreciendo mayores capacidades y bajando sus costos. Hasta el punto en que, en conjunto con las tecnologías de compresión de voz, resulta actualmente más económico utilizar “enlaces de datos” para transmitir conversaciones telefónicas.

De esta manera, se invirtió la situación inicial: de utilizar la red telefónica para cursar datos, se utiliza la red de datos, para cursar tráfico de voz.” [3]

2.2 Definición de VoIP

VoIP viene de las palabras en ingles Voice Over Internet Protocol. Como dice el término, VoIP intenta permitir que la voz viaje en paquetes IP y obviamente a través de Internet.

“La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y por ende desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.

La VoIP por lo tanto, no es en sí mismo un servicio sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales conocida como la PSTN, que son redes desarrolladas a lo largo de los años para transmitir las señales vocales. La PSTN se basaba en el concepto de conmutación de circuitos, es decir, la realización de una comunicación requería el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica.

En cambio, la telefonía IP no utiliza circuitos físicos para la conversación, sino que envía múltiples conversaciones a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

Según esto son evidentes las ventajas que proporciona las redes VoIP, ya que con la misma infraestructura podrían prestar mas servicios y además la calidad de servicio y la velocidad serian mayores; pero por otro lado también existe la gran desventaja de la seguridad, ya que no es posible determinar la duración del paquete dentro de la red hasta que este llegue a su destino y además existe la posibilidad de perdida de paquetes, ya que el protocolo IP no cuenta con esta herramienta.” [1]

2.3 Protocolos H323 y SIP

2.3.1 Protocolo H.323

“Su primera versión fue lanzada en 1996 y se define como “Estándar que especifica los componentes, protocolos y procedimientos que proveen unos servicios de comunicación multimedia para las comunicaciones de audio en tiempo real, vídeo y datos en redes ya sean LANs, WANs, MANs o Internet a través de IP”.

H.323 se deriva de la especificación H.320 para videoconferencia sobre redes RDSI y constituye el marco donde se definen protocolos para la creación de servicios multimedia sobre IP. Las arquitecturas interoperables de voz sobre IP se basan en la especificación H.323 v2.

El estándar H.323 se identifican claramente cuatro tipos de componentes, que interconectados proveen comunicación: Terminales, Gateway, Gatekeepers y la MCUs. El Terminal es el dispositivo a través del cual se comunicará el usuario, es decir, teléfonos IP, teléfonos software y terminales de videoconferencia. Los gateways proveen un acceso ininterrumpido a la red IP. Se interconectan con la PSTN según corresponda, a fin de asegurar que la solución sea ubicua. El otro elemento citado, el Gatekeeper, actúa como controlador del sistema y cumple con el segundo nivel de funciones esenciales en el sistema de VoIP como: autenticación, enrutamiento del servidor de directorios, contabilidad de llamadas y

determinación de tarifas. Por último, se tiene la Unidad de Control Multipunto (MCUs) que provee soporte para las conferencias entre tres o más terminales H323.

El funcionamiento básico de un sistema H.323 requiere el registro de todos los terminales en el Gatekeeper con un alias y su dirección IP asociada mediante el protocolo de señalización RAS (Registration, Authentication and Status).” [4]

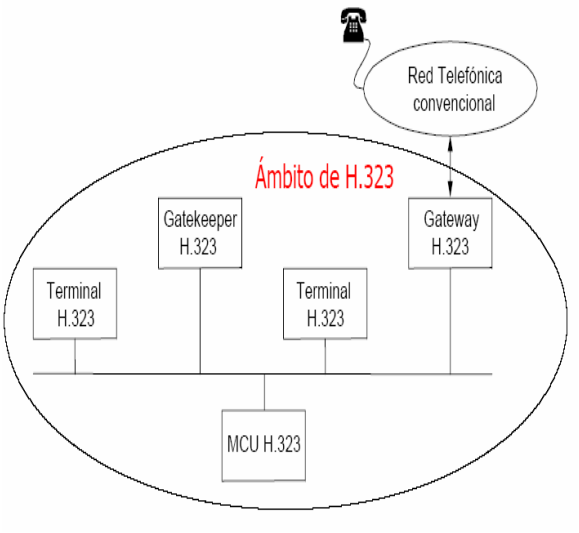


Figura 2.1 Componentes de un Sistema H.323

2.3.2 PROTOCOLO SIP

“El protocolo SIP (Session Initiation Protocol) fue introducido por la IETF en 1999, para el control de sesiones multimedia en redes IP. SIP es un protocolo de señalización para establecer las llamadas y conferencias. A diferencia de H.323 en SIP sólo se definen los elementos que participan en un entorno SIP y el sistema de mensajes que intercambian estos. Estos mensajes están basados en HTTP y se emplean esencialmente en procedimientos de registro y para establecer entre qué direcciones IP y puertos TCP/UDP intercambiarán datos los usuarios. En este sentido, su sencillez es altamente valorada por desarrolladores de aplicaciones y dispositivos.

SIP ha cobrado gran auge en el mercado principalmente por su fácil integración con HTTP, SMTP y mensajería, que lo hace ideal para el desarrollo de los servicios convergentes. La tecnología SIP está integrada por tres elementos principalmente: un User Agent SIP, un Servidor SIP y un Registro SIP. El User Agent es el software ubicado en el Terminal, de arquitectura cliente/servidor que maneja las peticiones de sesión. El Registro SIP da un servicio de información de ubicación; recibe información del Agente de Usuario y la almacena para proporcionarla a otros Agentes de Usuario.

Por su parte el servidor SIP está integrado por: Servidor Proxy SIP y un Servidor de Redireccionamiento SIP. El Servidor Proxy SIP es un servidor de tipo intermedio SIP, se encarga de reenviar peticiones desde el Agente de Usuario hacia el siguiente Servidor SIP, y retienen la información para efectos de contabilidad o facturación. El papel del Servidor intermedio de Redireccionamiento es responder a la resolución de nombres y la ubicación del usuario. El funcionamiento básico en caso de SIP requiere que el usuario al iniciar la sesión se registre con su dirección SIP-URI, un identificador similar a los utilizados en correo electrónico (el formato es user@domain), y su actual dirección IP en el Servidor de Registro.”[4]

2.3.3 H.323 VS. SIP

“Tanto H.323 como SIP para el establecimiento y señalización de llamadas, así como intercambio de capacidades, control de medios y servicios adicionales sobre redes IP. A continuación se establecen comparaciones entre ambas tecnologías, identificando diferencias, similitudes, ventajas, etc.

A la hora de hablar de teleconferencia ó videoconferencia sobre redes IP, H.323 ha sido la referencia durante más o menos los últimos cinco años. Sin embargo, desde la aparición de SIP, se comienza a poner en entredicho esta supremacía. Este hecho está fundamentado en la naturaleza propia de H.323 que expone una serie de factores que lo limitan como un protocolo para las grandes masas. Inicialmente H.323 se creó con la idea de extender SS7 hacia estas

redes, y siempre con la premisa de la total compatibilidad con los estándares anteriores, ya sean para conmutación de circuitos o de paquetes. En cierto modo, la idea era llevar la telefonía convencional hacia redes IP. Ahora bien, la integración de H.323 con Internet se ve obstaculizada por características propias de ésta tecnología. Por ejemplo, H.323 no usa ninguno de los estándares aprobados por el IETF para Internet: no proporciona servicios complementarios ni se aprovecha del trabajo que ya está hecho y que funciona correctamente.

A diferencia de SIP, H.323 no establece relación con protocolos de la red como HTTP, o los de correo electrónico (SMTP, POP3, etc.). Sin embargo hay que recordar que H.323, a pesar de ser un protocolo muy específico, ha sido la referencia de la industria hasta el momento.

H.323 sigue una dirección top-down como todo estándar de la UIT-T, por tanto, describe un marco específico y completo que abarca: protocolos detallados, estado de las máquinas y flujo de mensajes para comunicaciones multimedia. Esto incluye indicaciones específicas para factores como calidad de servicio, seguridad y movilidad. Por su parte SIP, sigue la filosofía IETF, donde los sistemas y las aplicaciones son enmarcados por la combinación de módulos. Los protocolos estandarizados por la IETF son independientes de las aplicaciones.

Un aspecto fundamental de SIP frente a H.323 es ésa modularidad del primero. SIP sólo gestiona sesiones, y en su más íntimo significado no aspira a nada más, siendo su uso para VoIP una aplicación de sus posibilidades. Todo aquello que escape de este marco no es realizado por SIP, que lo deja en manos de otros protocolos ó sistemas, según proceda. Para ver claro este concepto, pongamos como ejemplo la reserva de recursos en una red para asegurar una calidad de servicio (QoS); H.323 está diseñado verticalmente e implementa todo aquello necesario para tener una comunicación verbal y/o visual óptima. Por lo tanto, los gatekeepers de una red H.323 se encargan de la reserva de recursos y la QoS. Esto presenta el grave problema de que las tecnologías en este campo evolucionan muy rápidamente, y de que las soluciones tomadas hace un lustro hoy estarán posiblemente desfasadas.” [4]

A continuación se establecen las especificaciones y el comportamiento de cada estándar de acuerdo a características como:

- **Seguridad**

H.323 define mecanismos de seguridad y facilidades de negociación vía H.235, también puede utilizar SSL la capa de transporte. Por su parte SIP soporta mecanismos de autenticación vía HTTP.

- **Arquitectura**

H.323 cubre servicios como capacidad de intercambio, control de conferencia, señalización básica, QoS, registro, etc. A diferencia de SIP, que por ser modular, cubre servicios de señalización de llamadas, localización y registro de usuarios. Otras características son manejadas por protocolos ortogonales.

Las entidades que sostienen una red H.323 incluyen gateways, terminales, puentes de comunicación junto a un Gatekeeper. La arquitectura para este protocolo es par a par (peer-to-peer) soportando comunicación de usuario-por-usuario sin necesidad de una entidad de control centralizado.

SIP como se explicó inicialmente, incluye los user agents, análogos a los terminales de H.323 pero que pueden operar como cliente o servidor, dependiendo del rol que tome en una llamada particular, si es solicitando o respondiendo una petición de sesión. La arquitectura SIP requiere un servidor Proxy para enrutar las llamadas a otras entidades y un servidor de registro, los demás componentes de la red no están definidos y no son obligatorios para establecer una llamada.

- **Integración con Versiones Anteriores**

En SIP una nueva versión puede descartar algunas viejas características que no sean esperadas. Esto permite conservar partes del código, reduciendo la complejidad del protocolo, sin embargo, la compatibilidad entre diferentes versiones puede perderse. Por su parte H.323 permite la completa compatibilidad de todas las implementaciones, basadas en diferentes versiones del protocolo. Aunque esto es así, eliminar funcionalidades antiguas y añadir nuevas, presentaría inconvenientes, por lo que siempre se tendrá la rémora de un protocolo complejo.

- **Integración con PSTN**

H.323 toma protocolos de la tradicional PSTN como por ejemplo Q.931, por lo tanto, permite la integración con PSTN. Sin embargo, no emplea la tecnología de conmutación de circuitos, como SIP, ya que se basa en la conmutación de paquetes. Contrariamente, SIP no posee elementos comunes con PSTN y cada señalización debe ser "*shoe-horned*" en SIP.

- **Video y Data Conferencia**

H.323 soporta tanto la conferencia de datos como la de video. Tienen lugar procesos para el control de la conferencia y la sincronización de los streams de audio y video. SIP no soporta protocolos como el T.120 para la conferencia de datos. No posee mecanismos de sincronización ni de control para la conferencia.

- **Codificación de Mensajes**

En H.323 los mensajes son codificados en un formato binario compacto que es apropiado para conexiones de banda ancha y banda angosta. Este tipo de codificación se emplea para reducir el tamaño de la transmisión y resguardar el ancho de banda. SIP sólo entiende mensajes estilo direcciones URL y los mensajes son codificados en textos, en lugar

de binario. Esto facilita su entendimiento pero aumenta el tamaño del mensaje que será enviado.

- **Disponibilidad de Servicios**

A continuación se presenta una tabla comparativa de la disponibilidad de servicios en SIP y H.323

Tabla 2.1 Disponibilidad de servicios en SIP y H.323

CARACTERÍSTICA	SIP	H.323
Transferencia ciega	Sí	Sí
Transferencia asistida por operador	Sí	No
Llamada en espera	Sí, mediante SDP	No
Conferencias multicast	Sí	Sí
Conferencias multicast y unicast simultáneas	Sí	Sí
Posibilidad de uso de Gateways	Sí	Sí
Redireccionamiento	Sí	Sí
Buzones de voz/vídeo	Sí	No
Localización automática	Sí	No

Generalmente ambos protocolos soportan de señalización similares, aparte del hecho de que ambos están continuamente enriqueciéndose con nuevos métodos. Sin embargo, SIP destaca en el soporte para servicios móviles de carácter personal, con redireccionamiento de la llamada a varias posiciones distintas. En éste tema el soporte de H.323 es casi nulo.

- **Escalabilidad**

Inicialmente H.323 no contempló el aspecto de direccionamiento, ya que nace en el entorno de las redes LAN. Posteriormente se trató de subsanar este problema introduciendo el concepto de "zona H.323", que sin embargo sigue teniendo problemas de escalabilidad, y otros como el direccionamiento entre zonas. Con respecto a los componentes de red y el soporte de múltiples conversaciones, se dificulta para zonas H.323 muy grandes, ya que el Gatekeeper tiene que conocer el estado de cada llamada que maneja. En SIP cuando la carga de llamadas en la red es elevada, se pueden usar los servidores de redirección, que no mantienen ningún tipo de estado. Es más, aún manteniendo los servidores como proxies, podemos usarlos con ó sin estado ('stateful' ó 'stateless'), beneficiándose del hecho de que por defecto, SIP funciona sobre UDP.

- **Funcionalidad**

Cada protocolo maneja la configuración llamadas, el control de las llamadas, y medios de diversas maneras. H.323 contiene la definición de cada uno de ellos. Mientras que SIP define configuración de llamadas y uso de protocolos para control de llamadas, siendo manejado cada uno por separado. Por otro lado, está la capacidad de intercambio. Después de configurar la llamada en H.323, los terminales anuncian la capacidad que ellos tienen para variables como compresión y video, ya que dichas variables pueden cambiar durante la llamada, la configuración de la llamada puede ser cambiada a mitad de llamada (mid-call). Para el caso de SIP estos parámetros sólo pueden ser cambiados al inicial una nueva llamada. Para la comunicación multimedia, el hecho de que SIP no permita "*mid-call*" podría ser relevante.

- **Características Adicionales**

• H.323 es otro protocolo de señalización para sesiones interactivas en tiempo real.

- H.323 es un conjunto completo, integrado verticalmente por protocolos para conferencia multimedia: señalización, registro, control de admisión, transporte y codecs.

- SIP es un componente único. Trabaja con RTP, pero no es obligatorio. Puede combinarse con otros protocolos y servicios.

- H.323 procede del mundo de telefonía clásica (IUT).

- SIP procede de IETF: Aplica muchos conceptos de HTTP.

H.323 es el protocolo más maduro de los dos, sin embargo, la carencia de flexibilidad, limita su utilización. SIP está actualmente menos definido, pero tiene más escalabilidad lo cual, hace más fácil su integración con Internet. Establecer cual de los dos es mejor sería apresurado, aunque el de mayor característica favorable es SIP, es necesario analizar las características del sistema a implementar para tomar la decisión más conveniente.

2.4 Protocolos de VPN

2.4.1 Definición de VPN

“Una red privada virtual es un grupo de dos o más sistemas de computadora conectados "en condiciones seguras" a través de una red pública. Se puede instalar una VPN entre una máquina individual y una red privada (conexión a distancia de usuario a sitio) o entre redes privadas (de sitio a sitio). El tipo de seguridad difiere de un producto a otro, pero la mayoría de los expertos en seguridad coinciden en que las VPN deberían estar dotadas de encriptación, de una autentificación sólida de los usuarios o computadoras centrales distantes, y de mecanismos para ocultar o enmascarar información sobre la topología de la red privada frente a posibles atacantes desde la red pública.”[5]

2.4.2 Necesidades y surgimiento de las VPNs

"Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante *Remote Access Services*(RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos.

Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.” [6]

2.4.3 Estructura de las VPNs

“Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

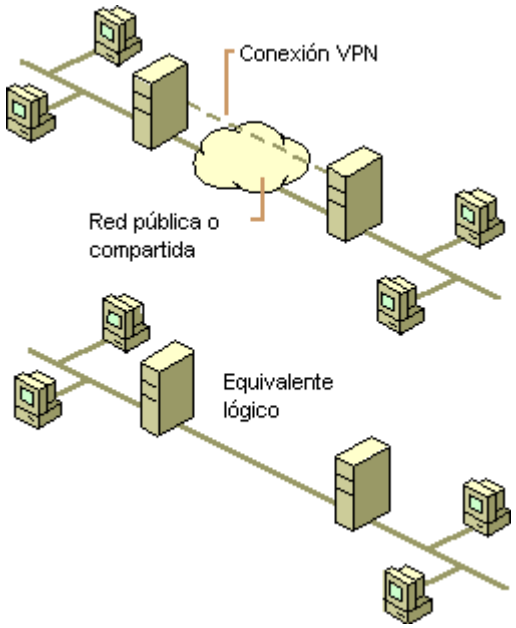


Figura 2.2 Red VPN

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la

empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de túneles (“Tunneling”) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de *hashing* para derivar un valor incluido en el mensaje como *checksum*.

Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autenticación son *Challenge Handshake Authentication Protocol* (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de *proposals* del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-*Point Tunneling Protocol* (PPTP), *Layer-2 Fowarding Protocol* (L2FP) y el modo túnel de IPSec."[6]

2.4.4 Protocolos utilizados en las VPNs

- **PPTP**

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

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.

El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo *Generic Routing Encapsulation* (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un encabezado de envío, un encabezado Ip, un encabezado GREv2 y el paquete de carga. El encabezado de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El encabezado IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

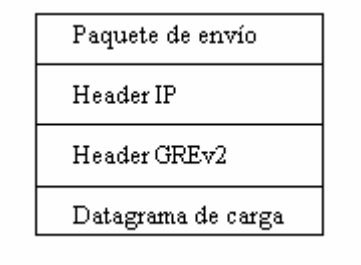


Figura 2.3. Capas de encapsulamiento PPTP

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, estándar en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un estándar propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

- **IPSec**

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad.

La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA

cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel es:

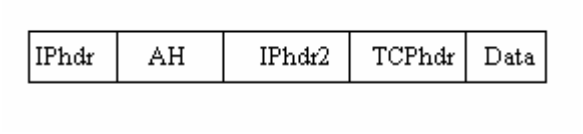


Figura 2.4. Paquete AH en modo tunel

Un ejemplo de paquete AH en modo transporte es:

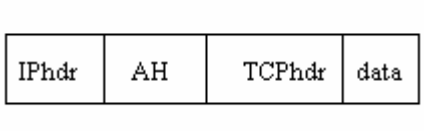


Figura 2.5. Paquete AH en modo transporte

Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:

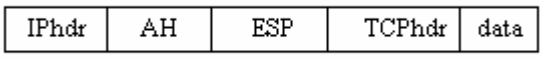


Figura 2.6. Combinación AH y ESP

Este tipo de paquete se denomina Transport Adjacency.
La versión de entunelamiento sería:

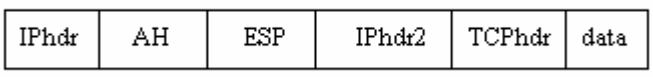


Figura 2.7. Paquete de entunelamiento

Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado.

Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.[6]

- **L2TP**

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.
El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:

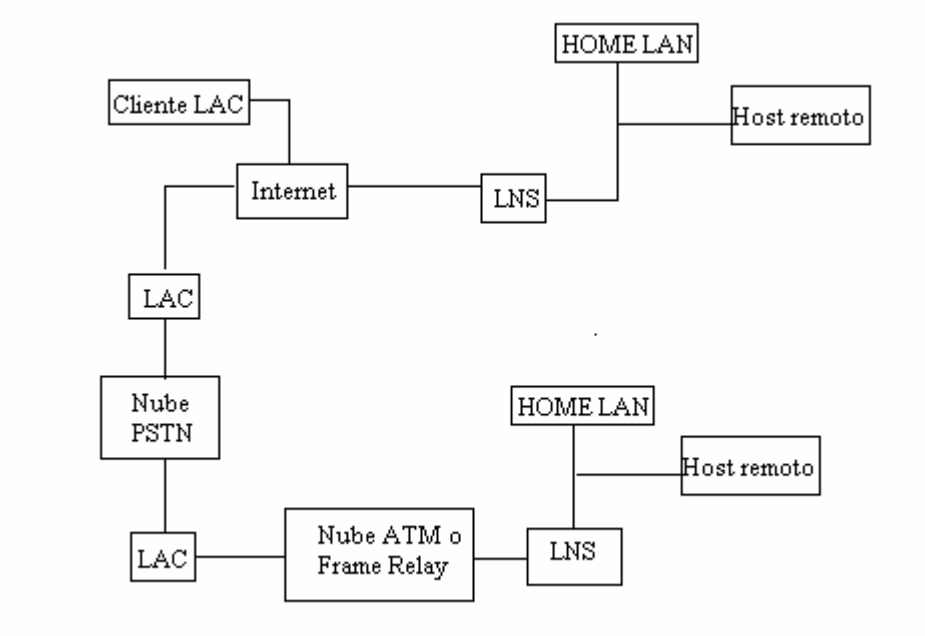


Figura 2.8. Escenario L2TP

Un L2TP Access Concentrador (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP. Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC. Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain. L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel. La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

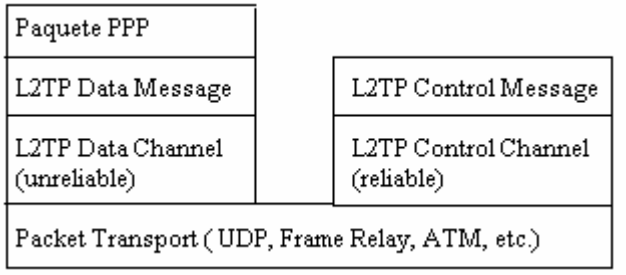


Figura 2.9. Relación entre PPP y L2TP

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión. [6]

2.5 Aspectos de Regulación de VoIP

La regulación que existe para la comunicación de voz sobre ip en el país, esta básicamente definida para la parte de cybercafes, locutorios o empresas que prestan servicios de Internet al publico. En el cual indica que esta prohibido el uso de *gateways* de voz sobre ip que vayan conectados a la PSTN normal. **Resolución No. 073-02-CONATEL-2005 articulo 4)**.

Siendo esta ley la vigente, y que no permitiría el uso de equipos se tiene como referencia una carta enviada en el ano 2005 al presidente de la senatel Dr. Hernan Leon, refiriéndose al uso de *gateway* de voz para empresas privadas y si es posible la conexión a la PSTN de los mismos, el cual supo manifestar en su carta de contestación que no se esta quebrantando ninguna ley al hacerlo de manera privada, siempre y cuando el uso sea únicamente para la empresa, sin fines de lucro.

Resoluciones del SENATEL y cartas enviadas en anexo 1.

CAPITULO 3

DISEÑO DE LA NUEVA RED

3.1 Diseño

Para el diseño se debe tomar en cuenta que requerimientos se necesita para poder cumplir con el objetivo de la empresa, que es compartir datos a través de Internet de sucursal a sucursal, y tener comunicación IP igualmente de sucursal a sucursal por lo que se presenta un esquema de los equipos que se emplearía para buscar la mejor solución.

El esquema que se plantea para arrancar en el diseño es el siguiente:

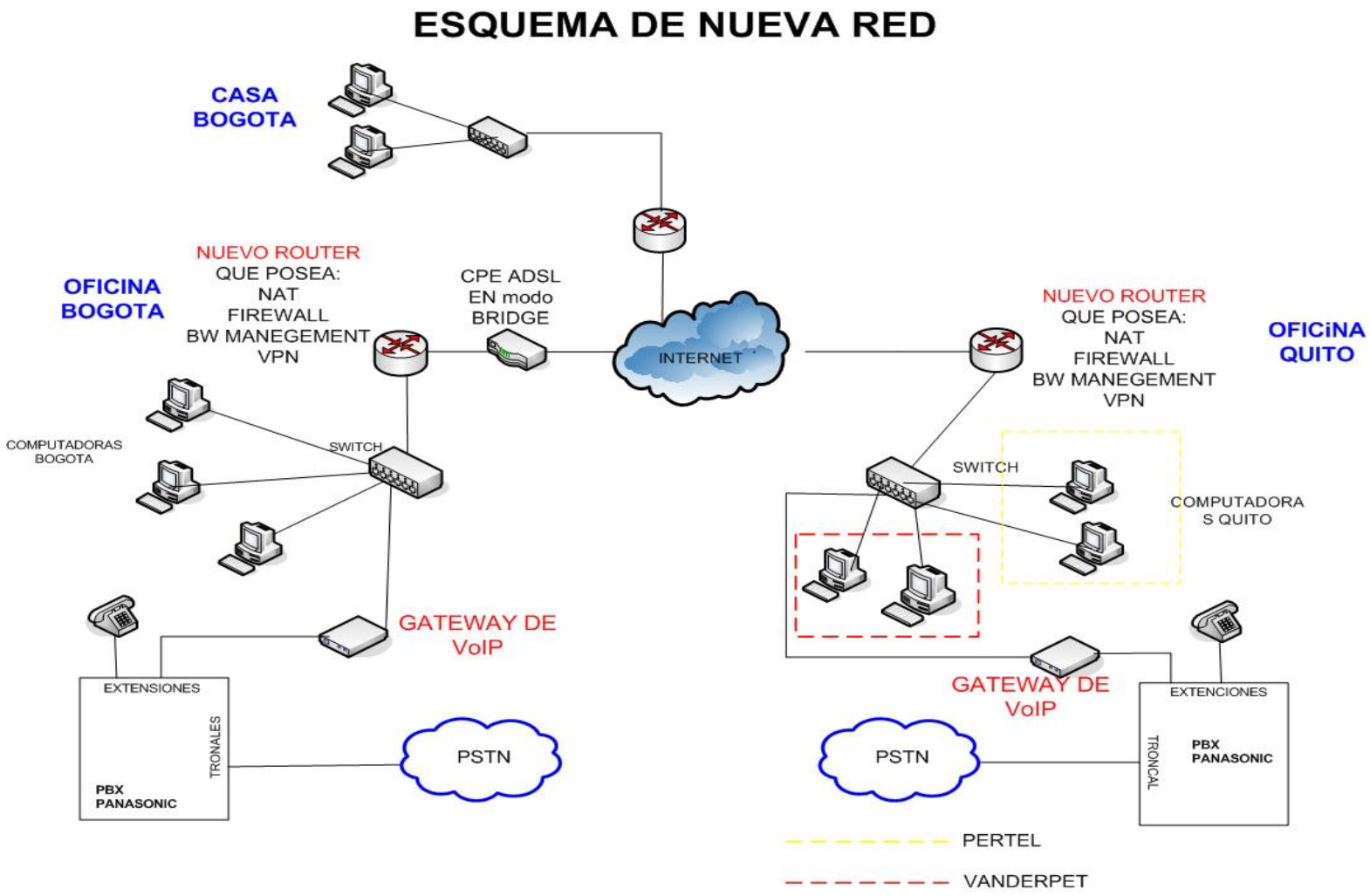


Figura 3.1 Esquema de nueva red

3.2 Estructura física

Las características de los equipos que se van a utilizar en la solución son los siguientes:

3.2.1 Características del Router

3 equipos que tengas y hagan las siguientes funciones:

- NAT
- Firewall
- BW management
- Port Forwarding
- 4 puertos LAN RJ-45
- 1 puerto WAN
- DHCP Server
- VPN (IPsec)
- Interfase Ethernet 10/100 auto negociable

3.2.2 Características del equipo de VoIP

2 equipos que posean las siguientes características:

- Protocolos H323 y SIP
- Codecs: G.729, G.723.1, G.711 como mínimo
- 1 puerto FXO para RJ-11
- Buffer de almacenamiento
- Que trabaje punto a punto sin servidor

3.2.3 Características del Switch

Estos equipos serán entregados por parte de la empresa son de capa 2 no administrables

3.2.4 Características de las Cámaras

Cámaras IP que ya posee la empresa, que se manejan con nivel de seguridad pidiendo nombre de usuario y clave de acceso para poder ingresar.

