UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

AMPLIANDO COBERTURA DE UNA RED CORPORATIVA DE VOZ Y DATOS. INTERCONECTANDO SUCURSALES REMOTAS VÍA INTERNET USANDO VPNs CON ENCRIPTACIÓN IPsec. DISEÑO E IMPLEMENTACIÓN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JUAN ORLANDO VARGAS FERNÁNDEZ

PROMOCIÓN
1997- I

LIMA – PERÚ
2009

AMPLIANDO COBERTURA DE UNA RED CORPORATIVA DE VOZ Y DATOS. INTERCONECTANDO SUCURSALES REMOTAS VÍA INTERNET USANDO VPNs CON ENCRIPTACIÓN IPsec. DISEÑO E IMPLEMENTACIÓN.

A mi esposa, mis padres y mis hermanos,
por quienes siempre encuentro un motivo
de inspiración y superación cada día de mi vida.

SUMARIO

El presente trabajo describe el desarrollo de un proyecto que fue ejecutado dentro de la red corporativa del