Para la selección del equipo que cumpla mejor con las características requeridas se va a comparar algunos que existen en el mercado, para escoger el que mejor cumpla a estas necesidades.

3.2.5 Comparación de Routers existentes en el mercado

NETGEAR Router/Firewall VPN FVS124GGE [5]

Figura 3.2 Router Netgear

Características:

Interfaces/Puertos 4 x RJ-45 10/100/1000Base-T Auto-sensing/Auto MDI/MDI-X LAN 2 x RJ-45 10/100Base-TX WAN

Información Técnica:

Ratio de Transferencia de Datos 10Mbps

25 Túneles VPN

Packet Filtering

IPSec

NAT-Traversal One-to-One NAT

NAT (de muchos a uno)

Protecciones del Firewall

Inspección de Paquete de Estado Denial of Service,

filtración URL,

Fitrado de contenidos,

Encriptación (DES, 3DES, AES),

autentificación (MD5, SHA1),

Router CISCO 1711R 4FE VLAN [5]

Figura 3.3. Router Cisco 1711R

Detalles del producto:	
General	
Device Type	Router
Memory	
RAM	96 MB (installed) / 128 MB (max)
Flash Memory	32 MB (installed) / 32 MB (max)
Networking	
Integrated Switch	4-port switch
Data Link Protocol	Ethernet, Fast Ethernet, PPP, MLPPP
Network / Transport Protocol	RSVP, IPSec, SLIP
Protocolo de enrutamiento	OSPF, HSRP
Administración Remota	SNMP, Telnet, HTTP
Modo de comunicacion	Half-duplex, full-duplex
Performance	VPN throughput (3DES IPSec) : 15 Mbps Firewall throughput : 20 Mbps VPN throughput (AES IPSec) : 4.5 Mbps Intrusion detection throughput : 20 Mbps
Capacidad	Virtual interfaces (VLANs) : 16 Concurrent VPN tunnels : 100
Características	Firewall protection, switching, DMZ port, auto-sensing per device, DHCP support, NAT support, hardware encryption, VPN, auto-negotiation, VLAN support, auto-uplink (auto, traffic shaping, Stateful Packet Inspection (SPI), DoS attack prevention, content filtering, Intrusion Detection System (IDS), URL filtering, , Weighted Fair Queuing (WFQ)
Compliant Standards	IEEE 802.1D, IEEE 802.1Q
Miscellaneous	
Encryption Algorithm	Triple DES, AES, IKE

Router-Firewall-Switch-VPN ZYXEL ZyWall2 [7]

Figura 3.4. Router Zywall 2

	General
Tipo de dispositivo	Aparato de seguridad
	Conexión de redes
Factor de forma	Externo
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Protocolo de conmutación	Ethernet
Red / Protocolo de transporte	PPTP, PPPoE
Protocolo de gestión remota	Telnet, HTTP, HTTPS
Capacidad	Túneles VPN IPSec : 5

Características	Protección firewall, conmutación, soporte de DHCP, soporte de NAT, asistencia técnica VPN, señal ascendente automática (MDI/MDI-X automático), Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), filtrado de contenido, activable, actualizable por firmware, prevención de ataque DDos
Algoritmo de cifrado	DES, Triple DES, AES, IKE, PKI, MD5
Método de autentificación	Secure Shell (SSH), certificados X.509
	Expansión / Conectividad
Interfaces	4 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (LAN / DMZ) ¦ 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN) ¦ 1 x gestión - RS-232 - RJ-45 ¦ 1 x serial - RS-232 – RJ-45

3.2.6 Cuadro comparativo para mejor selección de router

Tabla 3.1. Comparación entre Routers VPN

Router	Firewall	Nat	Vpn	Bw management	Port Forwarding	Costo $
Netgear	SI	SI	25 Vpn IpSec	NO	SI	$281
Cisco	SI	SI	100 vpn IPsec	SI	SI	$600
Zyxel	SI	SI	5 vpn IpSec	SI	SI	$250

Por costos y requerimientos a esta solución se empleara el Router Zywall 2 plus de marca ZYXEL.

3.2.7 Equipos de Voz sobre IP del mercado

Linksys SPA3102 Voice Gateway [10]

Figura 3.5. Gateway Linksys

Descripción del producto:

Linksys SPA3102 Voice Gateway with Router - pasarela de VoIP

Tipo de dispositivo: Pasarela de VoIP

Tipo incluido: Externo

Protocolo de interconexión de datos: Ethernet, Fast Ethernet

Red / Protocolo de transporte: TCP/IP, UDP/IP, ICMP/IP, PPPoE

Protocolo de gestión remota: HTTP, HTTPS

Protocolos VoIP: SIP v2

Interfaces de telefonía: 1 teléfono (FXS), 1 línea (FXO)

Características: Puerto DMZ, soporte de DHCP, soporte de NAT, soporte para Syslog

MVP130 Multitech [11]

Figura 3.6. Gateway de VoIP Multitech

Características

1 puerto analógico y 1 puerto digital para establecer una comunicación sobre redes IP existentes o sobre Internet.

Conectividad Ethernet y compatibilidad total con los enrutadores e infraestructura WAN existentes.

Conectores FXS/FXO y E&M por cada canal para realizar conexiones analógicas directas a teléfonos, sistemas combinados, compresión de la voz de hasta 5,3K por cada canal con soporte de múltiples algoritmos, incluyendo ITU G.723 y G.729.

Los equipos MultiVOIP Digitales se conectan directamente a las Centrales Telefónicas privadas o al Sistema Público de Telefonía a través de T1/E1 o PRI.

Soporte de H.323 o SIP para enviar voz sobre la Internet.

La Recuperación por Sistema Telefónico (PSTN fail-over) enruta automáticamente las llamadas hacia el Sistema Telefónico convencional cuando la red IP está inoperante.

Soporte de servicios suplementarios H.450 para ofrecer transferencia de llamadas, enrutamiento de llamadas, retención de llamadas, llamada en espera e identificación por nombre.

Compresión de voz de hasta 5.3 Kbps, por llamada.

Relevo de facsímiles en tiempo real T.38 para compatibilidad con otros equipos de VoIP.

Relevo de modulación de módem que soporta conexiones de módem sobre redes de IP (de hasta 14.4 Kbps).

SP5012 Dispositivo de acceso para Voz sobre IP FXO [11]

Figura 3.7. Gateway de VoIP Micrones

Características

Cumple con el estándar ITU-T H.323.

Provee un puerto RJ-11 de FXS para teléfonos analógicos o líneas troncal de conmutador.

Provee un puerto RJ-11 de FXO para líneas analógicas de la red telefónica pública o extensiones analógicas de un conmutador.

Provee dos puertos Ethernet RJ-45 10/100 Mbps.

Soporta los codificadores y decodificadores (CODEC) de voz estándar G.711A/g law, G.723.1, G.729A.

Provee un segundo tono de marcado para la red telefónica pública.

Provee la función inteligente de ruteo de llamada.

Soporta la característica de detección de actividad de voz (denominada VAD, por sus siglas en inglés *Voice Activity Detection*).

Soporta la característica de generación de ruido confortable (denominada CNG, por sus siglas en inglés *Comfort Noise Generation*).

Soporta la característica de cancelación adaptable de eco.

Soporta configuración vía consola Telnet y una interfase de navegador de Internet.

Soporta dirección IP estática, DHCP y PPPoE.

Soporta servicio de nombres de dominio dinámico (denominado DDNS, por sus siglas en inglés *Dynamic Domain Name Service*).

Soporta Calidad de servicio (QoS) al configurar los parámetros de tipo de servicio de paquetes de voz sobre IP.

Cumple con Microsoft NetMeeting V3.0.

Soporta TFTP/FTP para actualización de firmware.

Transmisión de voz y fax T.38.

3.2.8 Cuadro comparativos de equipos de VoIP para seleccionar el adecuado

Tabla 3.2 Comparación entre gateways de VoIP

Gateway de VOIP	**Protocolo SIP y H323**	**Codec G.723.1 G729 G711**	**Buffer (jiter)**	**Puertos FXS y FXO**	**Per to per**	**Costo $**
Linksys	Solo SIP	Si	No	No	Si	$97.2
Multitech	AMBOS	Si	Si	Si	Si	$336
Micronet	Solo H323	Si	Si	Si	Si	$249

Se selecciono el equipo MVP130 de marca multitech, debido a sus características que posee superando a cualquier otro equipo en el mercado. A parte de su hardware posee prestigio como uno de los equipos mas vendidos en el mundo por su gran calidad de voz. Es un equipo robusto fuerte que puede soportar condiciones ambientales extremas como la humedad, que se ha comprobado su trabajo en el oriente. A pesar de su precio, se lo considerara como una inversión puesto que vale la pena emplearlo para este escenario. Como caracteristica adicional, se ha comprobado que la comprensión que realiza de la voz es mucho mejor que la de otros equipos por ejemplo trabajando con coder G.729 que comprime a 8 kbps, utiliza un ancho de banda 14 Kbps reales.

3.3 Diseño Lógico

Para que se puedan ver, entender y conversar los equipos terminales deben existir reglas lógicas para el efecto. Es decir, necesitamos direccionamientos IP para cada equipo que va a pertenecer a esta red, tomando en cuenta que son tres redes distintas que están remotamente una lejos de la otra, y se van a comunicar a través de las VPN.

Se van a manejar tres redes distintas en cada sitio:

Ardila Quito – Red 1

Ardila Bogota – Red 2

Casa Sr. Ardila – Red 3

3.3.1 Diseño para la Red 1

Se debe tomar en cuenta el número de usuarios que están dentro de la red para dar el direccionamiento correcto. Tomando en cuenta que al ser redes privadas deben tener IP's privadas. Y que el requerimiento del gerente de la empresa es que se manejan dos redes distintas por ser dos empresas distintas y no deben compartirse información entre ellas.

Aquí laboran 14 personas por lo que se dará un IP de red con mascara de 24 bits.

La IP de red es la 192.168. 12.0 con mascara 255.255.255.0 para la parte LAN 1, para la parte LAN 2 la red 192.168.13.0 con mascara 255.255.255.0

La IP Wan que va al equipo es la IP Publica que entrega el ISP, es la 208.9.56.37 con mascara 255.255.255.252

Las IP que se asignaran a los equipos y cámaras son:

Zywall LAN	192.168.12.1
Zywall LAN ip alias	192.168.13.1
Gateway Multitech	192.168.12.250
Cámara 1	192.168.12.20
Cámara 2	192.168.12.21

3.3.2 Diseño para la Red 2

Igual que en Quito existen 10 personas trabajando en este local por lo que igual se dará una red con mascara de 24 bits.

Red : 192.168.0.0 Mascara: 255.255.255.0

Las IP que se asignaran a los equipos son:

Zywall LAN	192.168.0.254
Zywall WAN	201.245.21.126
Gateway Multitech	192.168.0.250
Cámara	192.168.0.39

3.3.3 Diseño para la Red 3

Para la casa del Sr. Ardila se empleara una la IP de red 192.168.14.0 con mascara de 24 bits.

La IP Lan del zywal es la 192.168.14.1/24

Para la IP wan para el equipo se va a dejar que el router obtenga la ip dinámicamente por parte del proveedor, es decir, con cliente dhcp, ya que para este lugar no se contrato una ip publica fija. Aquí se va a poner un access point a la cual se le asignara la IP 192.168.14.2/24

Todas las IP que se van a manejar son ip que la empresa ya tenia en cada una de sus redes, y no se cambio por recomendación de ellos para evitar conflictos en sus sistemas que ya vienen trabajando, pero se redefinieron algunas, ahora que van a estar conectadas las redes entre si. Igualmente las IP publicas ya las venían manejando en todas las sucursales por lo ya se tenia el dato de la IP para cada lugar.

Por lo que la red quedaría definida de la siguiente manera:

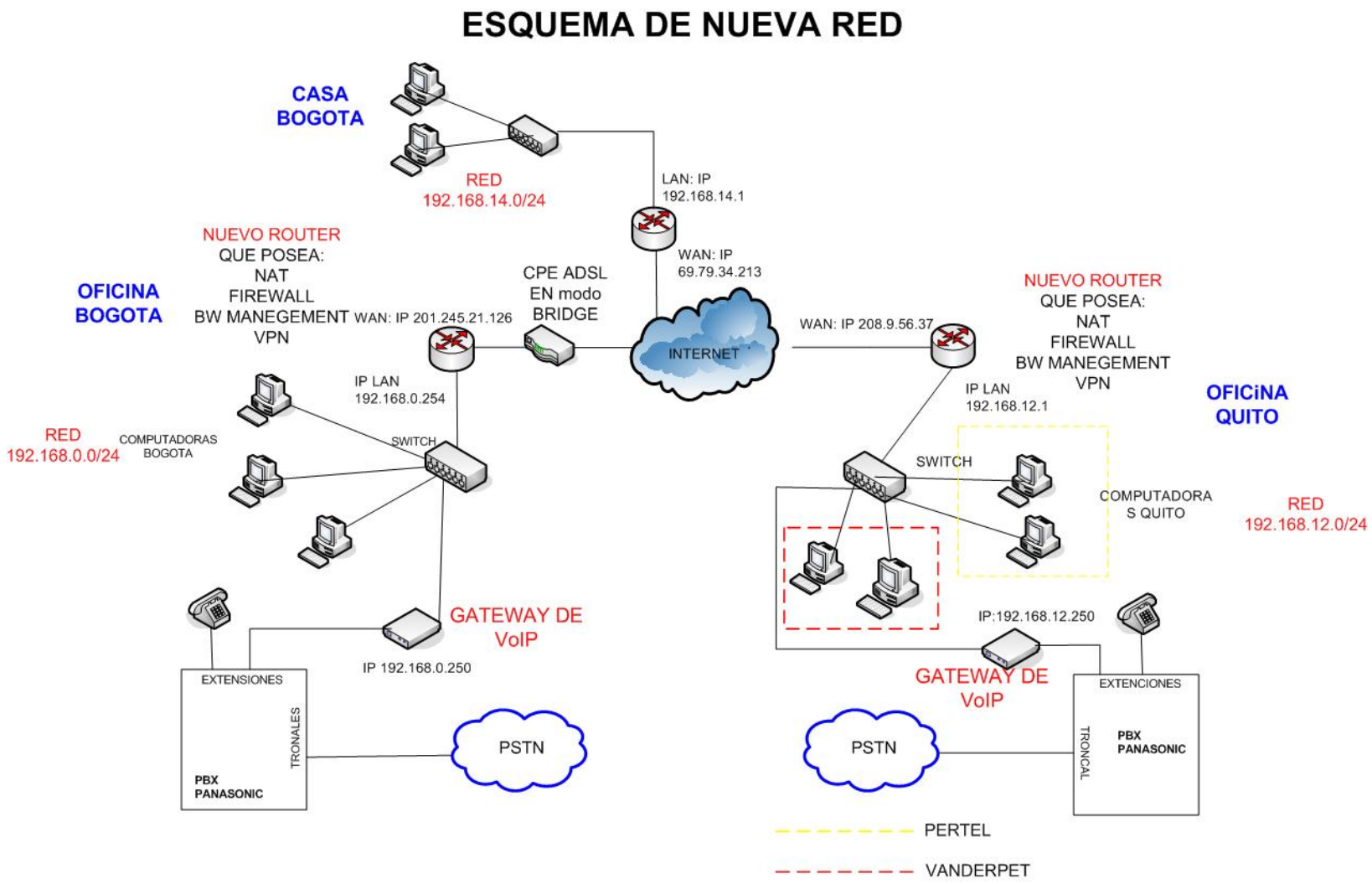


Figura 3.8 Diseño de nueva red

3.4 Configuración para los equipos y protocolos a emplearse

Para la configuración de los equipos se debe estandarizar que parámetros se van a ocupar en cada uno de los, teniendo en cuenta que se van a levantar VPN que para su entendimiento deben tener las mismas seguridades, así como la voz sobre deben tener la configuración exacta en cada uno de los equipos para su comunicación.

3.4.1 Las reglas para oficinas de Ardila en QUITO

Firewall

- De LAN a WAN, se permitirá que salga cualquier tipo de información hacia el exterior sin bloquear ningún puerto.
- De LAN a LAN, estará permitido todo trafico
- De WAN a LAN, se permitirá únicamente que se ingrese a las dos cámaras IP mediante puertos 80 y 81.
- DE VPN a VPN, todo servicio permitido.
- De WAN a WAN, permitido el ICMP, y administración remota del router mediante HTTPS puerto 444.

Nat

- Regla de Uno a varios, una IP Publica que manejara el router y a través de esta IP con puerto 80 y 81 se podrá acceder a las cámaras IP y todos los equipos atrás de este router navegaran con esta IP.

Vpn

Para la formación de la VPN, se debe ver los protocolos y encriptaciones que se empleara para formarla, teniendo en cuenta las seguridades debidas para que la información que va a

atravesar de Bogota a Quito o viceversa viaje completamente segura y nadie pueda corromper esta seguridad.

Como son dos reglas que se manejaran para formar las 2 VPN necesarias se empleara diferentes sistemas de claves y encriptaciones.

Vpn Oficinas UIO - BGT

Regla General:

Pre-shared Key: ardila2007

Ike Proporsal:

Modo de negociación: MAIN
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time: 28800
Key Group: DH1

IPsec Proporsal:

Modo de encapsulación: Túnel
Protocolo Activo: ESP
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time 28800
Perfect Forward Secrecy: DH1

Vpn Oficina UIO – Casa Ardila

Regla General:

Pre-shared Key: adpertel07

Ike Proporsal:

Modo de negociación: MAIN
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time: 28800
Key Group: DH1

IPsec Proporsal:

Modo de encapsulación: Túnel
Protocolo Activo: ESP
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time 28800
Perfect Forward Secrecy: DH1

VoIP:

Se va a trabajar con protocolo H323 debido a que este protocolo surgió para trabajar de punto a punto sin necesidad de un servidor y trabaja con protocolos que manejas QoS.

Se trabajara con codec G.729 de 8 Kbps de compresión. Puerto FXO.

3.4.2 Las reglas para la oficina de Ardila en BOGOTA

Firewall

- De LAN a WAN, se permitirá que salga cualquier tipo de información hacia el exterior sin bloquear ningún puerto.
- De LAN a LAN, estará permitido todo trafico
- De WAN a LAN, se permitirá únicamente que se ingrese a la cámara IP, y al equipo de voz sobre IP mediante puertos 80 y 81.
- DE VPN a VPN, todo servicio permitido.
- De WAN a WAN, permitido el ICMP, y administración remota del router mediante HTTPS puerto 444.

Nat

- Regla de Uno a varios, una IP Publica que manejara el router y a través de esta IP con puerto 80 y 81 se podrá acceder a la cámara IP, y a equipo de voz sobre IP y todos los equipos atrás de este router navegaran con esta IP.

Vpn

Para la formación de la VPN, se debe ver los protocolos y encriptaciones que se empleara para formarla, teniendo en cuenta las seguridades debidas para que la información que va a atravesar de Bogota a Quito o viceversa viaje completamente segura y nadie pueda corromper esta seguridad.

Regla General:

Pre-shared Key: ardila2007

Ike Proporsal:

Modo de negociación: MAIN
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5

SA life time: 28800
Key Group: DH1

IPsec Proporsal:

Modo de encapsulación: Túnel
Protocolo Activo: ESP
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time 28800
Perfect Forward Secrecy: DH1

VoIP:

Se va a trabajar con protocolo H323 debido a que cuando se conecta únicamente dos equipos punto a punto este responde de manera más rápida que SIP.

Se trabajara con codec G.729 de 8 Kbps de compresión. Puerto FXO.

3.4.3 Las reglas para la casa de Sr. Ardila en BOGOTA

Firewall

- De LAN a WAN, se permitirá que salga cualquier tipo de información hacia el exterior sin bloquear ningún puerto.
- De LAN a LAN, estará permitido todo trafico
- De WAN a LAN, No se permitirá ningún trafico
- DE VPN a VPN, todo servicio permitido.
- De WAN a WAN, permitido el ICMP, y administración remota del router mediante HTTPS puerto 444.

Nat

- Regla de Uno a varios, una IP Publica que manejara el router y todos los equipos navegaran en Internet a través de esta IP

Vpn

Para la formación de la VPN, se debe ver los protocolos y encriptaciones que se empleara para formarla, teniendo en cuenta las seguridades debidas para que la información que va a atravesar de Bogota a Quito o viceversa viaje completamente segura y nadie pueda corromper esta seguridad.

Regla General:

Pre-shared Key: adpertel07

Ike Proporsal:

Modo de negociación: MAIN
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time: 28800
Key Group: DH1

IPsec Proporsal:

Modo de encapsulación: Túnel
Protocolo Activo: ESP
Algoritmo de encriptación: 3DES
Algoritmo de autentificación: MD5
SA life time 28800
Perfect Forward Secrecy: DH1

CAPITULO IV

ANÁLISIS ECONÓMICO

4.1 Costos de equipos e instalación

Para el análisis económico se va a necesitar revisar todos los costos que van a intervenir, el costo de la inversión, que viene siendo el costo de los equipo y la instalación, el beneficio que se obtendrá es el ahorro en la planilla telefónica por ya no realizar llamadas internacionales. Y el gasto corriente que viene siendo el costo que vienen pagando por el consumo de Internet en las oficinas.

4.1.1 Costo de equipos e instalación

Para el costo de equipos tomamos los valores de los equipos que se vio anteriormente en las tablas de selección de equipos.

Tabla 4.1 Costo de equipos e instalación

Equipo	Valor unitario	Cantidad	Costo de equipos	Valor de instalación	Sumatoria
Router Zywall 2	$250	3	$750	$55	$805
MVP130	$336	2	$672	$200	$872
TOTAL					$1677

El valor total de la inversión será de $1950 dólares, valor se pretende recuperar en el plazo de un ano.

4.1.2 Gastos corrientes

Los costos que se vienen pagando por el servicio de Internet, y entran como gastos corrientes de cada mes son:

Tabla 4.2 Gastos corrientes

Gastos Mensuales	
Costo de Internet en UIO 320 Kbps	$45
Costo de Internet en BGT 600 Kbps	$46
Costo de Internet en BGT 128 Kbps	$20
Costo por IP pública ECU	$15
Costo por IP pública COL	$8
TOTAL	$134

Por lo que tienen un gasto corriente de 134 dólares mensuales.

4.1.3 Beneficios

El beneficio que obtendrán por la inversión realizada será el ahorro en el consumo de la línea convencional, es decir la línea de abonado de la PSTN, que se vera reflejada en la planilla telefónica sin llamadas internacionales y en el envío de archivos o documentos por valija a través de correspondencia o envíos por aeronave, ya que ahora la pueden compartir a través de la VPN.

Siendo así, se aprecia un cuadro con el ahorro que representara mensualmente tomando en cuanta que el consumo de teléfono es de 120 minutos diarios, que se desglosan en 90

minutos de Quito a Bogota y 30 minutos de Bogota a Quito. Y teniendo en cuenta los valores que cuesta el minuto de llamada internacional tanto en Ecuador como en Colombia.

Tabla 4.3 Beneficios económicos

	minutos	**costo**	**subtotal x día**	**días laborables**	**Total x mes**
De UIO a BGT	90	$0,16	$14,4		
de BGT a UIO	30	$0,12	$3,6		
			$18	$20	$360
Ahorro en envío de documentos					$20
TOTAL					$380

Todos estos valores, serán puestas en un flujo de caja y analizadas mediante formulas que miden que tan buena es una inversión, así saber si refleja un beneficio para la empresa esta adquisición para el lapso de un año.

4.2 Flujo de caja y obtención de costos de la inversión

Para al análisis se va a tomar los datos anteriormente descritos, poniendo que se tiene una tasa de inversión en el mercado del 9 % para un año. Con este porcentaje (i) se calculara el tir y el van para comprobar que la inversión es viable.

En resumen, tomando en cuanta los resultados obtenidos tanto en el TIR como en la VPN, se tiene los datos:

TIR = 9,84 %

VAN= 84,54

Y esto significa que, en el análisis para un año se va a obtener un VAN de 84,54, nos indica que ya se va a obtener una ganancia, en el lapso de un año por lo que el proyecto, si cumple las expectativas de ahorro en el consumo de la planilla telefónica principalmente. Además, se obtiene una tasa de oportunidad mayor que la se encuentra en el mercado 9,84 > 9 Por lo tanto, esto nos reafirma que el proyecto es rentable para la empresa.

El análisis se adjunta en anexo 2

CAPITULO V

IMPLEMENTACIÓN DEL PROYECTO

5.1 Configuración de routers

Ya basado en el análisis que se diseño anteriormente, se realiza el esquema de red Ardila por completo. Es decir con las ip que correspondes a cada equipo, con todos los equipos que intervienen en el escenario y este esquema sirve de guía para la implementación del proyecto.

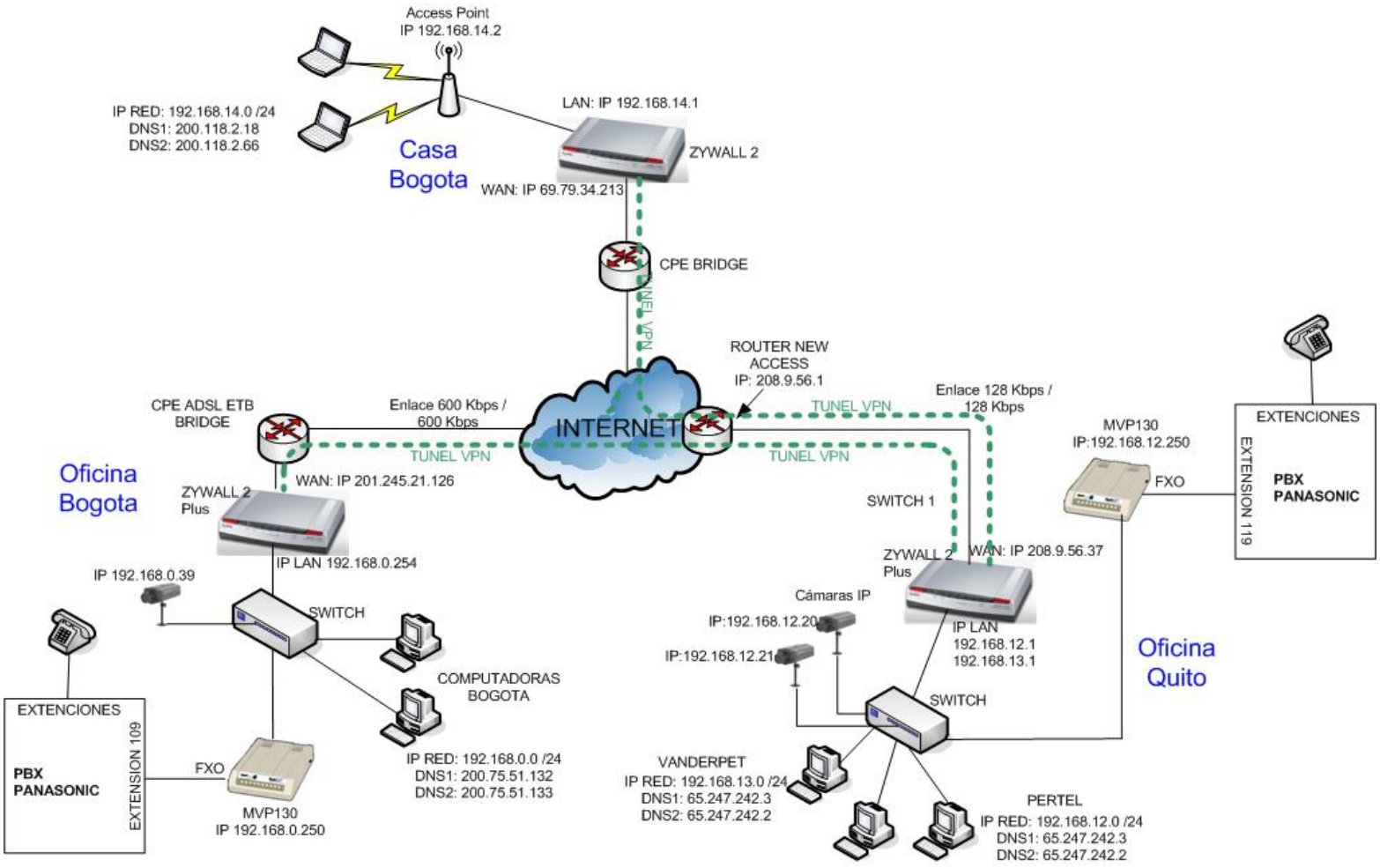


Figura 5.1. Esquema de red a implementarse

5.1.1 Configuración Zywall 2 Plus Oficina Quito

Versión del equipo y estado

Los routers zyxel se pueden actualizar con nuevos *firmwares*, donde van presentando algunos cambios que aumentan los *features* del equipo por lo que es importante verificar que el equipo quede con la última actualización.

Figura 5.2. Pantalla principal Zywall 2 UIO

Interfase LAN:

Para la configuración de la IP Lan corresponde a los parámetros definidos anteriormente, retirando las características como RIP y DHCP Server, que para este escenario no se lo va a emplear.

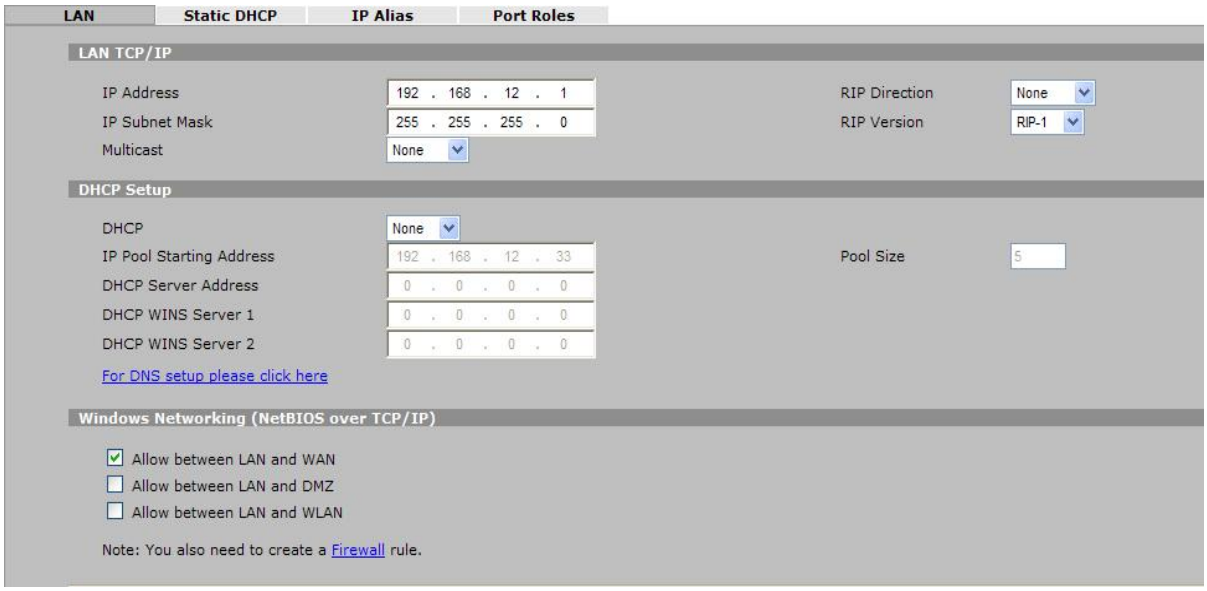


Figura 5.3. Interfase LAN del Zywall UIO

Ip Alias:

Se tienen dos redes la 192.168.12.0 para PERTEL y la 192.168.13.0 para VANDERPET por lo que se configura como IP alias a la red 2 simulando que el equipo posea dos ip para la parte lan o dos interfaces diferentes.

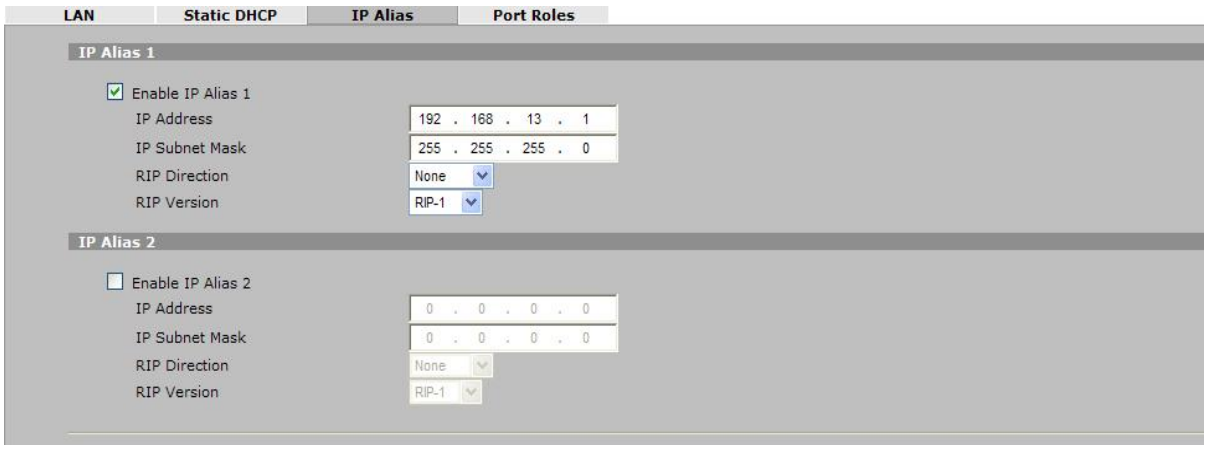


Figura 5.4. Interfase IP Alias zywall uio

Interfase WAN:

Se configura la IP que provee el ISP , indicando si el equipo va hacer NAT o trabajara como router puro, incluyendo características de enrutamiento dinámico como RIP.

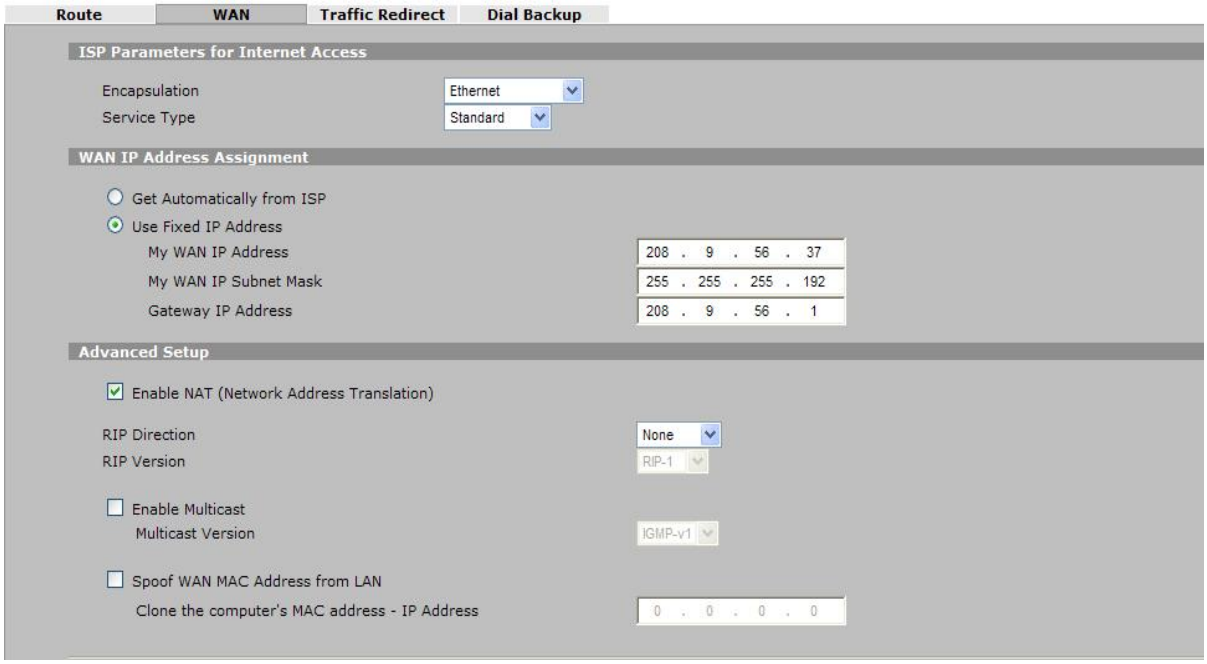


Figura 5.5. Interfase WAN del Zywall uio

Dns:

Se ingresa los DNS que maneja el proveerlo de Internet para que el equipo sirva como DNS Server y se puedan traducir los nombres por los dominios IP.

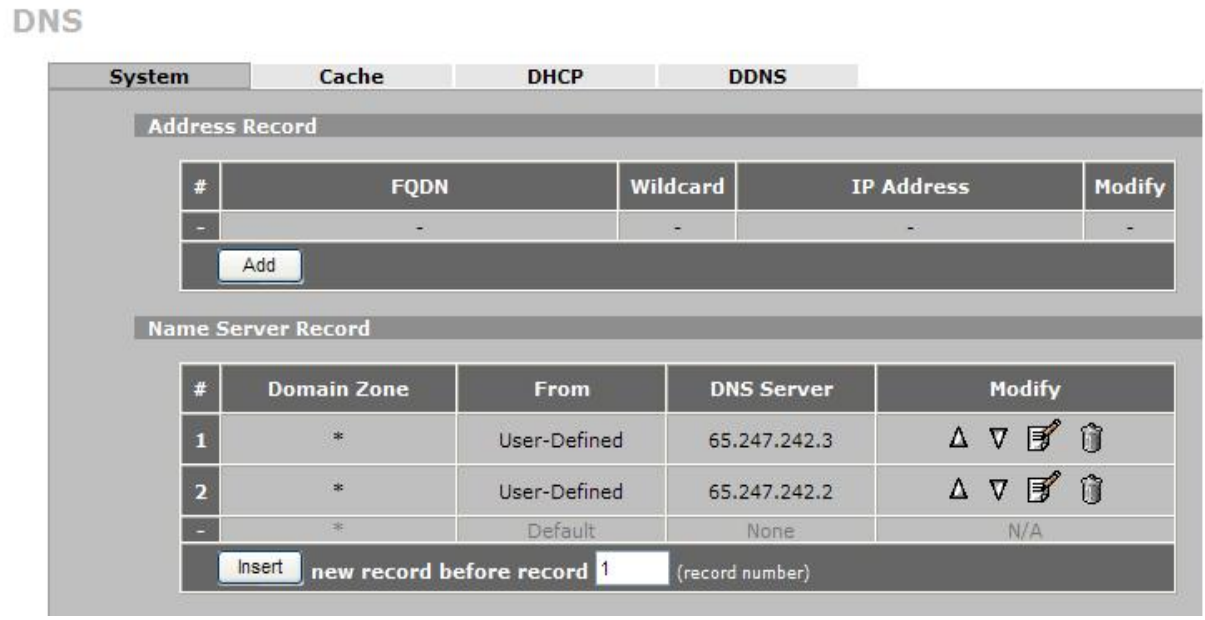


Figura 5.6. Pantalla de configuración DNS del Zywall

Firewall:

El firewall viene activado por defecto, con reglas generales como no permitir el paso de paquetes desde la WAN a la LAN por que se creara reglas especificas para habilitar los servicios requeridos.

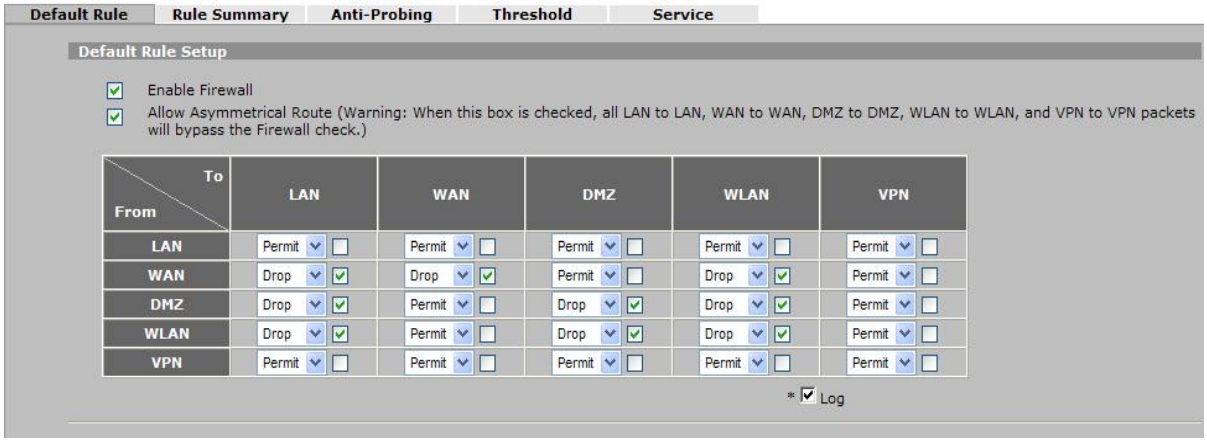


Figura 5.7. Interfaz del firewall del zywall 2 uio

Reglas para NAT:

Se crean dos reglas de Port Forwarding, para habilitar las dos cámaras IP en Quito, que puedan ser vistas desde el Internet con los puertos 80 y 81. A parte de hacer esta regla lógica hay que permitir esta acción dentro del firewall.

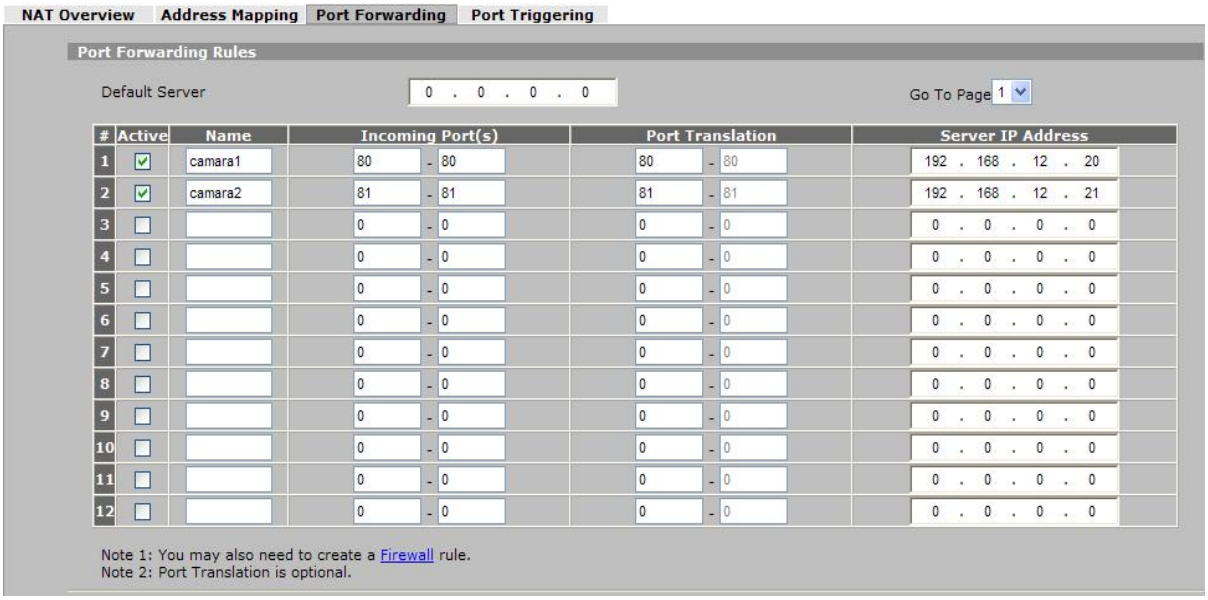


Figura 5.8. Reglas de Port Forwarding

Regla de Firewall para el DNAT:

Dentro del rule summary (reglas especificas del firewall), se selecciona la dirección del paquete, para el caso de las cámaras es de Wan a Lan, y aquí se crean las dos reglas para permitir el ingreso de cualquier usuario desde el Internet con puerto 80 y 81 a las cámaras IP.

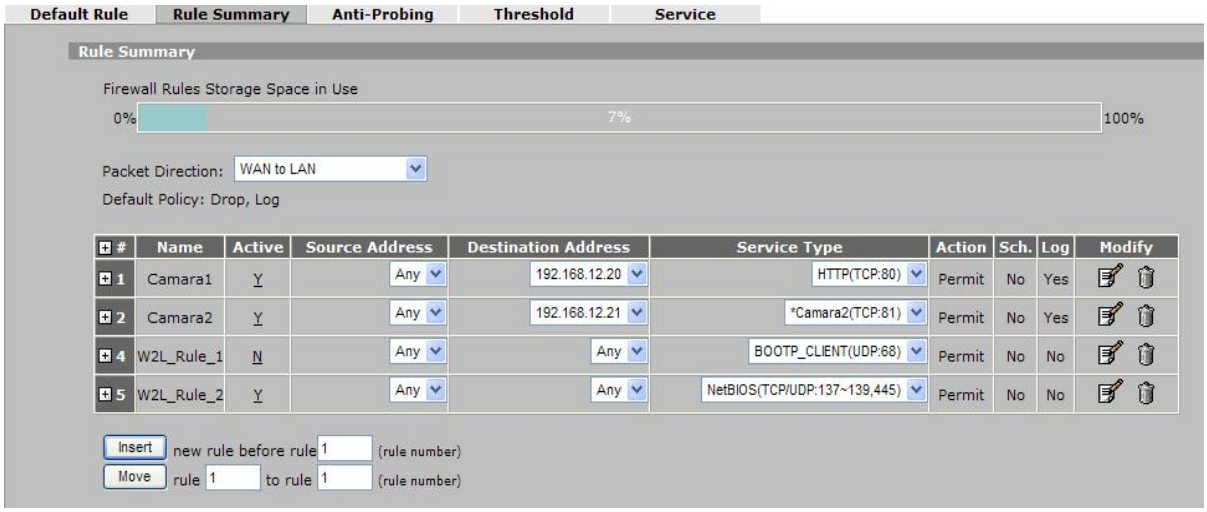


Figura 5.9. Reglas de Firewall para las cámaras

Administración remota:

Se da permisos de acceso remoto al equipo para poder administrarlo desde Internet mediante Https puerto 444, Telnet puerto 23 desde el Internet, y desde la parte lan con http en el puerto 90 por lo que una de las cámaras esta trabajando con el puerto 80 y habría problemas de conflicto de puerto entre los equipos. Al igual que las reglas de port forwarding para que están reglas puedan pasar se necesita crear una regla en el firewall que permita el acceso.

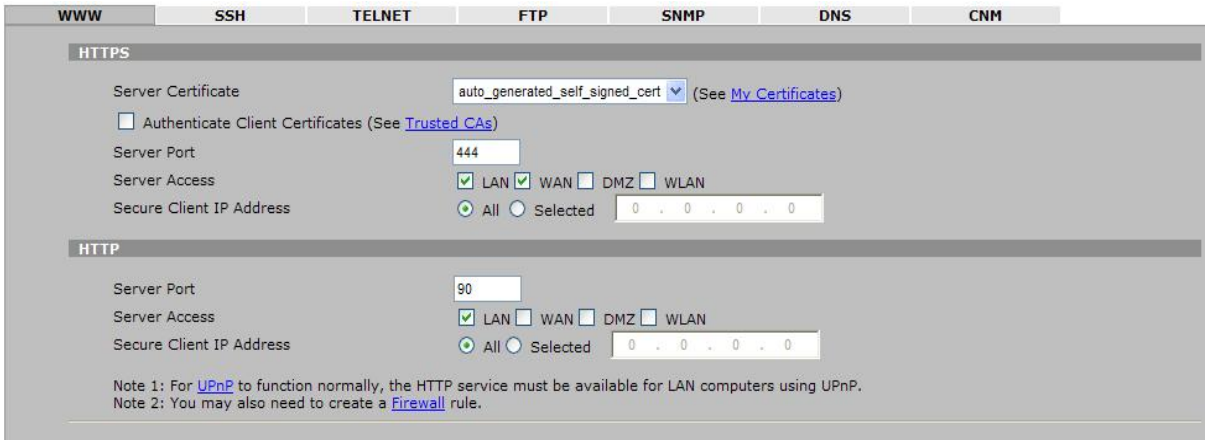


Figura 5.10. Reglas de acceso remoto al zywall uio

Regla de Firewall para la administración remota:

La dirección de las paquetes para la configuración remota del equipo es de Wan a Wan, mediante puerto https 444, así como, puerto 23 para telnet, y también se crea reglas para que pueda responder el equipo al ping hecho desde Internet.

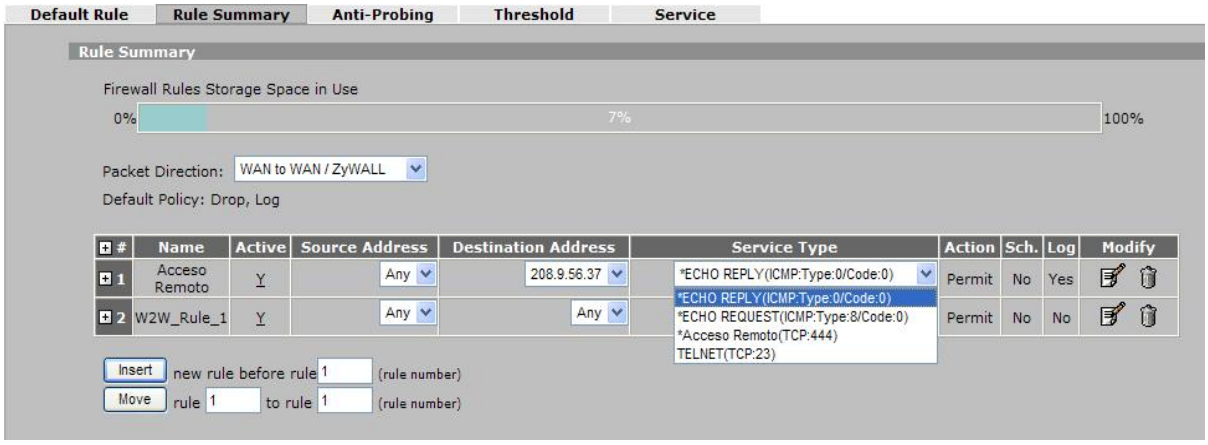


Figura 5.11. Regla de firewall para acceso remoto

Administración de ancho de banda:

Se segmenta ancho de banda del canal de comunicaciones para garantizar la calidad de telefonía IP y priorizarlo sobre los datos. Primero se crea una regla general entendiendo que WAN es todo trafico saliente es decir UPLOAD y LAN en es todo trafico de descarga DOWNLOAD. Aquí se restringe el ancho de banda a lo contratado por el proveedor, y activando la regla.

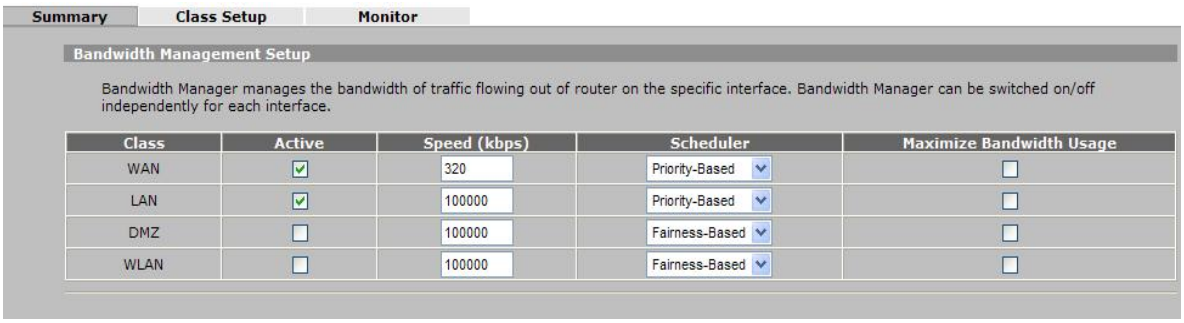


Figura 5.12. Regla general administración de ancho de banda

Reglas de filtrado ancho de banda Interfase LAN:

Dentro del Class Setup se crean las reglas específicas para cada servicio o para cada grupo de IP dependiendo como se desea hacer el control.

Para este caso se crean 3 reglas Vpn, VoIP e Internet, sumados los 3 dan 220 Kbps que es lo que tienen contratado en UIO. Cada servicio se maneja a través de prioridades siendo 7 el que posea mayor prioridad. Y se puede manejar la característica de borrow, que es la posibilidad que ese servicio puedo tomar prestado el ancho de banda de los servicios semejantes en caso de que este libre el canal.

Las clases se manejan a través de las IP de destino y las IP de fuente, igualmente recordando que LAN es download y WAN es upload.

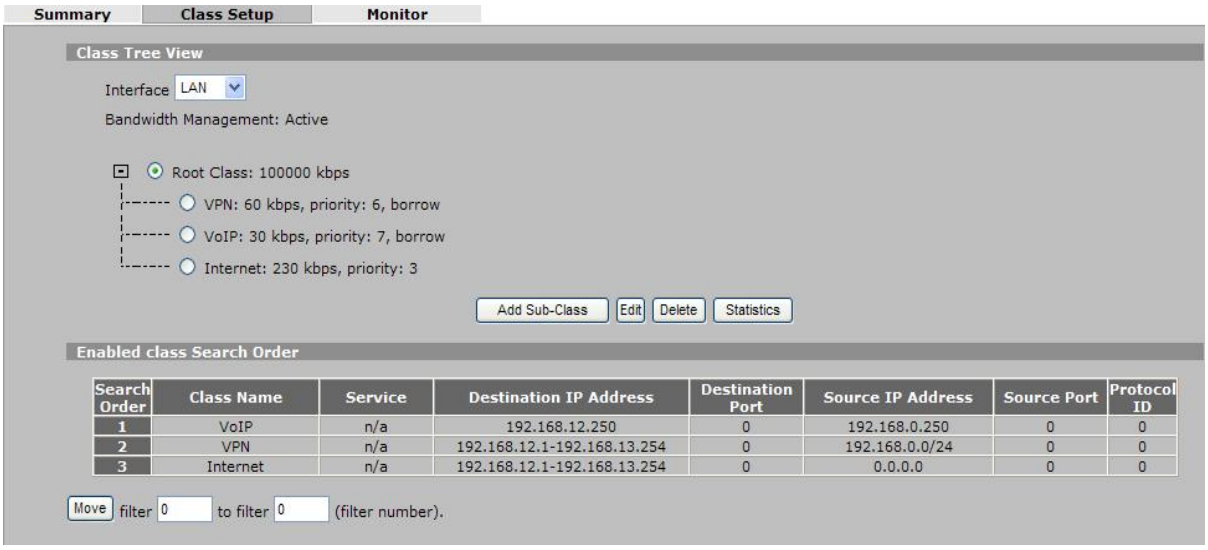


Figura 5.13. Configuración de servicios de BW LAN

Reglas de filtrado ancho de banda Interfase WAN:

Igual que la regla anterior pero la fuente y destino cambiado.

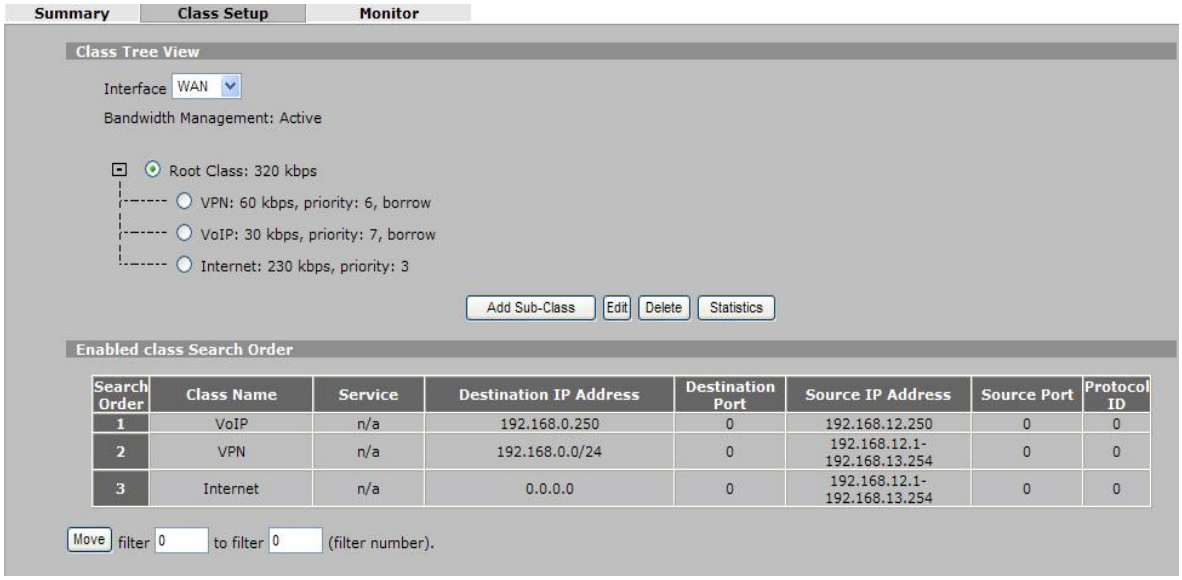


Figura 5.14. Configuración de servicios de BW WAN

Enlaces VPN:

Se establecen dos reglas: 1) VPN Quito- Bogota Oficinas, y
2) VPN Quito- Casa Bogota.

La formación de las VPN es de forma independiente tomando en cuenta las redes que van a formar la VPN tanto local como remota y las seguridades que se va a dar a las mismas, que ya fueron indicadas anteriormente.

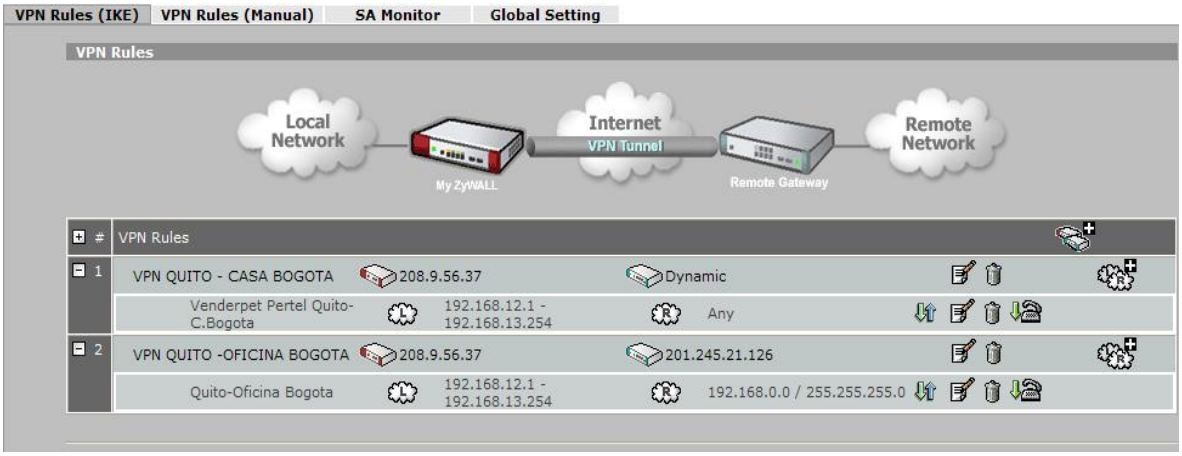


Figura 5.15. Formación de 2 VPN

Reglas VPN Quito – Bogota Oficinas:

Como regla general de la vpn, se debe ingresar la IP publica local (del equipo) y la IP publica remota (Equipo remoto), cuando es una VPN fija. La clave que va a validarse en ambos equipos en este caso ardila2007, luego las reglas de encriptación.

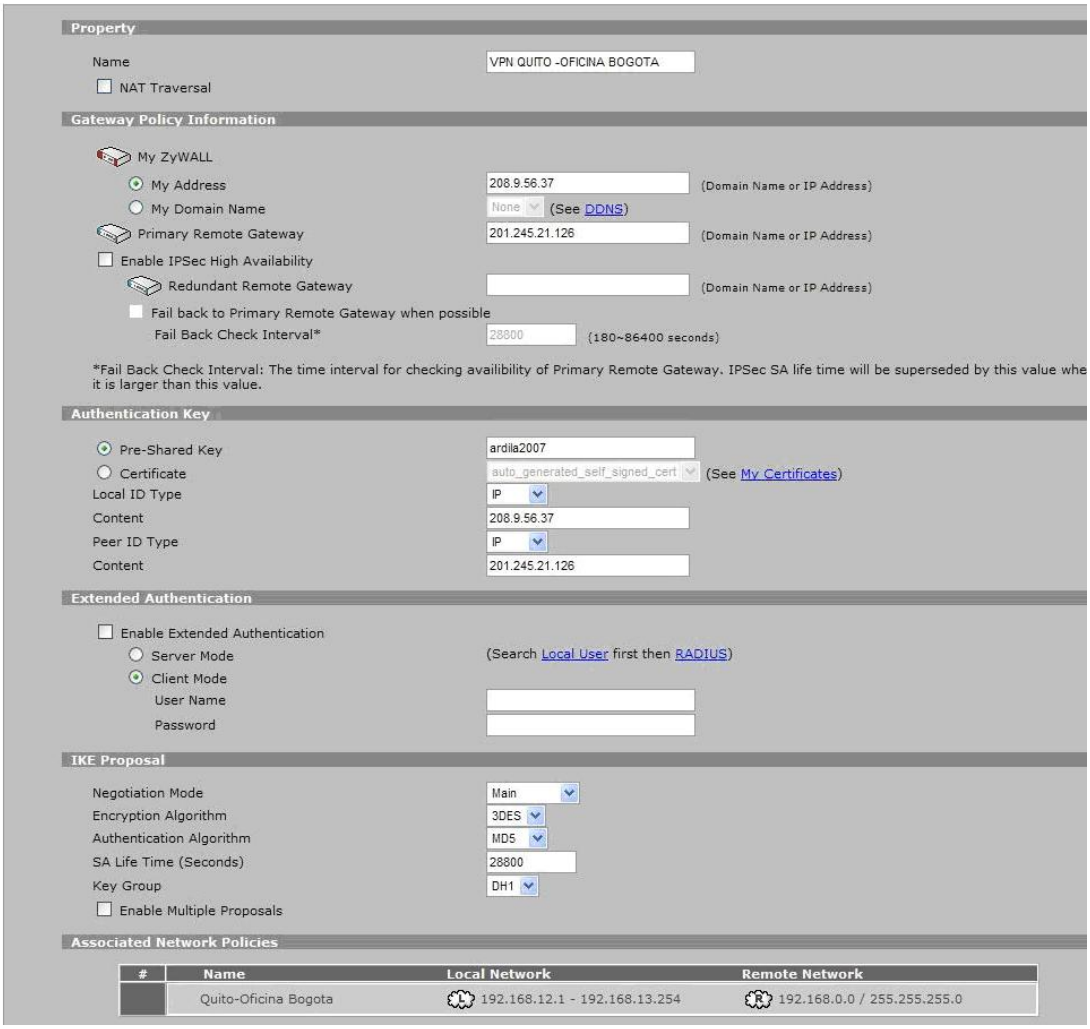


Figura 5.16. Regla General VPN Oficina UIO - BGT

Dentro de la regla especifica se colocan las redes privadas de ambas oficinas que van a compartir información en la VPN, así mismo las reglas de encriptación para la fase de intercambio de información.

Aquí también hay que colocar un visto en la casilla de *Nailed-up* que es para que este equipo sea el que comience la negociación, es decir, es el equipo que arranca el proceso de negociación para formación de la vpn. Y en la casilla *Active*, para que este activa esta regla.

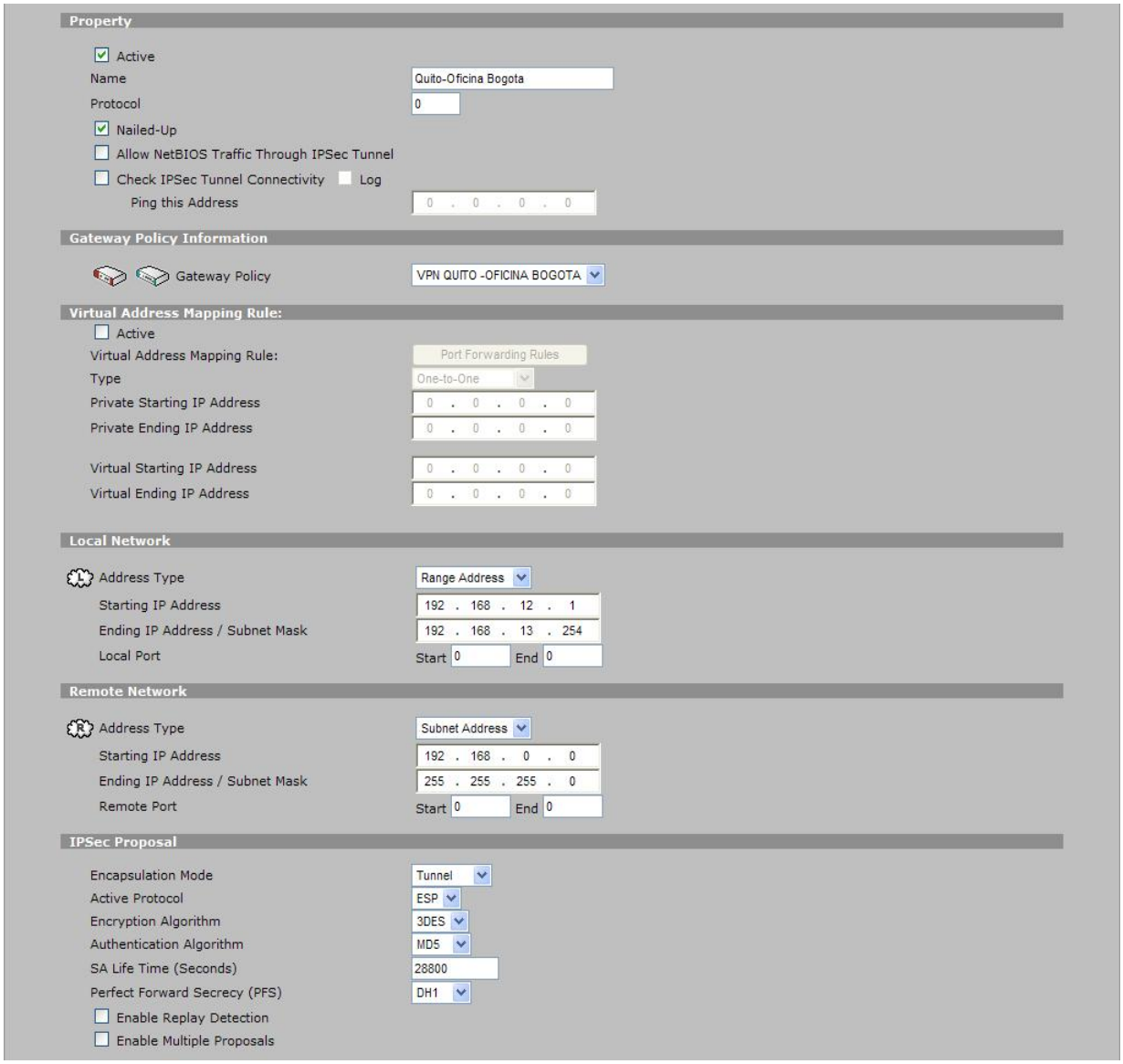


Figura 5.17. Regla especifica VPN oficina uio - bgt

Reglas VPN Quito – Casa Bogota:

Para esta regla se esta implementando una VPN dinámica, es decir donde no importa la IP que tenga el lado remoto si cumple con las reglas de seguridad así como con la clave de seguridad se puede formar la VPN. La ip para hacerla dinámica debe ser 0.0.0.0

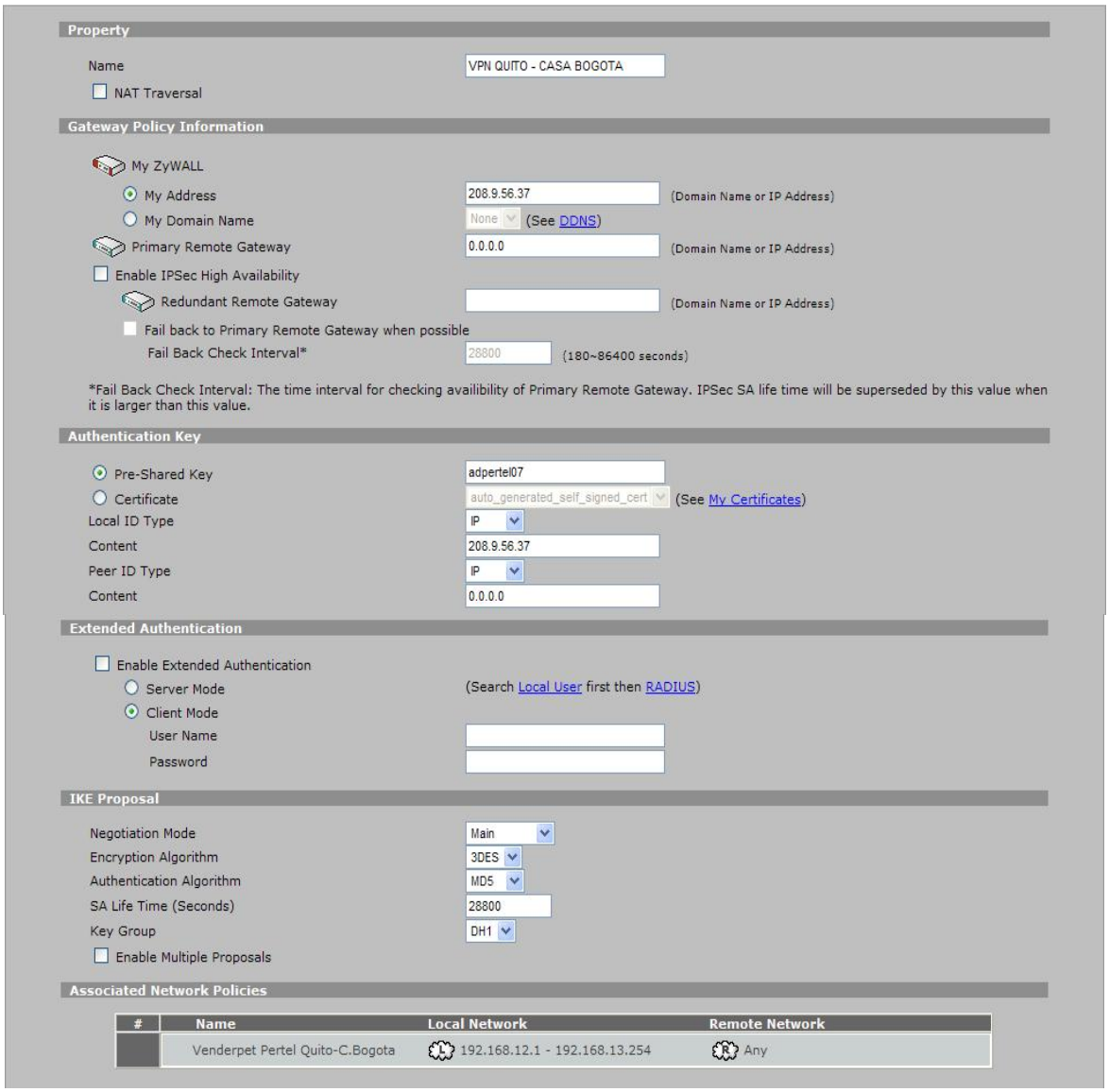


Figura 5.18. Regla General VPN UIO – casa BGT

Para la regla especifica como ip de red que va a formar la vpn es 0.0.0.0 con mascara 0.0.0.0 esto indica igualmente que le red privada del equipo remoto como no se conoce las ip que formaran la vpn, se pude conectar cualquier red o pc a la vpn, cumpliendo con las reglas de encriptación, y tomando en cuenta que en equipo remoto se notifica que ip serán parte de la vpn.

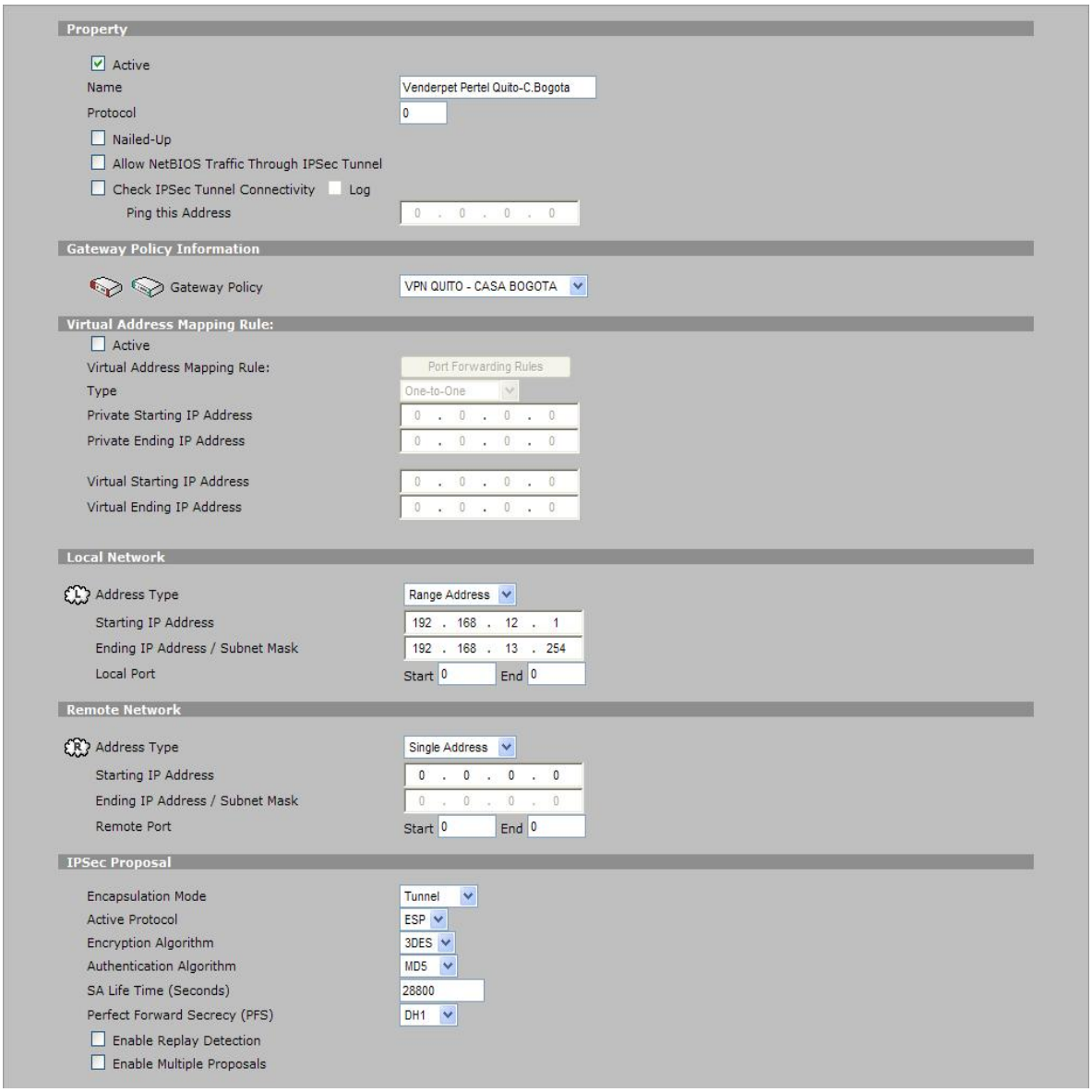


Figura 5.19. Regla especifica VPN UIO – casa Ardila

5.1.2 Configuración Zywall 2 Plus Oficina Bogotá:

Las características del equipo son las mismas que el instalado en UIO por lo que la configuración será casi parecida a la del equipo en Quito con algunas pequeñas diferencias que se describirán.

Clave de acceso: adardila07

Versión del equipo y estatus:

Figura 5.20. Pagina Home de Zywall de Bogota

Interfase Lan:

La red de las oficinas de bogota es la 192.168.0.0 con mascara de 24 bits, y aquí se pondrá la ip para el equipo que es la 192.168.0.254

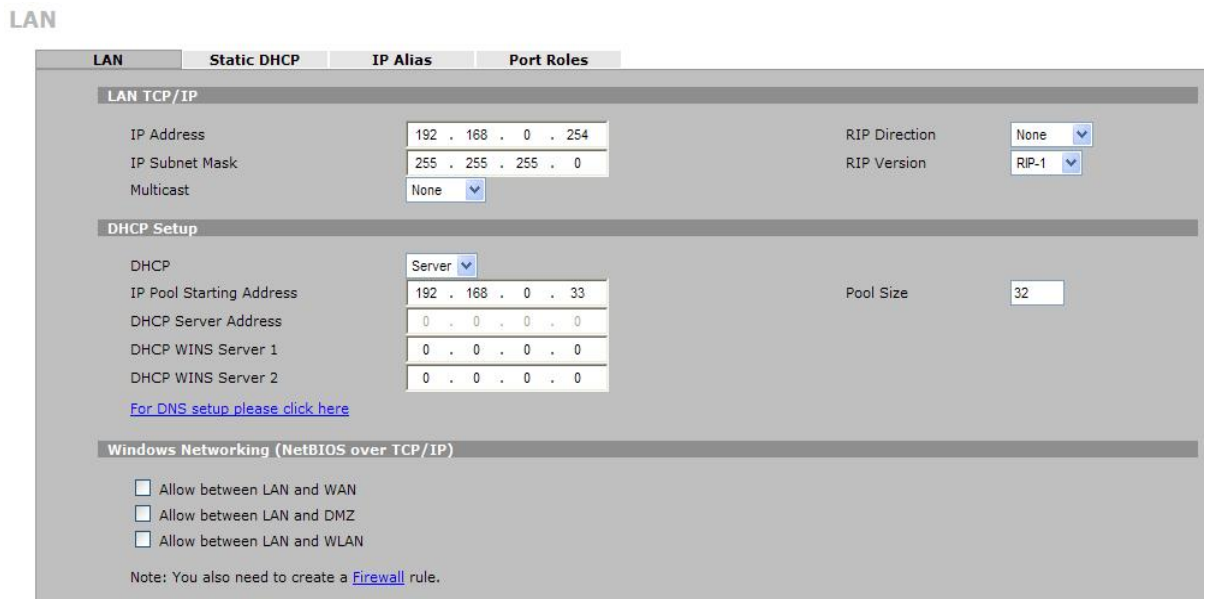


Figura 5.21. Interfase LAN Zywall BGT

Dhcp estático

Se configura al equipo como Server DCHP para que las maquinas en Bogota adquieran la dirección IP automáticamente según la siguiente lista:

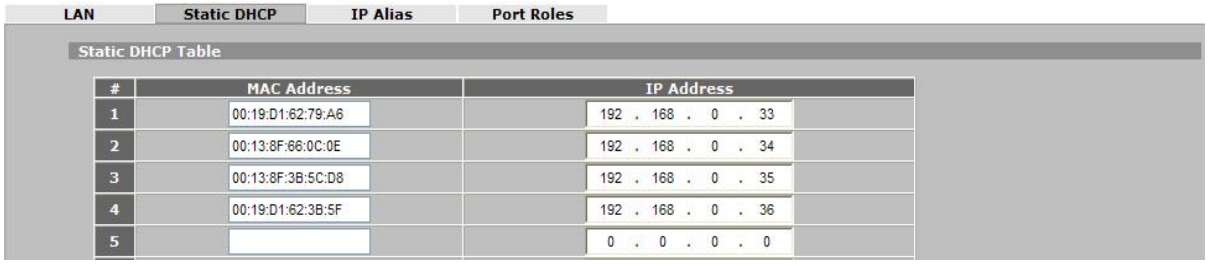


Figura 5.22. DHCP estático zywall BGT

Interfase Wan:

Se configura la IP publica fija que asigno el proveedor de Internet, con la característica de NAT para que ningún equipo atrás sea vista desde el exterior, y quitando la característica de rip porque no entrara a enrutar ninguna red.

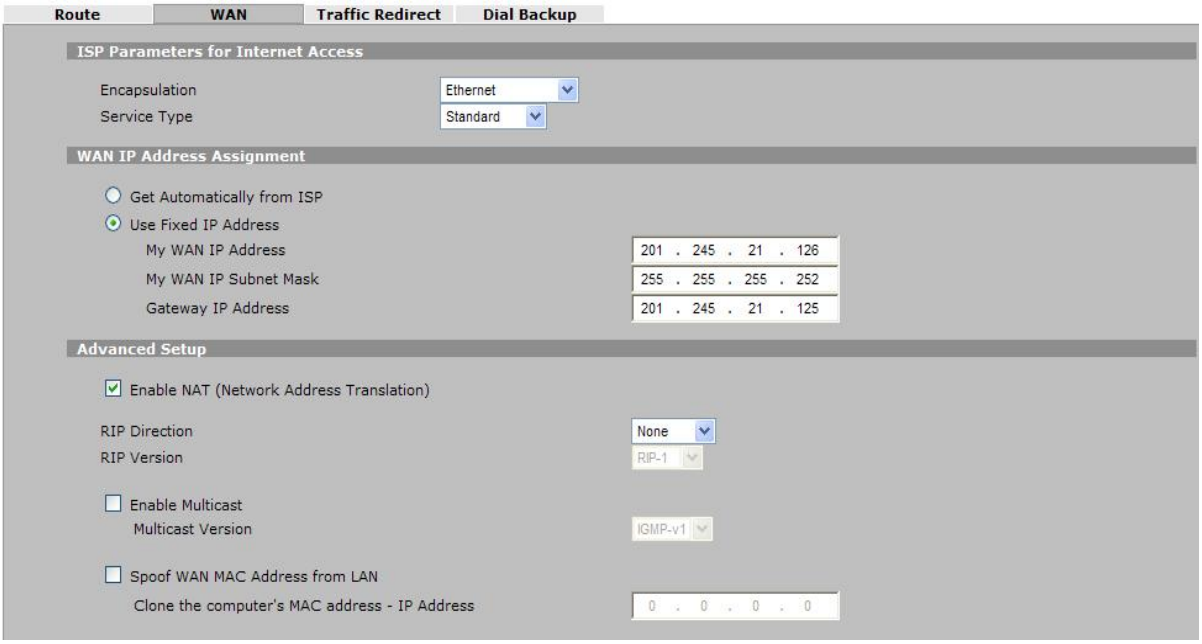


Figura 5.23. Interfase WAN Zywall BGT

Dns

Las ip que da el proveedor como servidor dns se ingresa en el equipo para que este sea un servidor dns para las computadoras de la Lan

Firewall

El firewall tiene que estar activado para evitar posibles intrusos dentro de la red privada. Va activada con las reglas por defecto.

Reglas de Dnat:

Se crea reglas de DNAT para acceder en Bogota Oficinas a una cámara IP y a la administración del equipo de VoIP. Esta regla de administración del equipo de Voz es para poder verificar el buen funcionamiento del mismo, ya que al encontrase en Colombia no es posible ir a verificar la configuración en caso de algún problema.

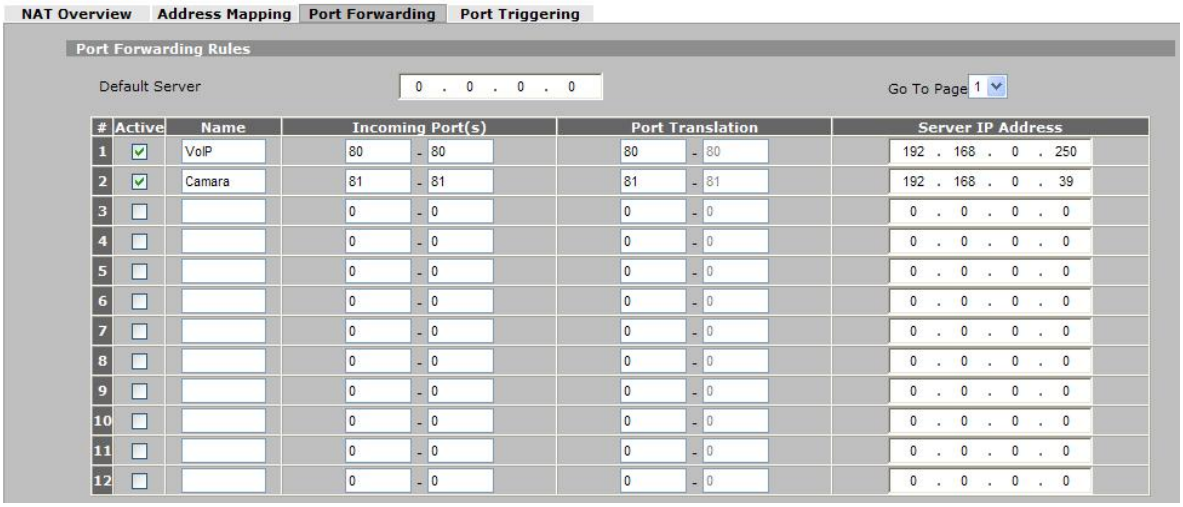


Figura 5.24. Reglas de DNAT Zywal BGT

Regla de DNAT en Firewall:

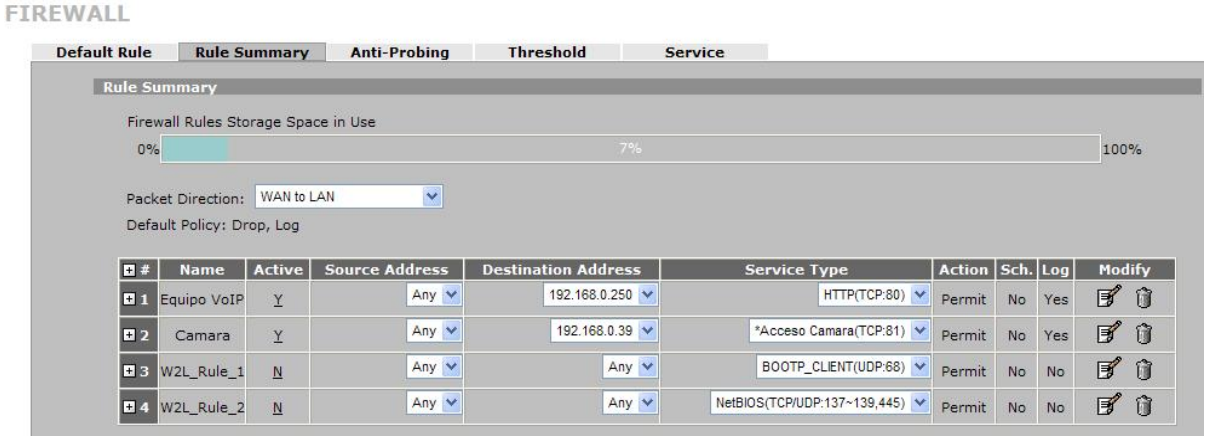


Figura 5.25. Regla de Firewall para la cámara y el equipo VoIP Oficinas BGT

Administración remota

Se configuro el acceso al equipo desde Internet mediante protocolo Https pero por puerto 444 y TELNET puerto 23.

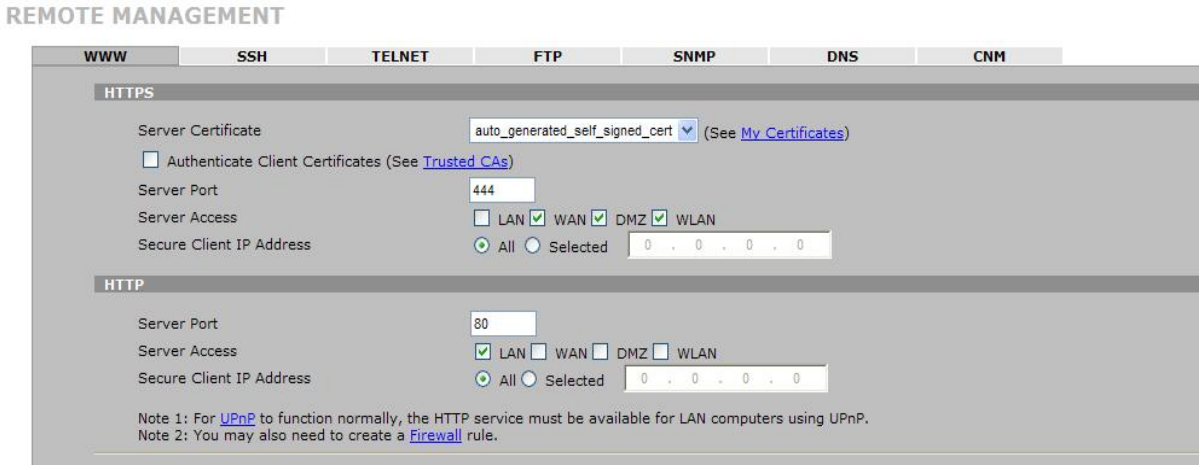


Figura 5.26. Administración remota zywall BGT

Regla de Firewall acceso remoto

Regla de wan a wan permitiendo que se acceda al equipo por puerto 444 por telnet y que responda al ping.

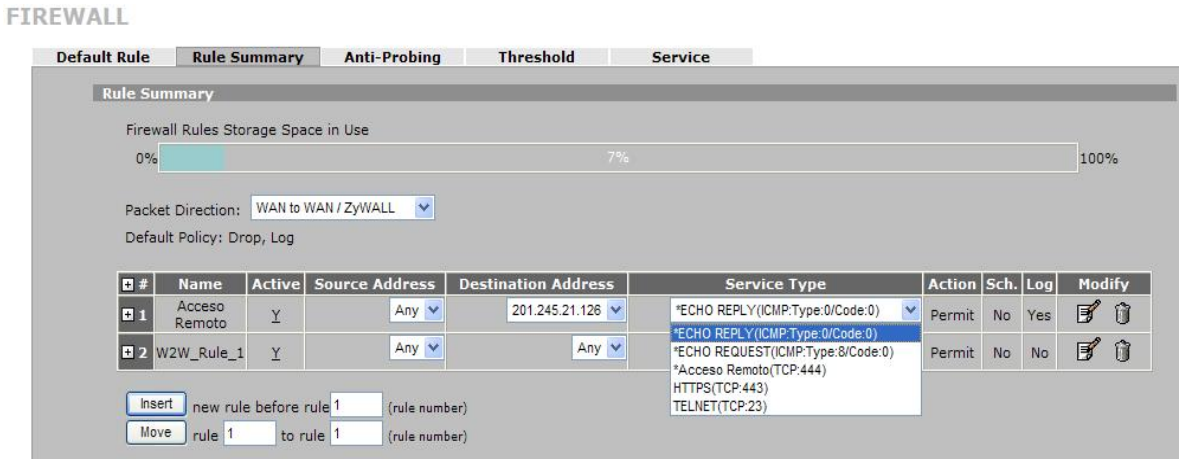


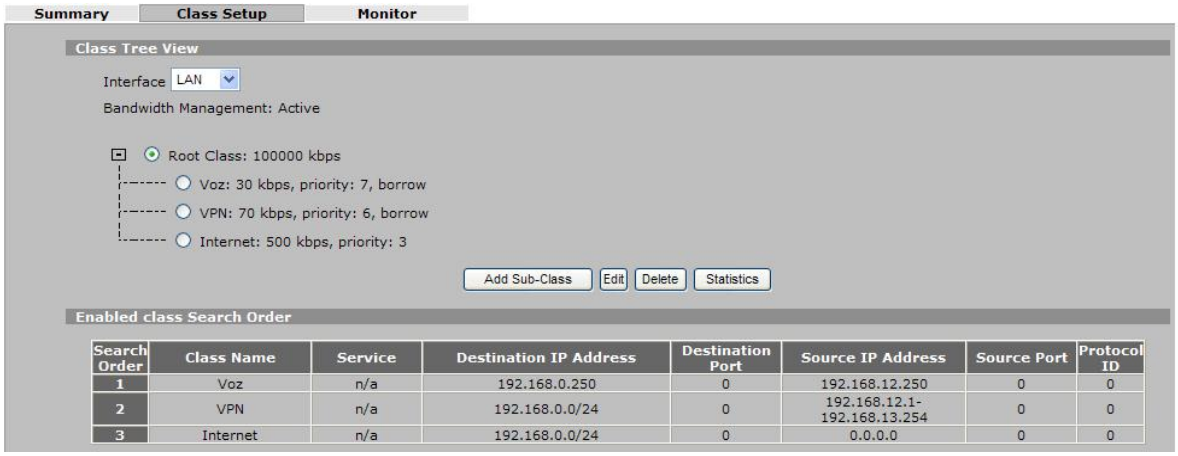
Figura 5.27. Regla de firewall para administración remota Zywall BGT

Administración de ancho de banda

Se segmenta ancho de banda del canal de comunicaciones para garantizar la calidad de telefonía IP y priorizarlo sobre los datos. En la regla general se configura la restricción de ancho es decir el ancho de banda contratado al ISP. Para este caso son 600 Kbps.

Reglas de filtrado ancho de banda Interfase LAN, esta es la regla de download, es decir las de descargar y mas importantes ya que aquí es donde llegan a inundar el canal de comunicación. Para la creación de esta regla se mameja a traves de las ip de fuente y las ip de destinatario. Siendo el Internet la ip 0.0.0.0 ya que esta representa cualquier ip. Y tomando en cuenta el ancho de banda asignada para cada servicio, asi como la prioridad que se quiera dar, en este caso especifico se da prioridad a la voz sobre ip.

Aquí también se tiene la opción de *borrow* que es que tome prestado el ancho de banda de las clases del mismo nivel en caso de que estas estén desocupadas.



Search Order	Class Name	Service	Destination IP Address	Destination Port	Source IP Address	Source Port	Protocol ID
1	Voz	n/a	192.168.0.250	0	192.168.12.250	0	0
2	VPN	n/a	192.168.0.0/24	0	192.168.12.1-192.168.13.254	0	0
3	Internet	n/a	192.168.0.0/24	0	0.0.0.0	0	0

Figura 5.28. Administración de BW LAN

Reglas de filtrado ancho de banda Interfase WAN. Son las mismas reglas de download pero para upload, por lo que fuente y destinatario se veran cambiadas.

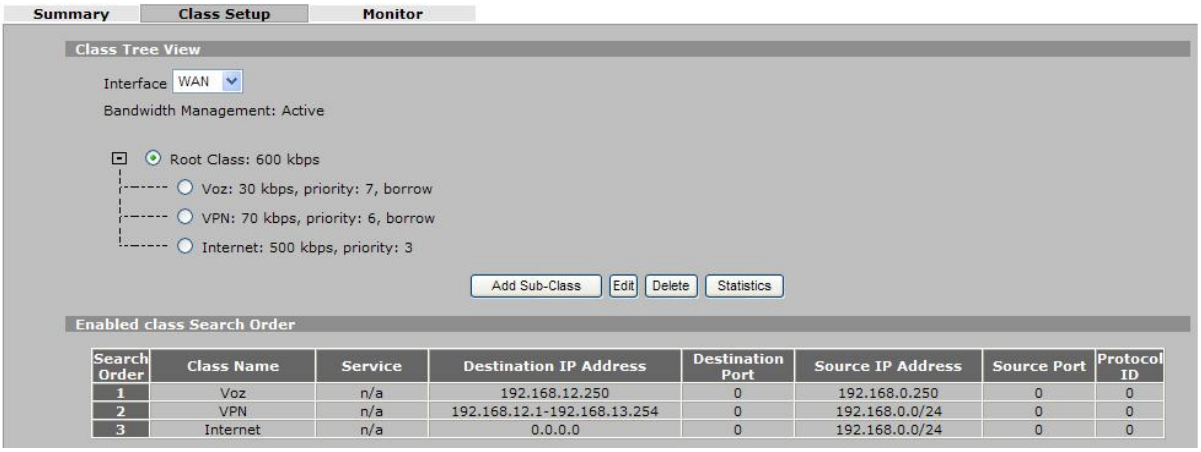


Figura 5.29. Administración de BW WAN

Enlace VPN

Se crea la regla correspondiente de Bogota Oficinas un túnel hacia Oficinas Quito.

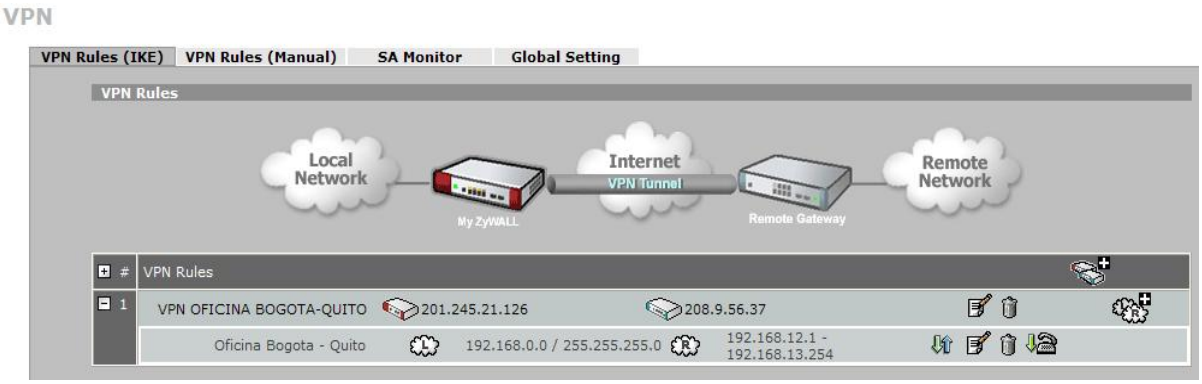


Figura 5.30. VPN entre oficinas BGT y UIO

Reglas de VPN Oficinas Bogotá – Quito, se configura la vpn con las IP's publicas, la clave que se intercambiara para creación del túnel y las encriptaciones que se van a dar a esta clave para que no sea descifrable para que los hackers no puedan obtener información importante de la empresa.

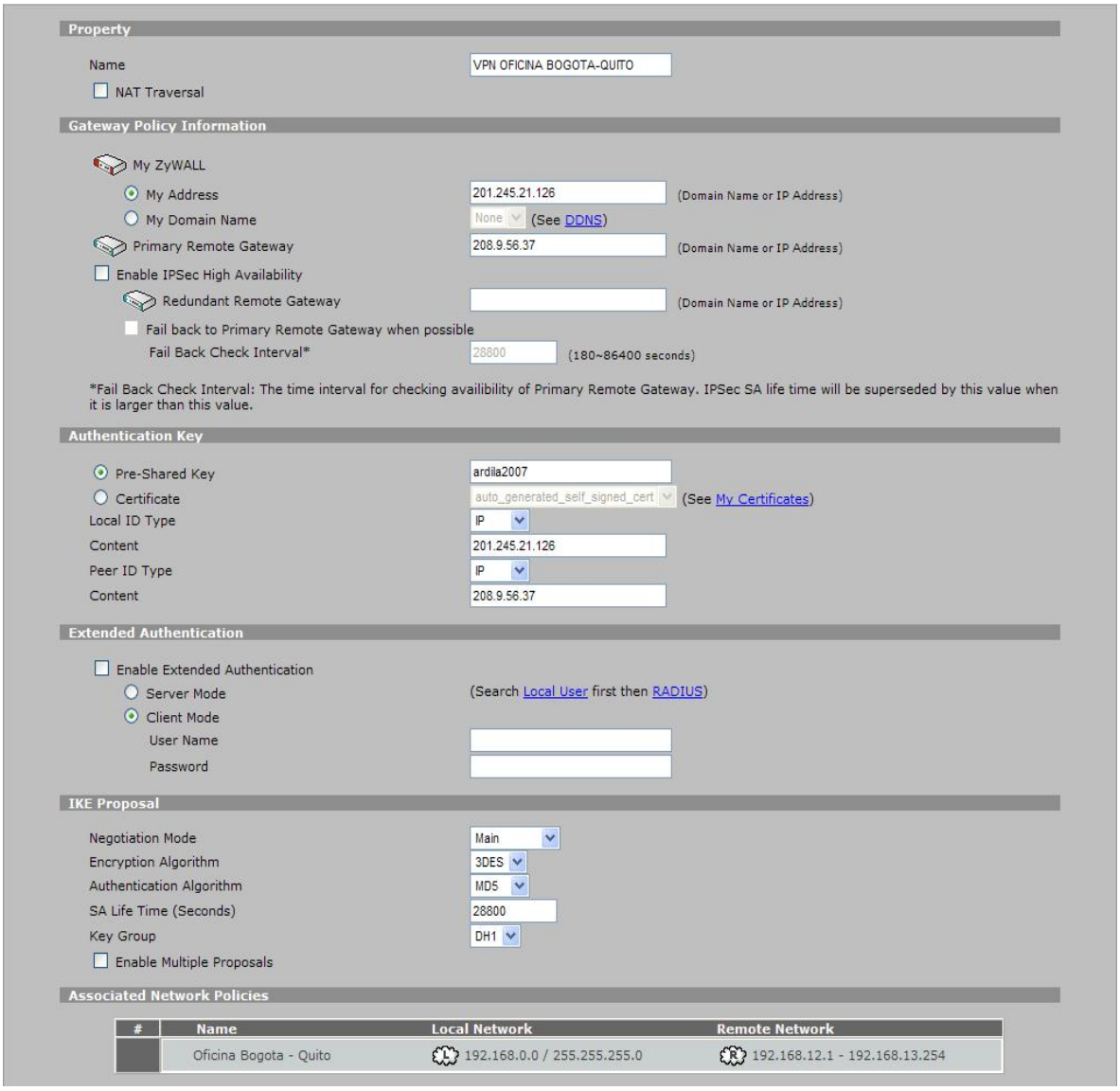


Figura 5.31. Regla general VPN de Oficinas BGT a UIO

Para la regla específica intervienen las redes privadas de cada oficina, y la forma de encriptación como va a viajar la información a través de la Internet, es preferible tomar encriptaciones fuertes para que no se pueda descifrar la información que viaja a través de la VPN.

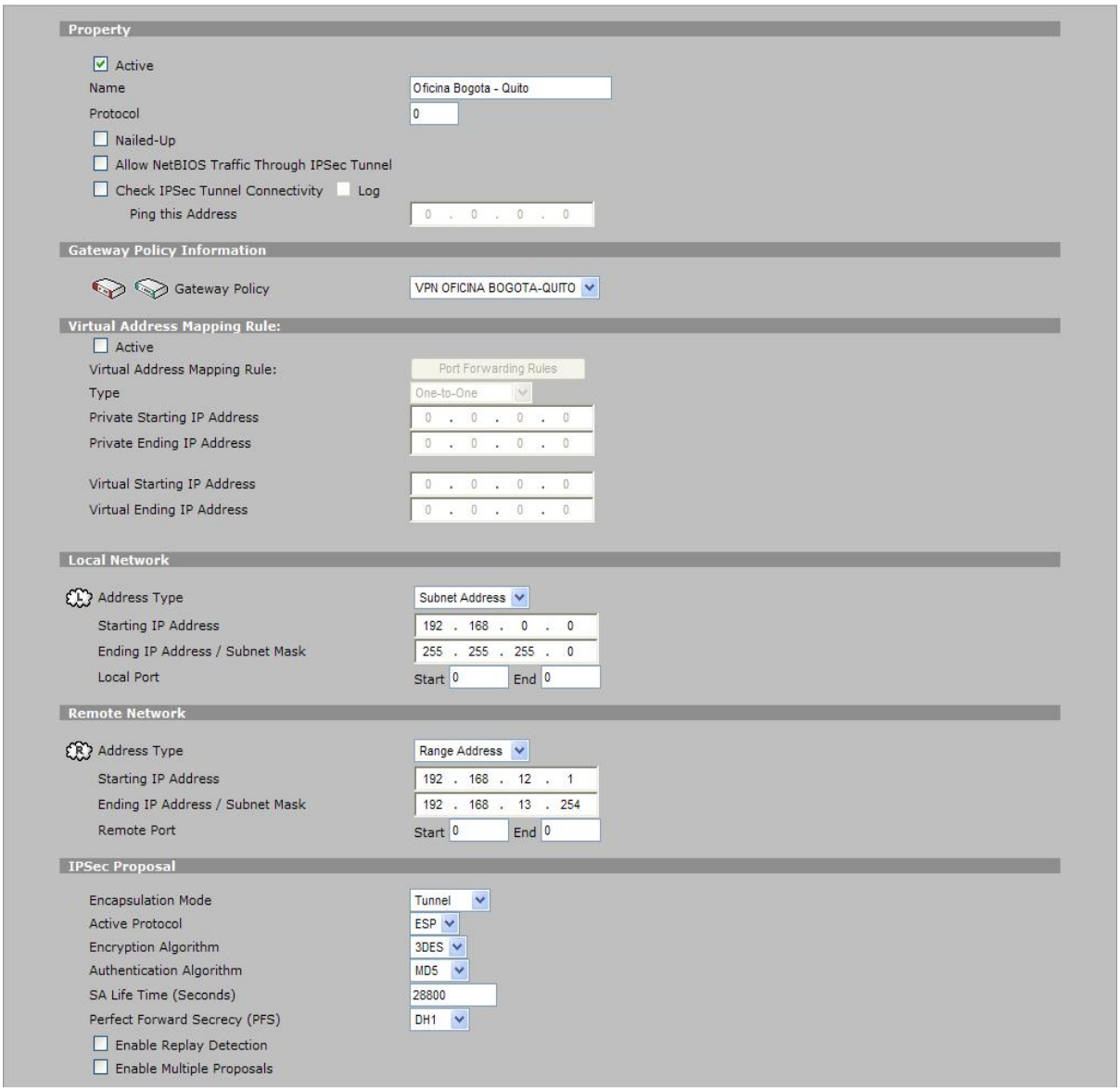


Figura 5.32. Regla especifica de VPN BGT a UIO

5.1.3 Configuración Zywall 2 Casa Bogotá:

Clave de acceso: adardila07

Versión y Estado:

Se puede visualizar el firmware del equipo para comprobar si no existe uno nuevo para este equipo y a su ves ver la ip wan y lan del equipo con la que esta trabajando el equipo.

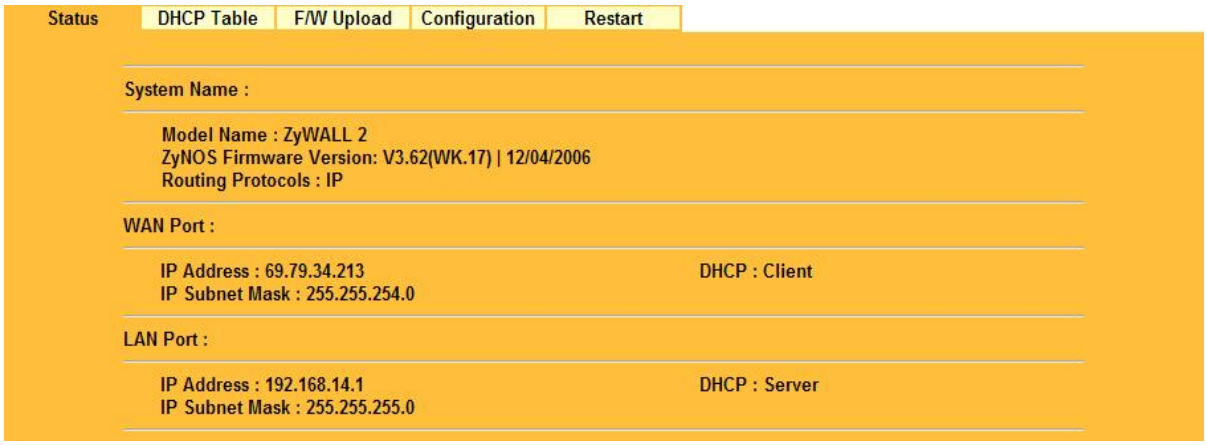


Figura 5.33. Estado de zywall casa Ardila

Interfase LAN:

Se configura la ip con la que va a trabajar el equipo y si se desea que el equipo sea un DHCP Server para las pc que se conecten a través de este equipo.

Igualmente se selecciona si se desee que trabaje como router puro activando RIP pero al hacer NAT no necesitamos esta opción por lo que se la deshabilita.

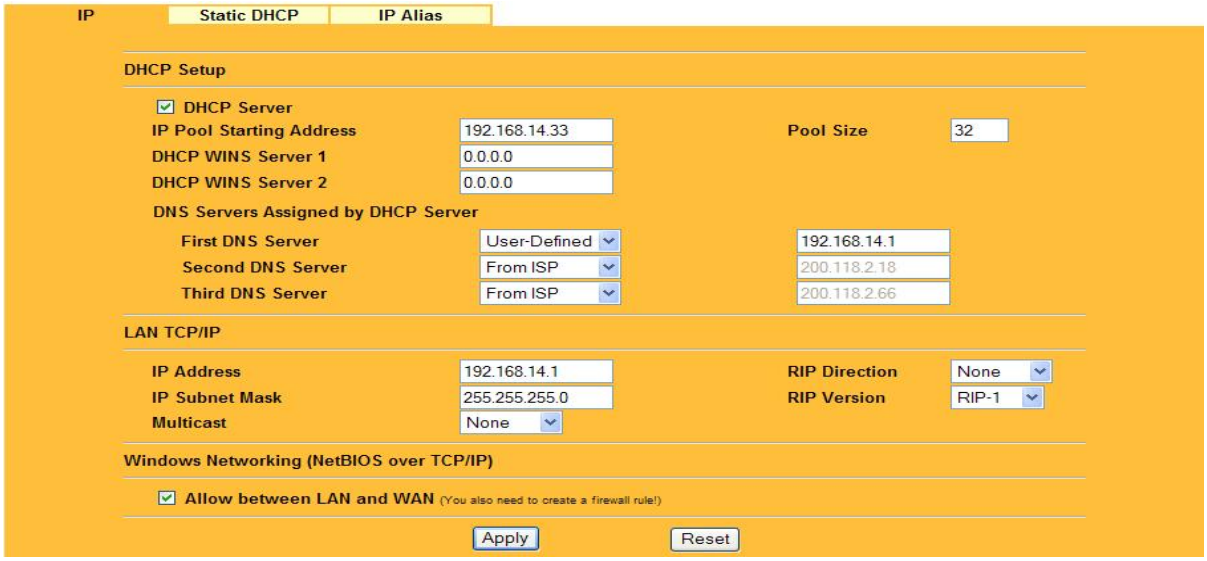


Figura 5.34. Interfase LAN zywall casa Ardila

Interfase WAN:

Para la interfase wan se configura para que obtenga automáticamente la ip del ISP, ya que en este punto no se contrato una IP publica fija, entonces la ip se entrega dinámicamente por lo que cambian cada cierto tiempo. También se selecciona que el router trabaje como router puro con NAT o con Multiple NAT.

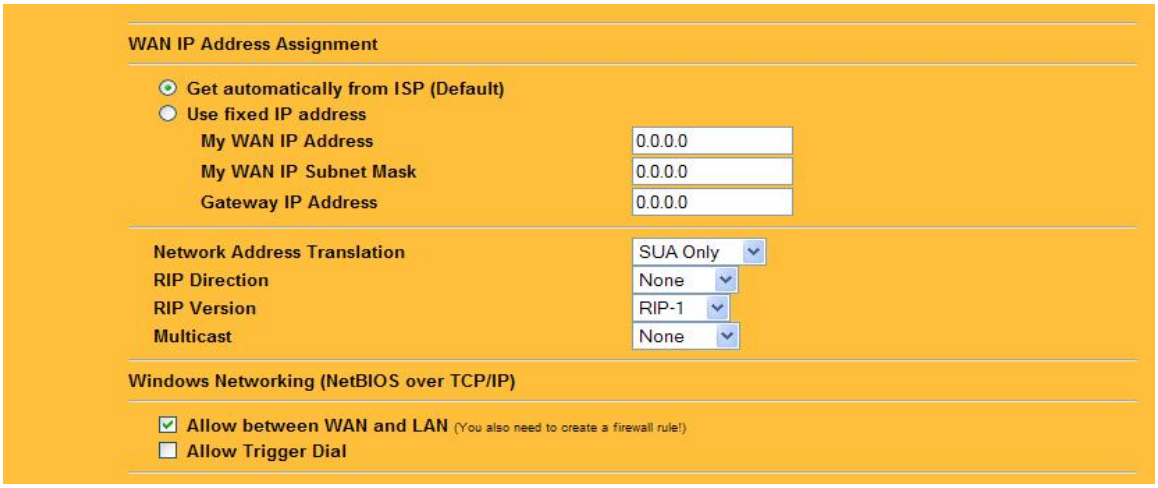


Figura 5.35. Interfase WAN zywall casa Ardila

Firewall

El firewall se activa para evitar intrusos en la red privada y se crearan las reglas específicas para la administración remota del equipo.

Administración remota

Se accede al equipo desde Internet a través de https:444 y Telnet:23

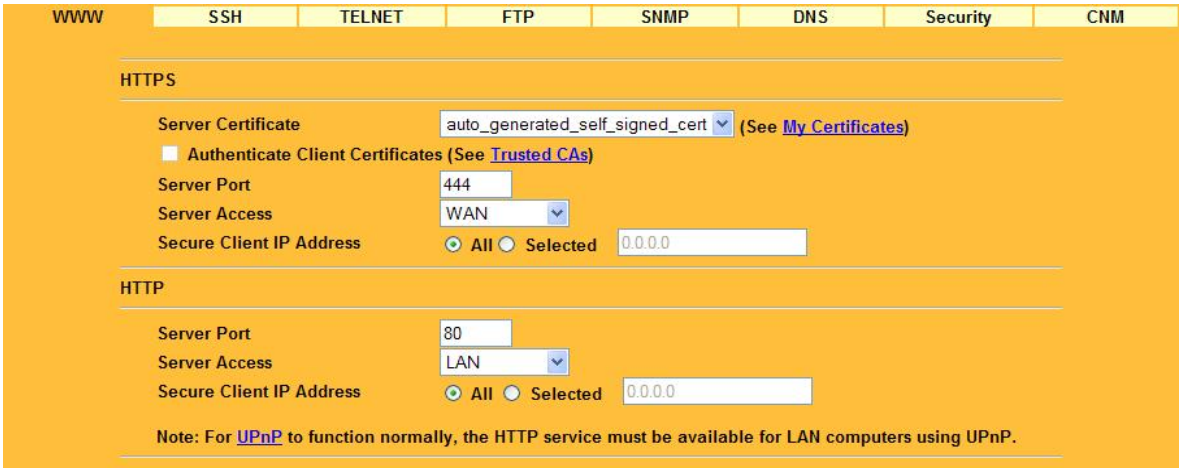


Figura 5.36. Administración remota del zywall casa Ardila

Enlace VPN

Se establece desde Casa Bogotá un túnel hacia Oficinas Quito.

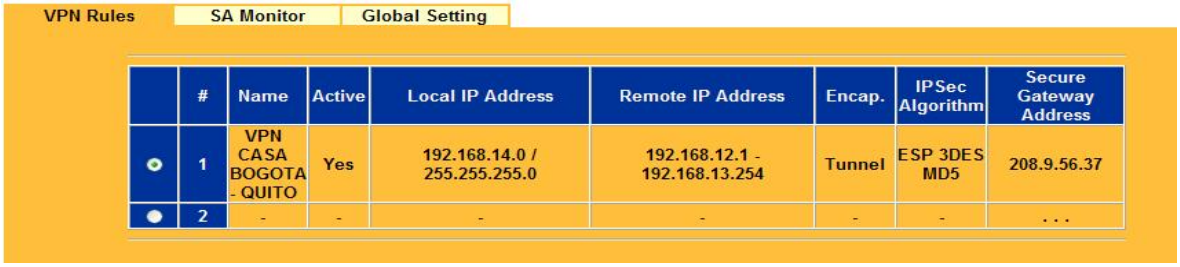


Figura 5.37. Regla de VPN en zywall casa Ardila

Regla general de VPN Casa Bogotá a Oficinas Quito. Este equipo se va a enganchar con el equipo de las oficinas de Quito mediante una regla dinámica, es por esto que como IP del router se debe poner 0.0.0.0 esto significa que puede tomar cualquier ip que este en el puerto wan del equipo. El resto de encriptaciones y claves se configura normalmente.

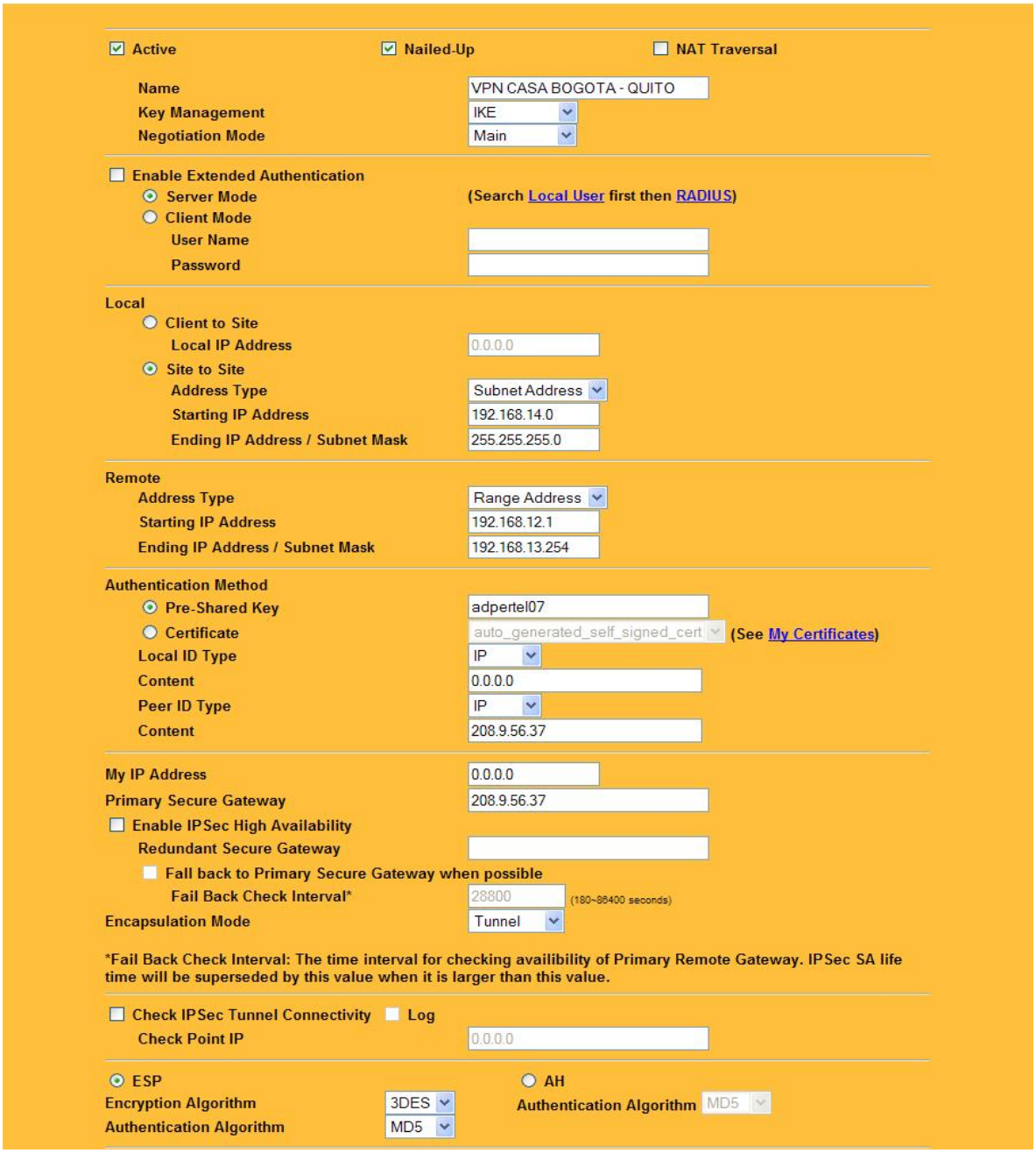


Figura 5.38. Regla de formación de VPN casa Ardila - UIO

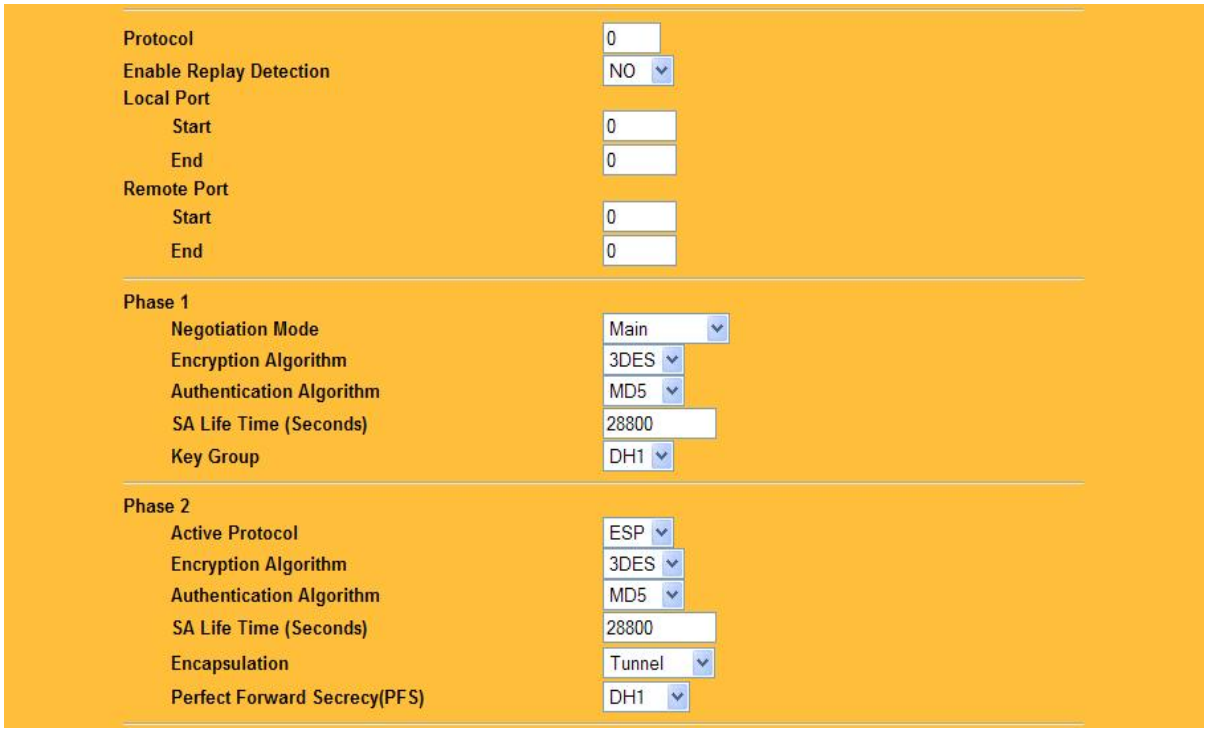


Figura 5.39. Reglas de encriptación para VPN casa Ardila - UIO

5.2 Configuración de equipos de voz sobre IP

El esquema implementado en el cliente es FXO – FXO, es decir los dos gateways de VoIP están conectados a extensiones de las respectivas centrales telefónicas PANASONIC modelo TEM824.

En Quito el gateway de un puerto Multitech MVP130 esta conectado a la extensión 119 y en Bogotá otro MVP130 a la extensión 109.

5.2.1 Plan de marcación:

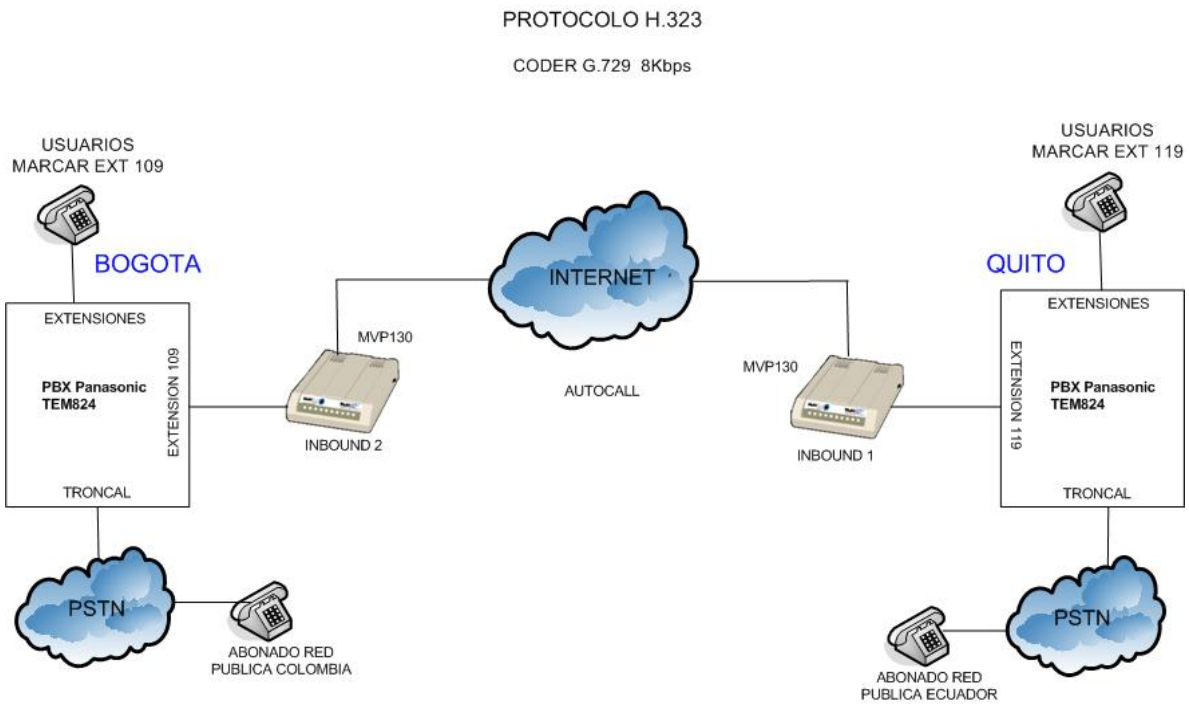


Figura 5.40. Plan de marcación VoIP

1) Para comunicase desde Oficina Quito a oficina Bogotá:

Se marca la extensión 119 luego se debe esperar por tono de marcado y luego digitar cualquier extensión que se desea comunicar en Bogotá.

2) Para comunicarse desde Oficina Quito a usuarios en la red publica de Colombia:

Se marca la extensión 119 luego se debe esperar por tono de marcado, después digitar 9 y se tiene tono de marcado de la red publica, posteriormente se podrá marcar cualquier línea telefónica del territorio colombiano.

3) Para comunicarse desde Oficina Bogotá a Oficina Quito:

Se marca la extensión 109, se espera por tono de marcado y se digita la extensión deseada de los usuarios de Quito.

4) Para comunicarse desde Oficina Bogota a usuarios en la red publica de Ecuador:

Se marca la extensión 109 luego se debe esperar por tono de marcado, después digitar 9 y se tiene tono de marcado de la red publica, posteriormente se podrá marcar cualquier línea telefónica del territorio ecuatoriano.

5.2.2 Configuración de Gateway de voz Quito:

Clave de acceso: User: VoIPardila password: adardilaecu

Configuración IP:

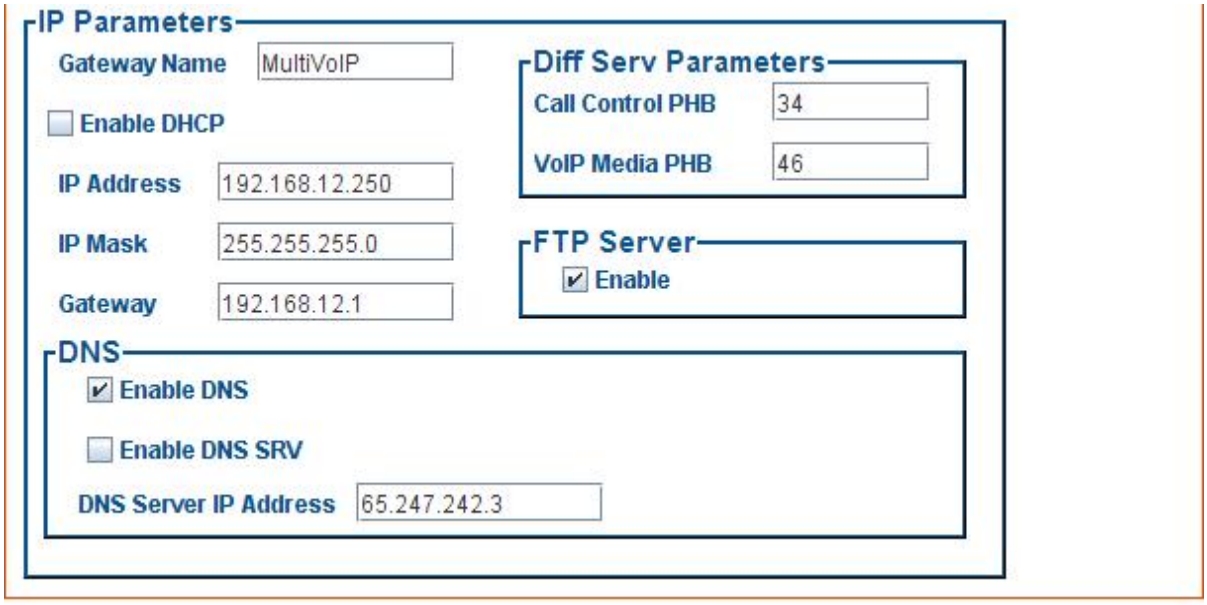


Figura 5.41 IP de gateway de Voz UIO

Parámetros de canal de Voz:

Selección del coder ha emplearse en la comunicación el G.729 que comprime la voz a 8 Kbps, selección de características avanzadas que posee el equipo como supresión de silencio, esto permite que cuando no se detecte voz disminuya el ancho de banda, la cancelación de eco, permite que no se escuche la voz como muy lejana y el FEC que es para retrasmitir paquetes en caso de que alguno no llegue y exista una excelente comunicación.

El equipo posee características de fax que no se va a emplear por lo que es mejor desactivar para que no ocupe procesamiento. Otra configuración que se a realiza aquí es el autocall, esta característica del equipo nos permite que el equipo al detectar señal en su puerto analógico, es decir, el puerto que va a la central, automáticamente marque el numero hacia el otro equipo VoIP, que es el numero 2.

El jitter, es un buffer de almacenamiento y envío, esto permite que el equipo actué de mejor manera cuando existe tiempos demasiados altos en el envió de paquetes de un lugar a otro.

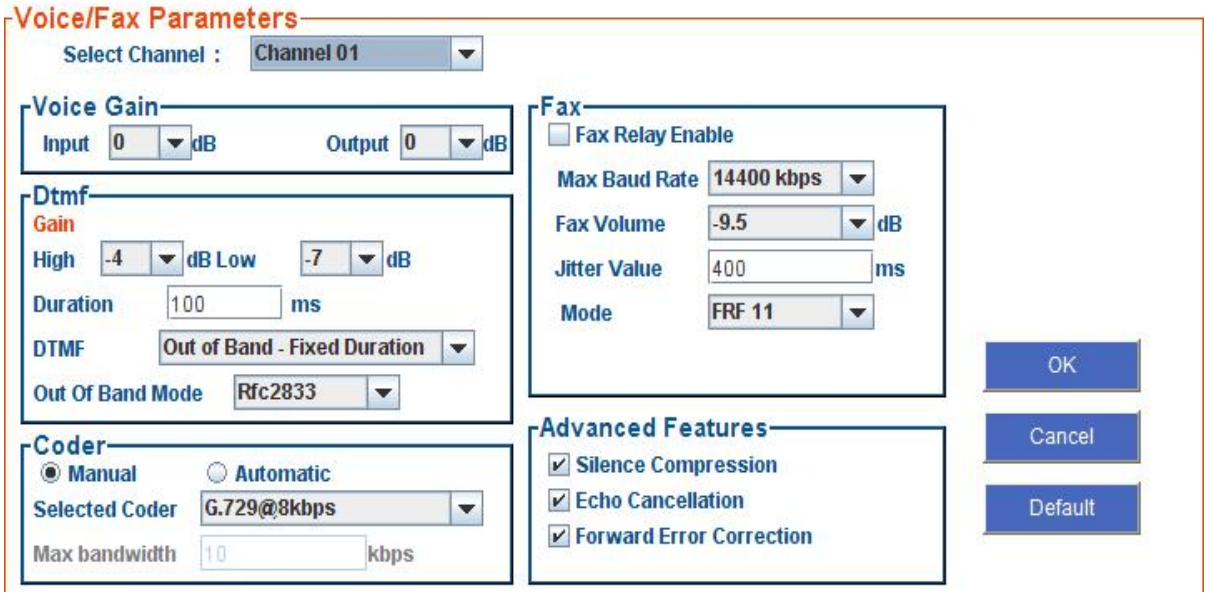


Figura 5.42. Configuración de parámetros equipo VoIP UIO

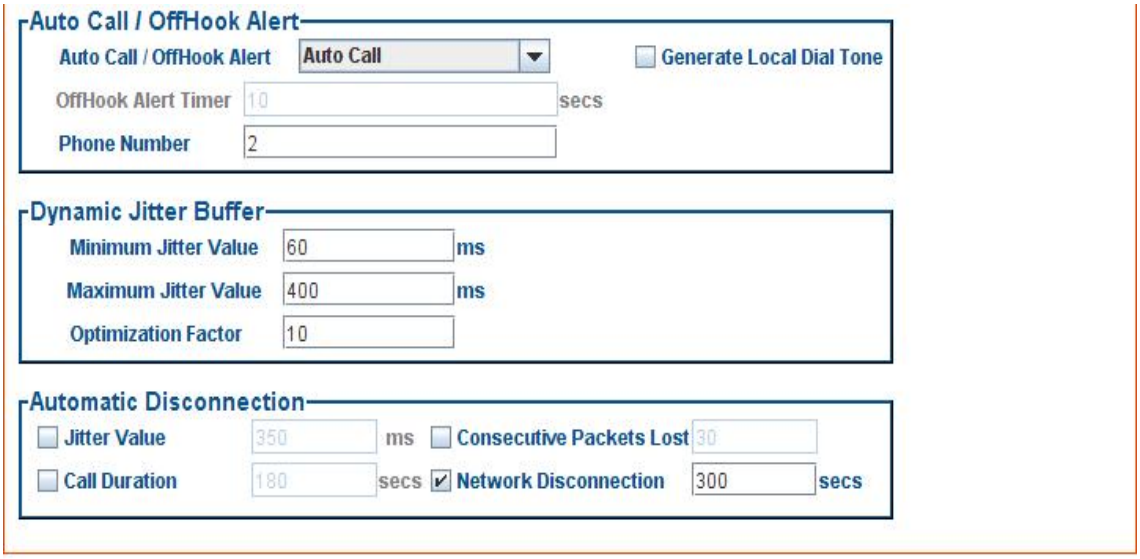


Figura 5.43. Configuración de autollamada equipo VoIP UIO

Parámetros del puerto o Interfase

Se selecciona como quiere que trabaje el puerto analógico como FXO, receptor de voltaje o como FXS, emisor de voltaje ya que este equipo posee esa ventaja de trabajar en los dos modos. Pudiendo modificar parámetros de cuantos timbre quiere que de antes que de tono de ocupado.

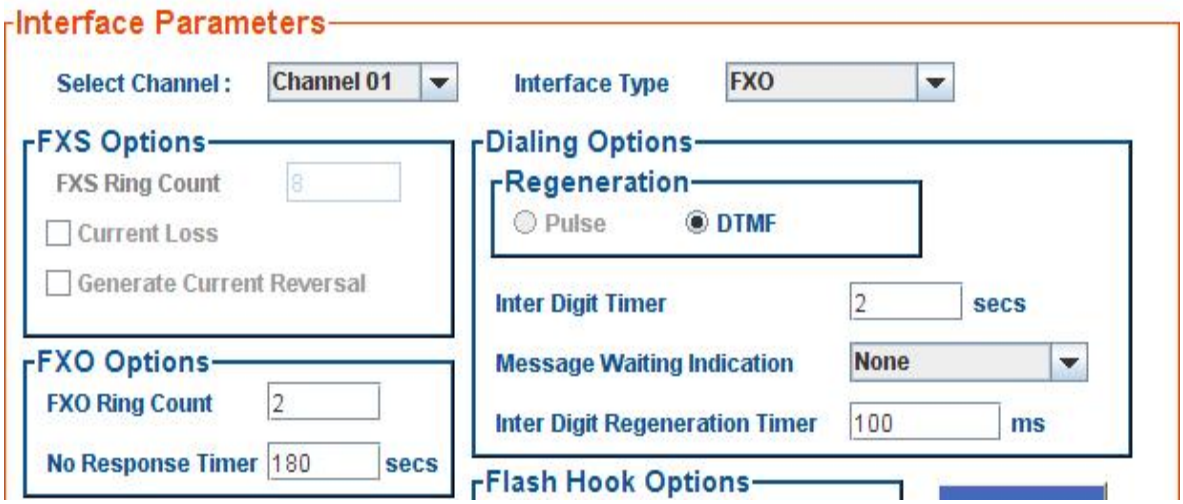


Figura 5.44. Parámetros de Interfase MVP130 UIO

Outbound

El outbound como su nombre lo indica, es el lugar donde se va a configurar la guía telefónica donde se relaciona el número de los equipos remotos la ip con la cual se va a comunicar y el protocolo a emplearse.

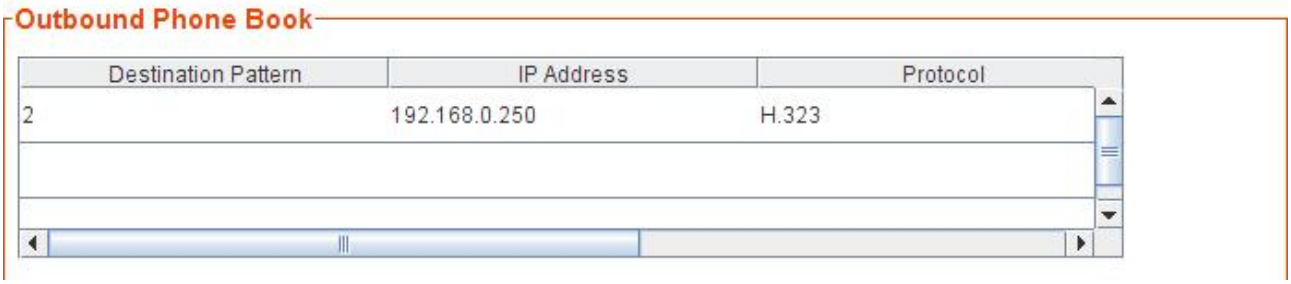


Figura 5.45. Outbound phone book MVP130 UIO

Inbound:

El indbound es el numero que corresponde al equipo, en este caso al equipo de UIO le corresponde el numero 1.

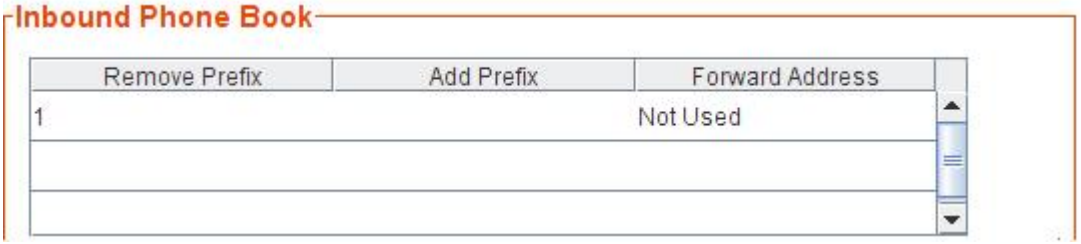


Figura 5.46. Indbound Phone Book MVP130 UIO

5.2.3 Configuración de Gateway de voz Bogotá:

Clave de acceso: User: VoIPardila , password: adardilacol

Configuración de la IP que corresponde al equipo con su respectiva mascara y puerta de salida.

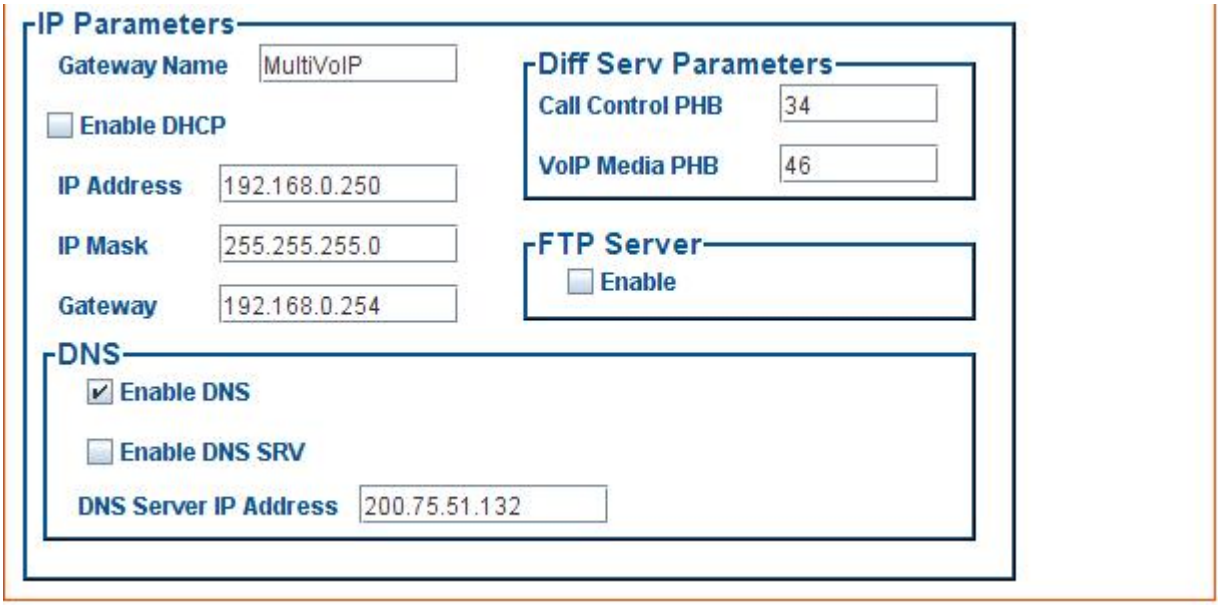


Figura 5.47. Ip de equipo VoIP BGT

Se configura los parámetros de comunicación como el coder, los opciones avanzadas, el autollamado, que deben ser las mismas que el equipo de quito para que se pueda establecer la comunicación con el mismo.

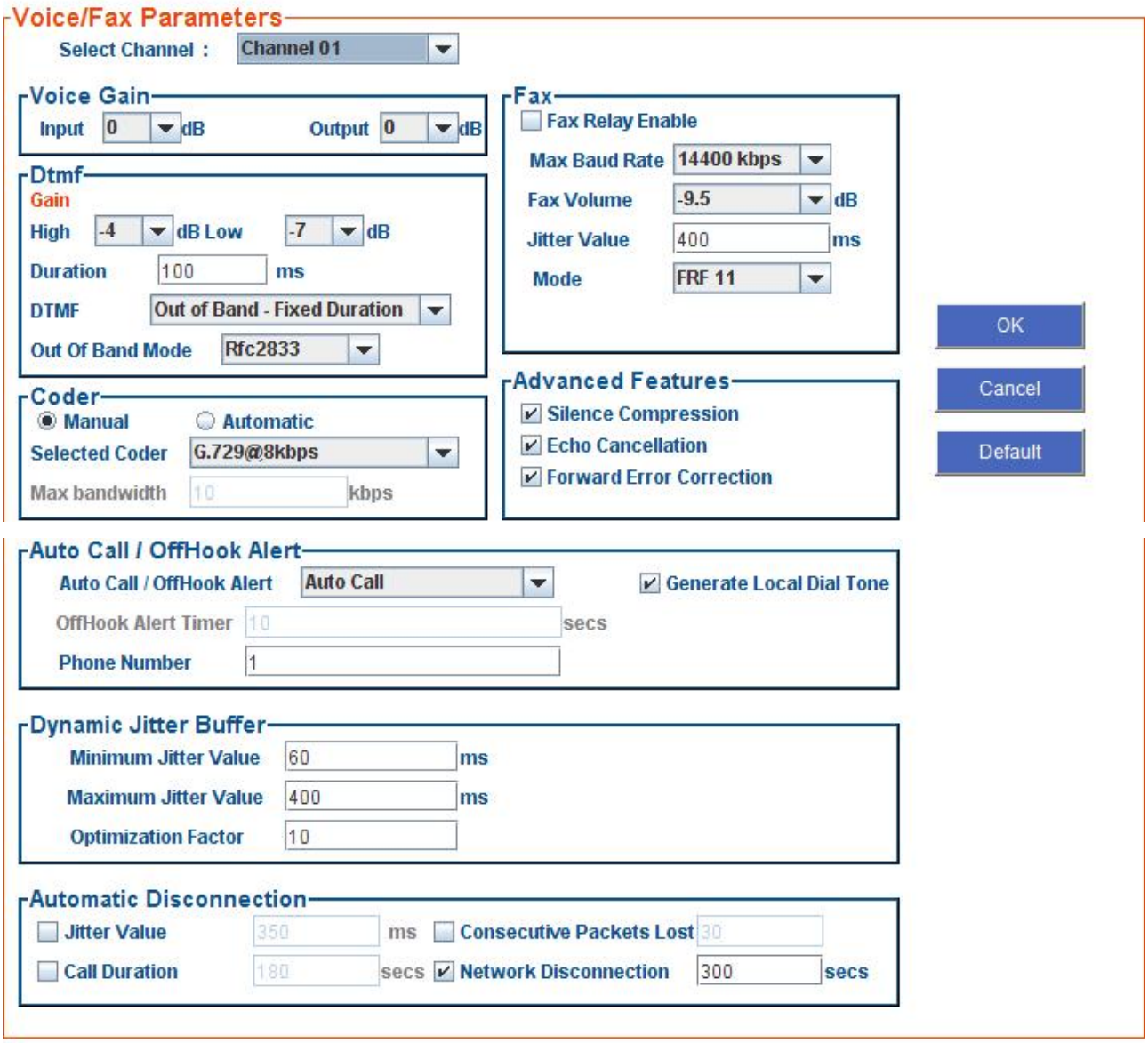


Figura 5.48. Parámetros de la voz MVP130 BGT

Parámetros del puerto o Interfase, seleccionamos como quiere que trabaje el puerto analógico como FXS o FXO, para este caso como va conectado a una extensión de la central va como puerto FXO.

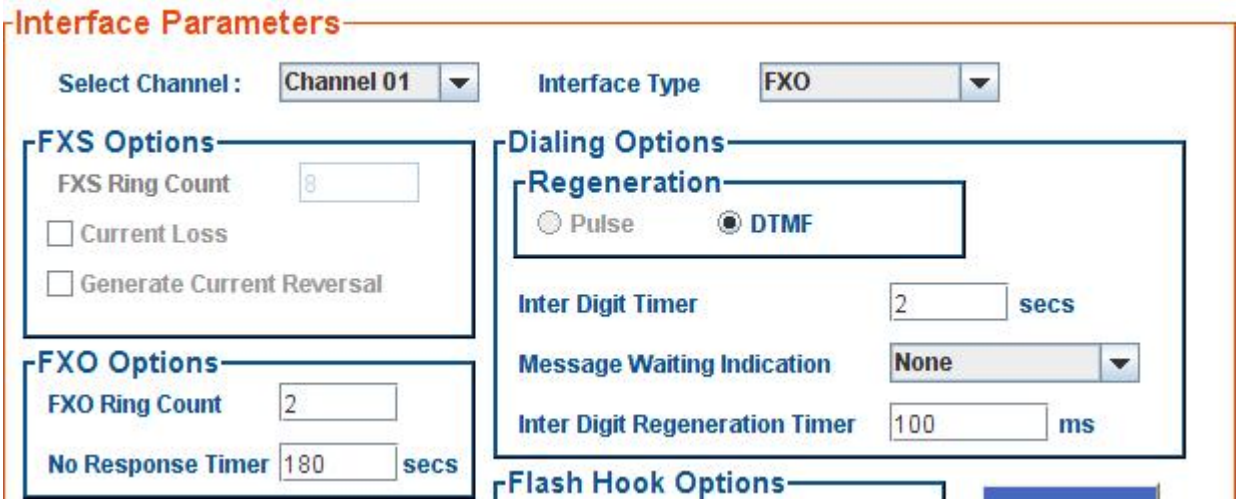


Figura 5.49. Parámetro de la interfase MVP130 BGT

Outbound, se ingresa el numero que corresponde al equipo de las oficinas de quito con su respectiva ip y el protocolo que se van a comunicar.

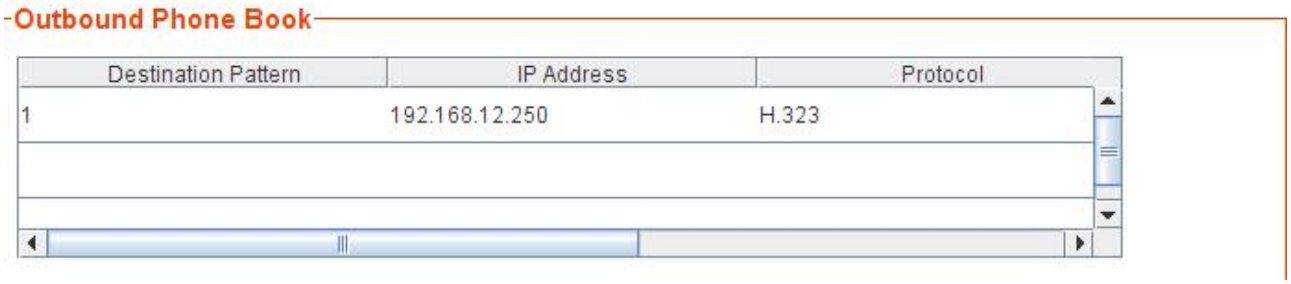


Figura 5.50. Outbound MVP130 BGT

Inbound, el numero con el que el equipo de UIO vera a este equipo que corresponde al numero 2.

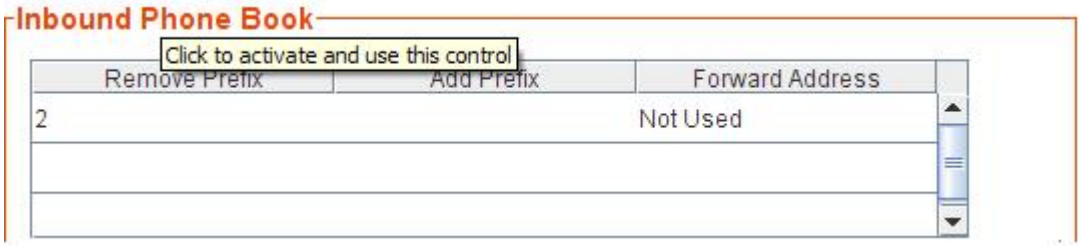


Figura 5.51. Indbound MVP130 BGT

5.3 Pruebas de acceso a cámaras, a routers y formación de VPN

Para estas pruebas se empleo la herramienta NMAP para comprobar el acceso a los puertos que fueron configurados para el acceso de las cámaras, para la administración remota del equipo Zywall. Estas pruebas fueron satisfactorias como se puede apreciar en anexo 3.

Para la verificación de la formación de la VPN, es mismo router Zywall ofrece la posibilidad de comprobar que se este levantando y formando la vpn a los diferentes sitios como se puede apreciar en anexo 3.

Se ha revisado todos los requerimientos pedidos por la empresa y se ha comprobado que todo esta operando correctamente por lo que estas pruebas fueron completadas en un 100% y todo esta operando correctamente.

5.4 Pruebas de comunicación de voz

Para las pruebas de comunicación de VoIP, la única forma de poder tener un indicativo de la calidad de la comunicación en basados en el criterio de las personas que lo utilizan a diario mediante una encuesta a los empleados de la empresa. Ver anexo 4

De donde se obtuvo los siguientes resultados de las 12 personas encuestadas:

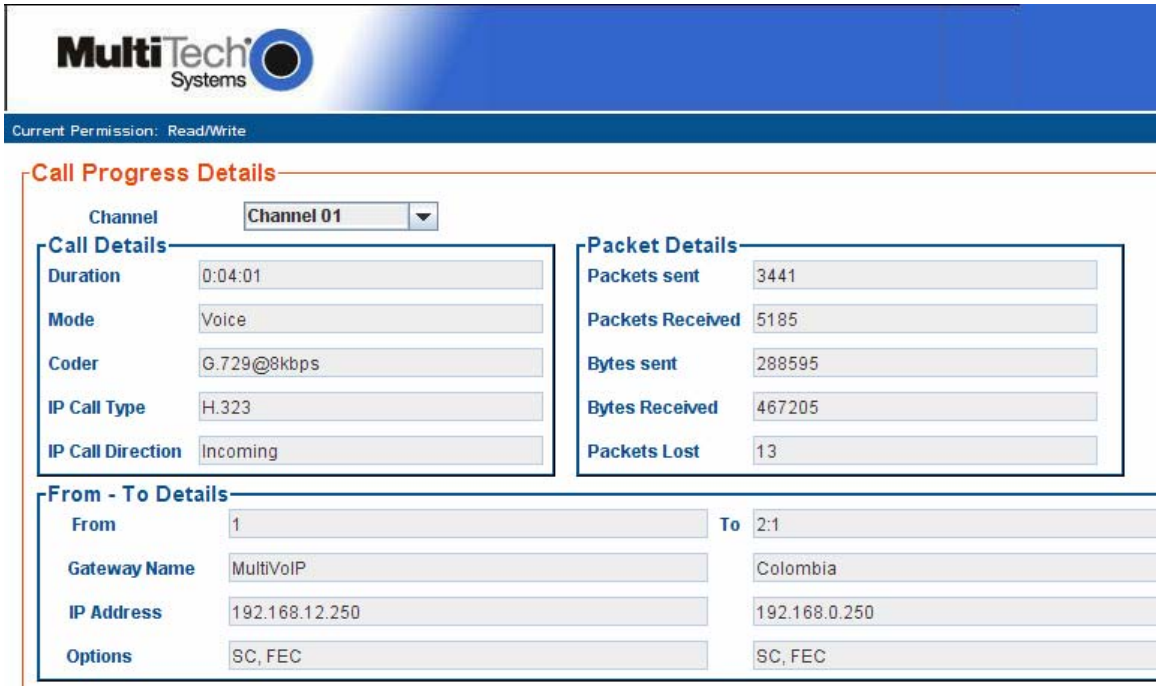
De la encuesta realizada, se obtuvo que se tiene una calidad promedio de la comunicación mediante los gateway de voz sobre ip igual a 8, siendo este calificado en una escala del 1 al 10 en la encuesta, donde 1 es mala y 10 es excelente.

Haciendo una comparación entre la comunicación mediante líneas convencionales y la comunicación VoIP, se obtuvo que de las 12 personas consultadas, 8 encuentran la comunicación igual, 2 mejor y 2 peor. Es decir, haciendo un balance se puede decir que la comunicación de voz es igual.

También se analizo la calidad de servicio en horas pico, es decir, cuando la mayor cantidad de gente esta navegando en Internet, de las personas consultadas 10 coincidieron que la comunicación no se degrada, es decir, no afecta al canal de comunicación la navegación, como sabemos esto gracias a la administración de ancho de banda. Y 2 dijeron que si se degrada.

Por lo tanto, se concluye que la comunicación es buena, y se puede comunicar a cualquier hora a Colombia sin ningún inconveniente, teniendo una comunicación clara sin retardos ni interferencias.

Y a su vez se puede comprobar el funcionamiento del mismo en el call progress que posee el equipo para indicar que equipo esta llamando a donde y duración de la comunicación.



5.52 Formación de llamada desde UIO a BGT

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

La implementación de dos redes privadas virtuales entre las oficinas de Quito, la oficina de Bogota – Colombia y la casa del gerente en Bogota, cumplieron la expectativa de la corporación Intertrading Ardila, ahora es posible compartir información entre sucursales, y poder acceder a cualquier computador mediante escritorio remoto. A su vez, se implemento la comunicación a través de voz sobre ip, al tener una herramienta de trabajo que es el Internet se esta aprovechando al máximo esta ventaja, la comunicación IP se esta convirtiendo en una parte fundamental para las empresas por el ahorro en el consumo telefónico sin emplear las líneas comerciales, especialmente cuando poseen sucursales en distintas ciudades como es el caso de la corporación Ardila.

La administración del ancho de banda dentro de los routers instalados, es una característica que permite que se controle el canal de comunicación en los sitios, ya que mediante este, se esta separando servicios y así no se vean afectados especialmente con la navegación a Internet. De esta manera también se esta dando calidad de servicio a la comunicación de voz sobre ip.

Con una Red Privada Virtual establecemos túneles entre los centros remotos y la sede principal, permitiendo el acceso a los archivos compartidos y pc de la Intranet central a todos los usuarios de cada delegación como si se encontrasen en una misma red local.

La utilización de una Red Privada Virtual, además de proteger las comunicaciones nos permite optimizar los recursos utilizando una única línea para el acceso a Internet y para las comunicaciones con las delegaciones, eliminando de esta forma la necesidad de contratar líneas punto a punto para ello. La seguridad es uno de los factores fundamentales y de éxito de la utilización de esta tecnología, ya que garantiza en todo momento que sus comunicaciones sean fiables.

6.2 Recomendaciones

Para toda comunicación de voz sobre ip, así se tenga un enlace dedicado entre los sitios remotos, es necesario crear reglas de administración del ancho de banda cuando este canal es compartido con otros servicios como la navegación a Internet. Cuando los usuarios navegan a diferentes sitios y realizan descargas de archivos pueden llegar a inundar el canal que les da el proveedor y esto afecta especialmente a la voz sobre ip, porque va a existir retardos o entrecortes en la comunicación.

Las reglas de encriptación para la formación de la VPN, deben ser muy seguras para que estas no sean descifradas y la información se fugue hacia personas no deseadas. Pero también hay que tomar en cuenta los tiempos en que se demora la información en encriptarse y desincriptarse en cada uno de los sitios por lo que tampoco hay que escoger parámetros que demoren mucho este proceso.

ANEXOS

ANEXO 1

REGULACIONES EN EL ECUADOR PARA LA VOIP

Regulación de los centros de acceso a Internet y ciber cafés

(Resolución No. 073-02-CONATEL-2005)

Consejo Nacional de Telecomunicaciones CONATEL

Considerando:

Que el avance tecnológico ha impulsado el crecimiento de nuevas tecnologías sobre diferentes servicios y aplicaciones de telecomunicaciones como la internet, cuya utilización debe masificarse, debido a la gran variedad de aplicaciones;

Que la Resolución 399-18-CONATEL-2002, publicada en el Registro Oficial 643 de 19 de agosto del 2002, contiene las normas que regulan de manera adecuada la prestación de servicios que ofrecen los ciber cafés o centros de información y acceso a la red internet, sin embargo es necesario incorporar aspectos relacionados con el uso de voz sobre Internet;

Que el plan de conectividad y las políticas de masificación de Internet establecidas por el Consejo Nacional de Telecomunicaciones requieren la participación de diferentes estamentos de la sociedad, así como marcos regulatorios flexibles que permitan el acceso de la gran mayoría de la población a la red de Internet;

Que en comisión conformada por delegados de los miembros del Consejo Nacional de Telecomunicaciones, se analizaron los mecanismos adecuados para el funcionamiento y operación de los centros de información y acceso a la red de internet o “Ciber Cafés”;

Que la regulación debe basarse en criterios objetivos, no discriminatorios, proporcionales y transparentes; y,

En ejercicio de sus facultades legales,

Resuelve:

Expedir **LA REGULACIÓN DE LOS CENTROS DE ACCESO A INTERNET Y CIBER CAFÉS.**

Art.1.-Definir como “Ciber Cafés” a los “Centros de información y acceso a la red de Internet”, que permiten a sus usuarios acceder a dicha red mediante terminales de usuario final, en un punto, local o ubicación determinados, abiertos al público o a un grupo definido de personas, mediante el uso de equipos de computación y demás terminales relacionados.

Art.2.-Se prohíbe expresamente la prestación de servicios de telecomunicaciones finales o portadores sin contar con el título habilitante correspondiente y solo se los podrá prestar mediante convenios de reventa, de conformidad con lo dispuesto en la legislación vigente.

Art.3.-La voz sobre internet podrá ser ofrecida por los centros de información y acceso a la red de internet o “Ciber Cafés” de acuerdo a las siguientes condiciones:

a. La voz sobre internet podrá ofrecerse exclusivamente para tráfico internacional saliente, prohibiéndose su utilización para la realización de llamadas locales, regionales, llamadas de larga distancia nacional, llamadas a servicios celulares o llamadas a servicio móvil avanzado;
b. El número de equipos terminales asignados para uso de voz sobre internet, en ningún caso podrá exceder del 25% (veinticinco por ciento) de la capacidad total de terminales instalados para atención al público en los “Centros de información y acceso a la red Internet” o “Ciber Cafés”;
c. Los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” que cuenten con dos (2) o tres (3) terminales totales, podrán asignar solo uno para uso de voz sobre internet;
d. Los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” que ofrezcan voz sobre Internet, de conformidad con lo señalado en los literales a) y b) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente resolución;
e. Los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones reportes relacionados con las aplicaciones prestadas por los ciber cafés en los formatos a publicarse en la página web del CONATEL; y,

f. Los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones, reportes relativos al tráfico de voz que cursan por internet en los formatos a publicarse en la página web del CONATEL.

Art.4.-Se prohíbe a los “Centros de información y acceso a la red de Internet” o “Ciber Cafés” el uso de dispositivos de conmutación, tales como Gateways o similares que permitan conectar las llamadas sobre internet a la red telefónica pública conmutada, a las redes de telefonía móvil celular o del servicio móvil avanzado y de esta manera permitan la terminación de llamadas en dichas redes.

Art.5.-Quedan excluidos de la presente regulación los establecimientos que deseen ofrecer voz sobre internet y que no cumplan con las condiciones establecidas en los artículos 3 y 4 de la presente resolución, independientemente de la facilidad tecnológica que utilicen; dichos establecimientos deberán sujetarse a lo que se establece en el “Reglamento del servicio de telefonía pública”.

Art.6.-Quedan excluidos de la presente regulación los locutorios, cabinas y otros establecimientos que ofrezcan el servicio de transmisión de voz, ya sea por medio de conmutación de paquetes o utilizando conmutación de circuitos. Estos establecimientos deberán sujetarse a lo que se establece en el “Reglamento del servicio de telefonía pública, o a la reventa de servicios”.

CARTA ENVIADA A SENATEL PARA APROBACIÓN DEL USO DE VOZ SOBRE IP EN LAS EMPRESAS

ALDEBERAN
...su socio tecnológico

N# 3650

Guayaquil, 9 de Agosto 2005.

Secretaria Nacional De Telecomunicaciones
13:25
10 AGO 2005

Señor Doctor
HERNAN LEON GUARDERAS
SECRETARIO NACIONAL DE TELECOMUNICACIONES
Quito. 02-2947800 ext 703

De nuestras consideraciones:

Por medio de la presente solicito muy respetuosamente a usted se nos indique dado que ostenta la autoridad en el uso de todo lo relacionado con las Telecomunicaciones la respuesta a la siguiente inquietud:

Es conocido y popularmente usado la transmisión de VOZ sobre los enlace de datos perfectamente permitidos por la ley y según se indica en el REGLAMENTO GENERAL A LA LEY DE TELECOMUNICACIONES REFORMADA (Decreto No 1790) Articulo 14, pero no encontramos ningún articulo ó documento formal que sustente el uso de las líneas telefónicas de las operadoras (Pacifictel, Andinatel, Linkotel, Alegro, etc..) por medio de estos enlaces de datos. Detallare con un ejemplo nuestra inquietud para que no se mal interprete el uso que se desea dar:

Los usuarios de la oficina en Guayaquil se comunican por medio del enlace de DATOS usando tecnología VoIP con el commutador de la oficina en Quito pero en lugar de llamar a un colega dentro de la oficina utiliza la salida en este caso de ANDINATEL y llama a un cliente en Quito.

Nuestra inquietud radica si es posible realizarlo dentro de un marco legal o si existe alguna disposición que indique la falta.

Por la atención brindada y en espera de su respuesta, le anticipo mis agradecimientos.

Atentamente,

Ing. Mónica Beltrán
Gerente General

Guayaquil: Cdla. Urdenor II Mz.245 V.3 Teléfono: +593 4 2384 472 Email: mercadeo@aldeberan.com.ec

SENATEL
Secretaría Nacional de Telecomunicaciones

Oficio No. **SNT-2005-** 1669

Quito, 14 SEP 2005

Señora Ingeniera
Mónica Beltrán
Gerente General
ALDEBERAN
Guayaquil.-

Referencia (S/N / 09-05-05)
(HT-3650; 10-08-05)

De mi consideración:

Con relación al oficio de la referencia, mediante el cual se consulta si existe un artículo o documento formal que sustente el uso de líneas telefónicas de las operadoras autorizadas a través de enlaces de datos pertenecientes a una red privada, debo indicar que el Reglamento General a la Ley Especial de Telecomunicaciones Reformada define conexión como la unión que permite el acceso a una red pública de telecomunicaciones desde la infraestructura de los prestadores de los servicios de reventa, servicios de valor agregado y redes privadas, cuyos sistemas sean técnicamente compatibles.

Por lo tanto, la conexión entre una red privada y una red pública es legal, mientras sea utilizada únicamente para beneficio del titular del permiso de red privada y bajo ninguna circunstancia preste servicios a terceros.

Atentamente,

Dr. Hernán León Guarderas.
SECRETARIO NACIONAL DE TELECOMUNICACIONES

Av. Diego de Almagro N31-95 y Alpallana, Edif. Senatel. Telfs: 2947800 Fax: 2901010
Call Center 1-800SENATEL, Casilla 17-07-9777. www.conatel.gov.ec Quito-Ecuador

ANEXO 2

ANÁLISIS DE COSTOS

ANALISIS DE COSTO BENEFICIO

COSTOS Mensuales con los que vienen trabajando	
Costo de Internet en UIO 320 Kbps	45
Costo de Intenet en BGT 600 Kbps	46
Costo de Internet Casa Ardila 128 Kbps	20
Costo por IP plublica ECU	15
Costo por IP plublica COL	8
Total	134

INVERSION INICIAL		
	Precio + Instal.	
Equipo Zyxel por unidad	250	805
Equipo Multitech por unidad	436	872
Total	686	1677

BENEFICIOS para 1 Meses	
Ahorro en la planilla telefonica (en Col y en Ecu)	360
Ahorro en envio de documentos	20
Costo de llamadas internacionales por minuto ECU	0,16
Costo de llamadas internacionales por minuto COL	0,12
Total de beneficios	380

Tasa de interes 8%	0,08

Utilizacion del equipo por dia en minutos	120 minutos minutos	costo	subtotal x dia	dias laborables	Total x mes
De UIO a BGT	90	0,16	14,4		
de BGT a UIO	30	0,12	3,6		
			18	20	360

FLUJO DE CAJA PROYECTO ARDILA

CONCEPTO	MENSUALES	ANUALES
INVERSIÓN INICIAL		-1677
GASTOS CORRIENTES	-134	-1608
AHORRO LLAMADAS y ENVÍOS	380	4560

MESES	0	1	2	3	4	5	6	7	8	9	10	11	12
CONCEPTO	**MES DE INVERSIÓN**	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
FLUJO DE FONDOS													
A.- FLUJO DE BENEFICIOS													
1.- Ahorro		380	380	380	380	380	380	380	380	380	380	380	380
TOTAL BENEFICIOS	-	380	380	380	380	380	380	380	380	380	380	380	380
B.- FLUJO DE COSTOS													
1.- Inversión Fija	-1.677,00												
2.- Gastos Corrientes		134	134	134	134	134	134	134	134	134	134	134	134
TOTAL FLUJO DE COSTOS		134	134	134	134	134	134	134	134	134	134	134	134
FLUJO ECONÓMICO (A-B)	-1.677,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00	246,00
FLUJO FINANCIERO	**-1.677,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**	**246,00**

CALCULO DEL TIR Y VAN PARA PROYECTO ARDILA

r1=	0,09

F1/(1+i)^n

r2=	0,06

MESES	FF	TASA DE DESCUENTO (1+i)^n	FFA
0	$ -1.677,00		- 1.677,00
1	$ 246,00	1,09	225,69
2	$ 246,00	1,19	207,05
3	$ 246,00	1,30	189,96
4	$ 246,00	1,41	174,27
5	$ 246,00	1,54	159,88
6	$ 246,00	1,68	146,58
7	$ 246,00	1,83	134,57
8	$ 246,00	1,99	123,46
9	$ 246,00	2,17	113,27
10	$ 246,00	2,37	103,91
11	$ 246,00	2,58	95,33
12	$ 246,00	2,81	87,46
		VAN	$ 84,54

MESES	FF	TASA DE DESCUENTO (1+i)^n	FFA
0	-1.677,00		- 1.677,00
1	$ 246,00	1,06000	232,08
2	$ 246,00	1,12360	218,94
3	$ 246,00	1,19102	206,55
4	$ 246,00	1,26248	194,86
5	$ 246,00	1,33823	183,83
6	$ 246,00	1,41852	173,42
7	$ 246,00	1,50363	163,60
8	$ 246,00	1,59385	154,34
9	$ 246,00	1,68948	145,61
10	$ 246,00	1,79085	137,37
11	$ 246,00	1,89830	129,59
12	$ 246,00	2,01220	122,25
		VAN	$ 385,43

$$TIR = r_1 + (r_2 - r_1) * VAN_1 / (VAN_1 - VAN_2)$$

FÓRMULA PARA LA INTERPOLACIÓN PARA EL CÁLCULO DE LA TIR

TIR= 0,08+(0,06-0,08)*-110,37/(-110,37-96,58)

TIR= 0,098429

TIR= 9,84%

9,9899%	TIR EXCEL
77,56	VAN EXCEL

R= Al trabajar con una tasa de descuento (tasa de oportunidad) del 8% el VAN es positivo por lo tanto el proyecto es viable.

La TIR es mayor a la tasa de oportunidad (0,098>0,09), esto reafirma la conclusión de que el proyecto es rentable, porque el valor que se paga es menor que el que se espera recibir.

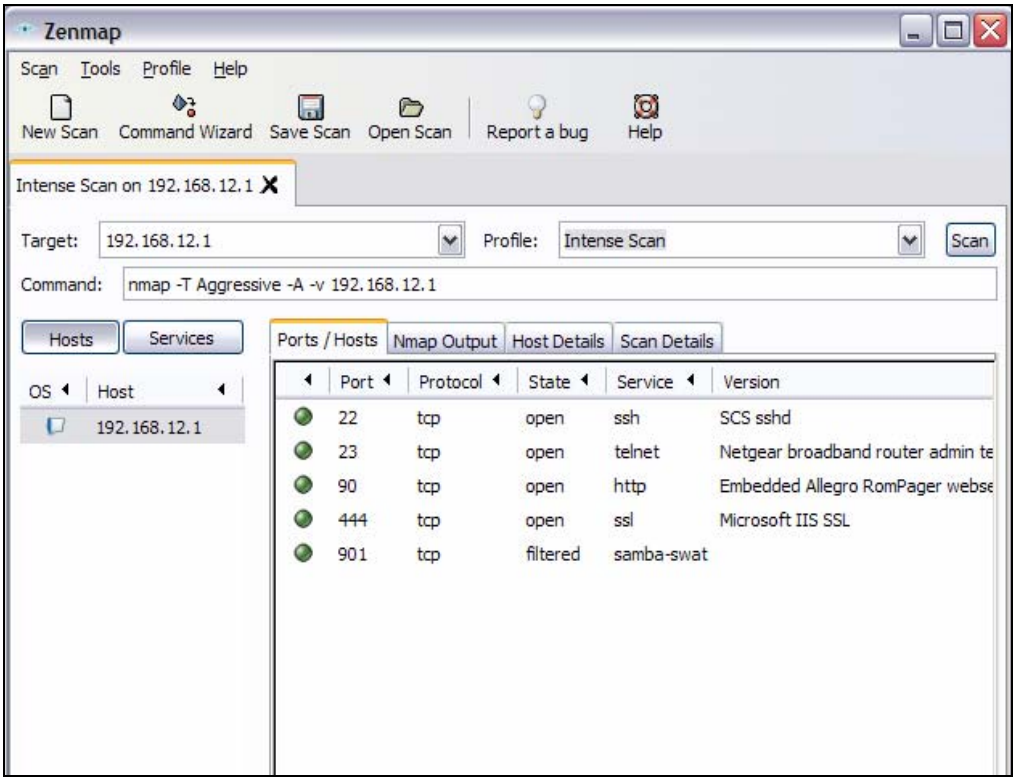
ANEXO 3

Pruebas de funcionamiento de Firewall, Nat y Vpn

Pruebas con Routers Zyxel de levantamiento de VPN y paso de puertos

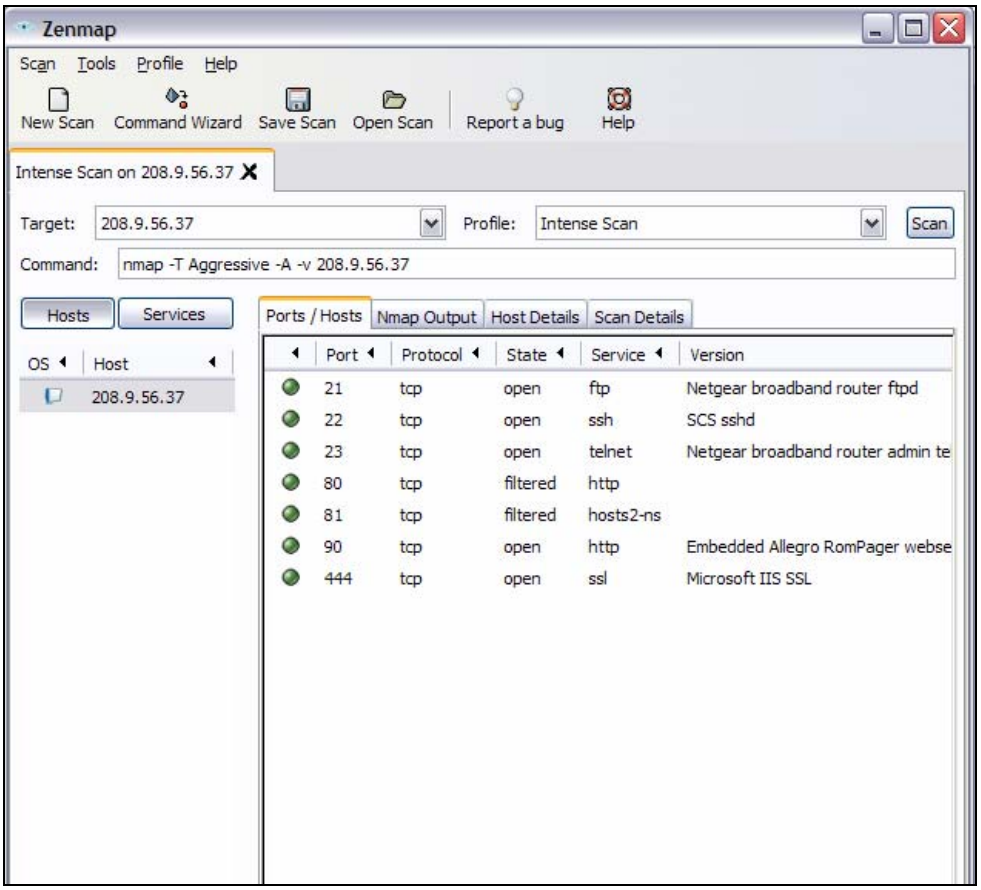
1) Pruebas de paso de puertos WAN en oficinas UIO con herramienta de software NMAP

Chequeo de la Ip privada 192.168.12.1



Chequeo de puertos ip lan mediante NMAP

Chequeo a la IP publica 208.9.56.37

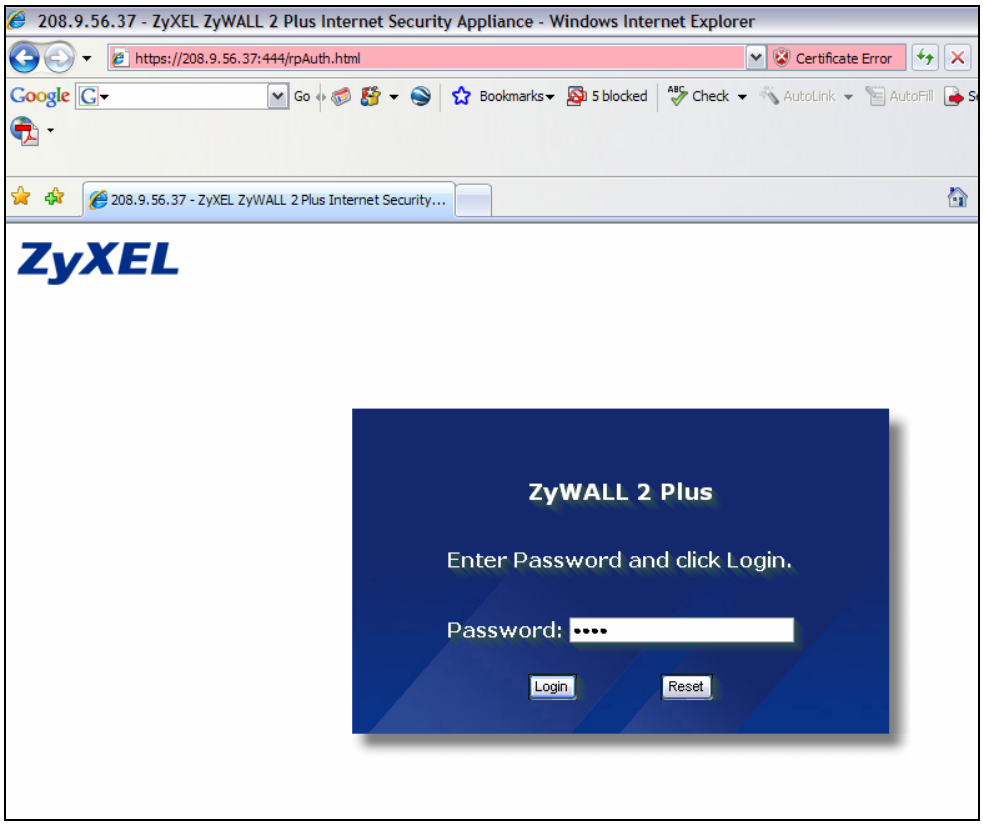


Prueba de puertos con NMAP a Zywall UIO

Como se puede observar en la prueba se esta cumpliendo con la reglas creadas en el NAT y Firewall del equipo permitiendo únicamente el paso de los puertos para administrar las cámaras (80 y 81), el puerto para administración del equipo (21, 22, 23, 90 y 444) y ningún otro puerto mas.

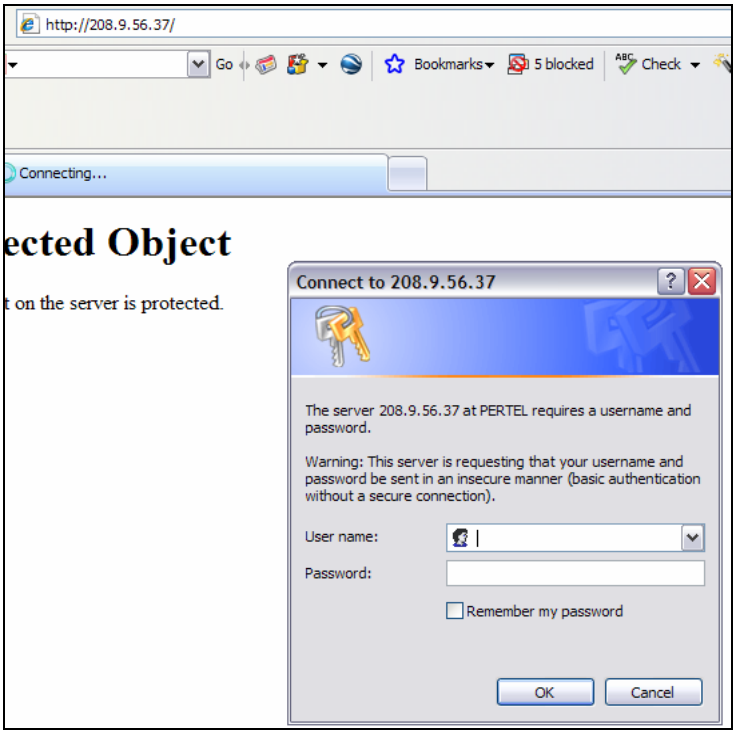
También se puede comprobar via web browser:

2) Ingreso al equipo via https puerto 444



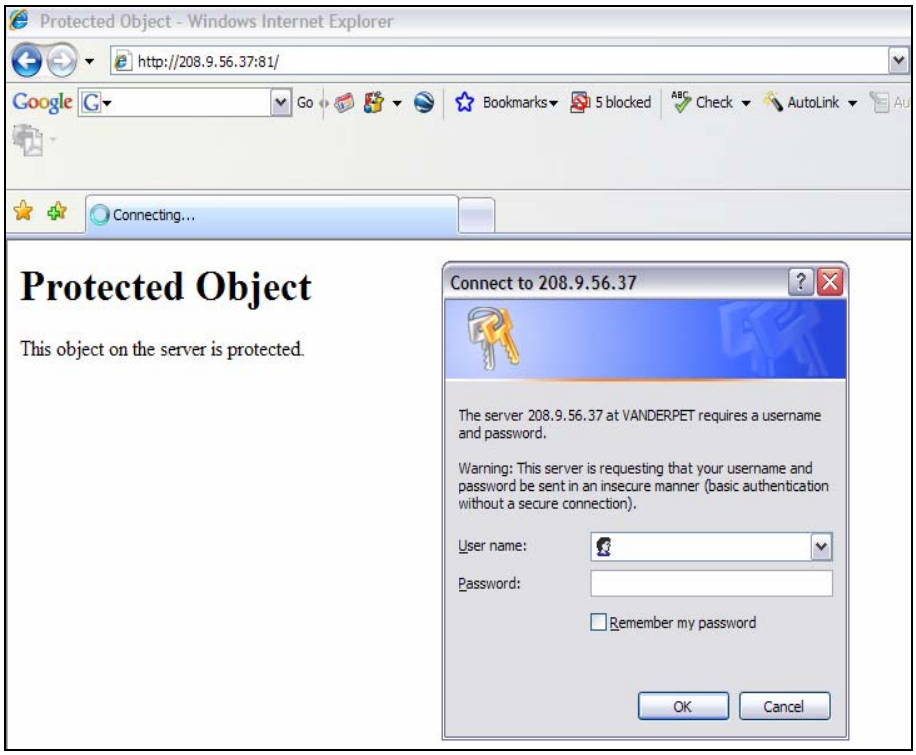
Ingreso Zywall UIO remotamente por https

3) De igual manera se ingresa a una de las cámaras por puerto 80 y puerto 81



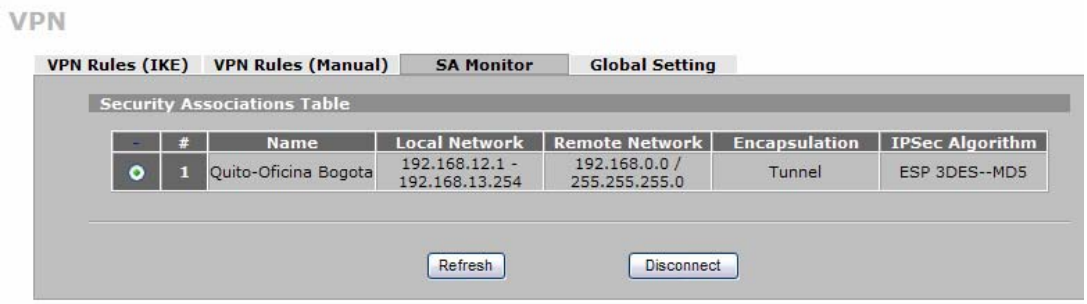
Ingreso remoto a la camara Ip de UIO puerto 80

Las cámaras permiten su ingreso mediante un user y un password que por razones de seguridad no se entrego para las pruebas pertinentes solo lo pudieron comprobar los que tienen el acceso permitido.



Ingreso remoto a la camara Ip de UIO puerto 81

4) Como prueba de verificación de la VPN se puede observar en el router el estatus de formación de la VPN

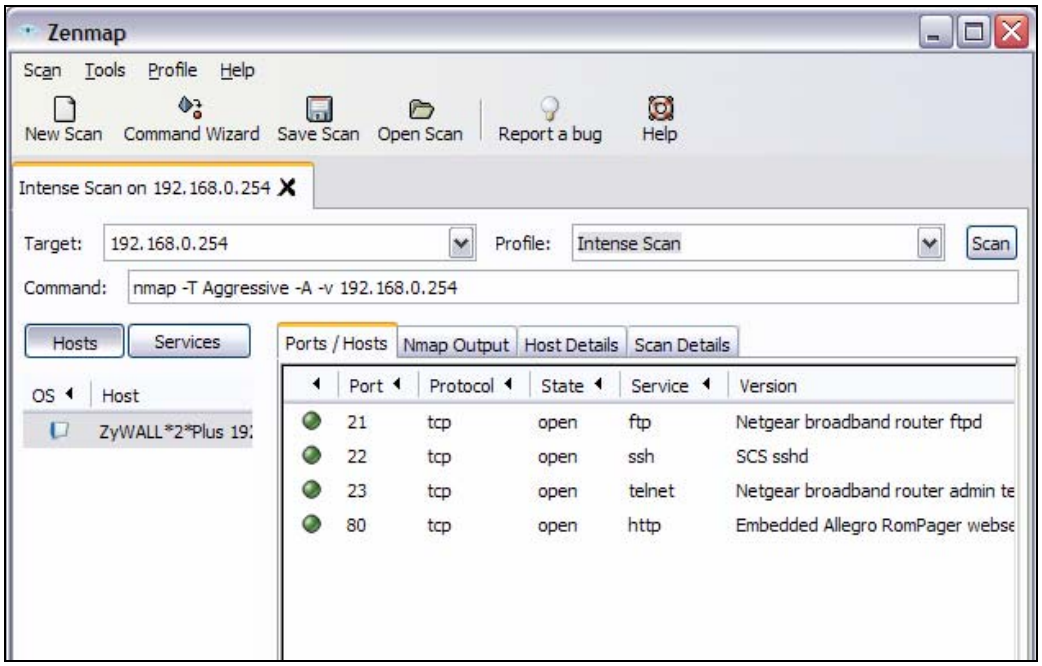


Verificación de formación de VPN

Igualmente se realizan el mismo tipo de pruebas para el router zywall de la oficina de Bogota

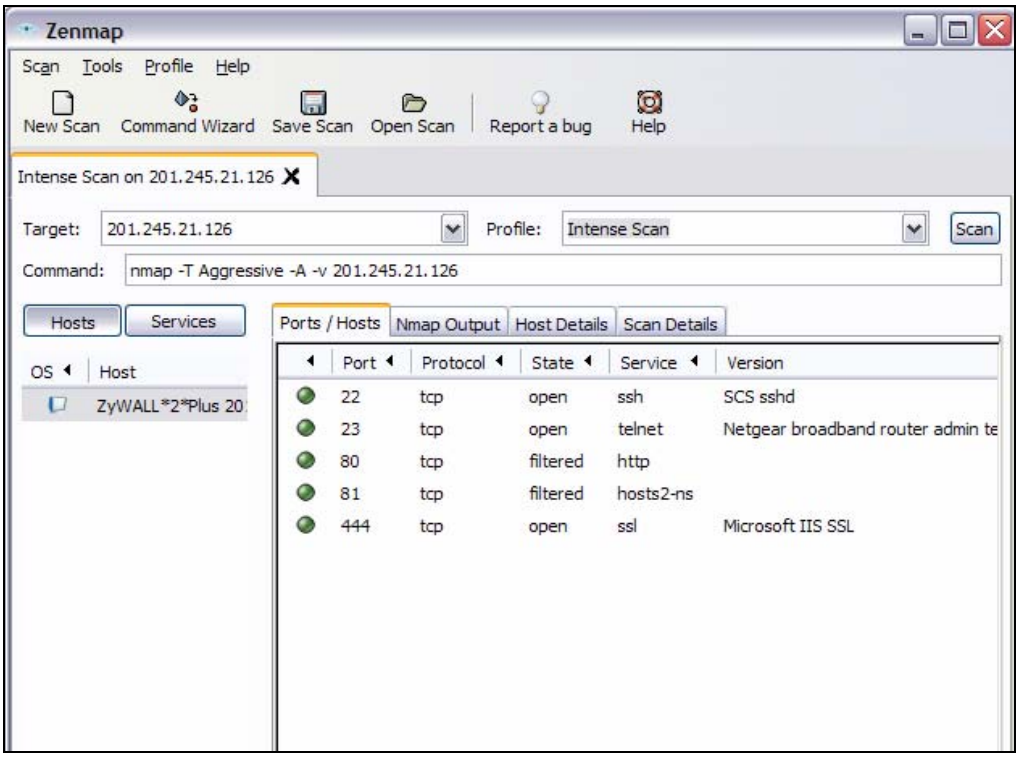
1) Revisión de puertos mediante NMAP

Revisión de la IP lan 192.168.0.254



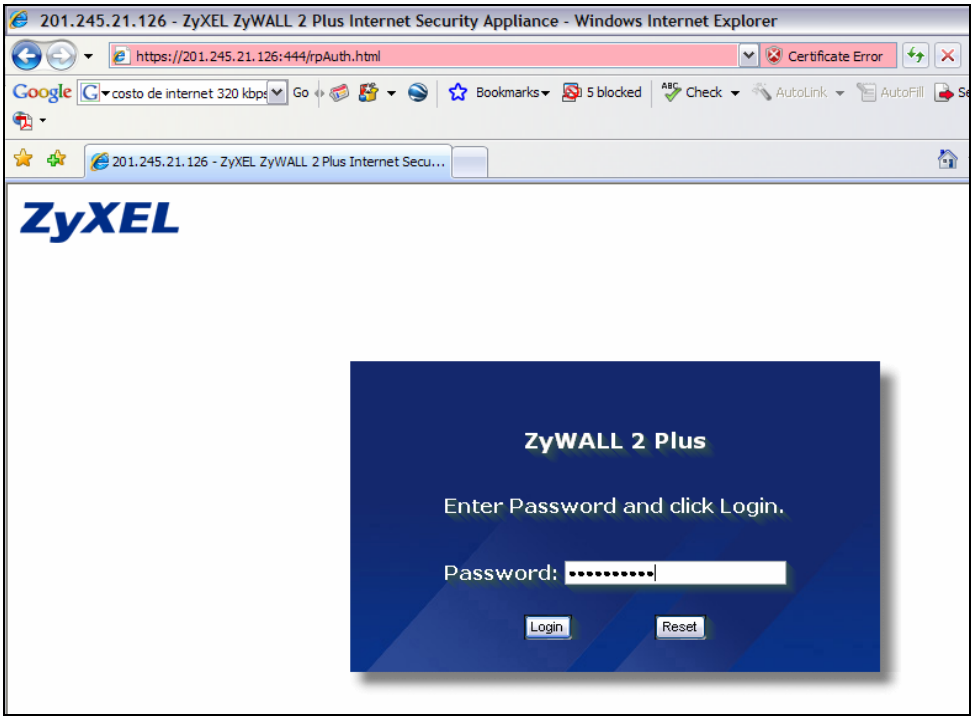
Verificación de puertos desde la IP LAN

Revisión de la IP wan 201.245.21.126



Comprobación de puertos desde la IP wan mediante NMAP

2) Verificación de acceso remoto al router via web browser https puerto 444

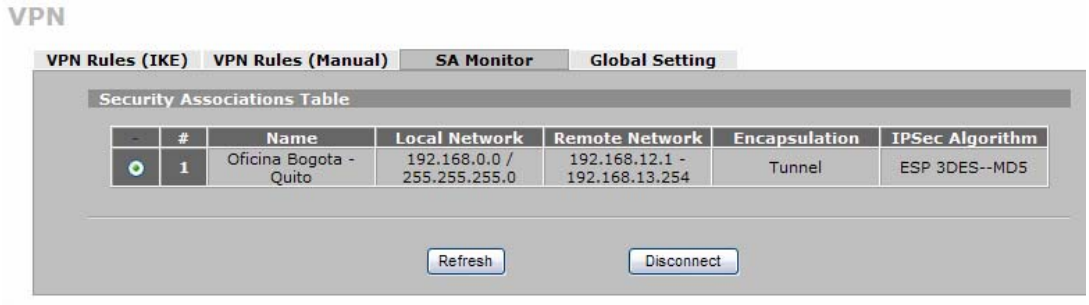


Acceso remoto a zywall de BGT por https

3) Verificación de ingreso al equipo de VoIP via web browser puerto 80

Acceso remoto al equipo de VoIP por puerto 80

Como prueba de verificación de formación de la VPN el router zyxel nos presenta una pantalla donde se puede observar el estado de la VPN



Verificación de la formación de la VPN en el zywall BGT

ANEXO 4

ENCUESTA DE CALIDAD DE SERVICIO DE LA COMUNICACIÓN VOIP

ENCUESTA SOBRE COMUNICACIÓN VOIP

1.- A utilizado comunicación VoIP anteriormente?

Si ☐

No ☐

2.- Con que frecuencia llama a las oficinas de Colombia?

Todos los días ☐

Cada semana ☐

Cada 15 días ☐

3.- Comparada con la comunicación a través de las líneas telefónicas convencionales como percibe la comunicación a través de Internet?

Mejor ☐

Igual ☐

Peor ☐

4.- En horas pico percibe que la comunicación de voz sobre IP se degrada?

SI ☐

NO ☐

5.- En una escala del 1 al 10, donde 1 es mala y 10 es excelente, como calificaría a la comunicación de voz sobre IP?

☐

6.- Recomendaría este servicio a otras empresas?

SI ☐

NO ☐

BIBLIOGRAFÍA

[1] Rosario, Marco, El estandar VoIP, http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml, 2006, mayo 2008

[2] Ruiz, Jose, VPN – Redes Privadas Virtuales, http://isa.uniovi.es/~sirgo/doctorado /VPN.pdf, marzo 2002, mayo 2008

[3] Ing. Joskowicz, José, Redes Unificadas, http://iie.fing.edu.uy/ense/asign/ redcorp/material/ 2004/Redes%20Unificadas.pdf, Julio 2006, mayo 2008

[4] Ing. Sosa, Fanny, Estandares de VoIP SIP vs. H323, http://neutron.ing.ucv.ve/ comunicaciones/Asignaturas/DifusionMultimedia/Tareas%2020051/Estandares%20de%20 VoIP%20SIP%20vs%20H323.doc

[5] European Centre for Medium-Range Weather Forecasts, http://www.wmo.int/pages/ prog/www/TEM/Guidance-doc/IPSec-technote-SP.pdf, 2003, mayo 2008

[6] Ing. Hevia, Mariano, http://www.monografias.com/trabajos12/monvpn/ monvpn.shtml?monosearch, 2002, mayo2008

[7] Pctiendas, http://www.pctiendas.com/router-firewall-vpn-netgear-prosafe-fvs124gge-p-26820.html, 2008, mayo 2008

[8] Mercadolibre, http://computacion.mercadolibre.com.pe/routers-switches, 2008, mayo 2008

[9] Agalisa, http://tienda.agalisa.es/product_info.php?cPath=59_164_214&products_id= 6615, 2008, mayo 2008

[10] http://www.controlp.com/productos.asp?id=22646&IVA=SI

[11] http://www.empretel.com.mx/ORINOCO/descripcion.asp?llave=19300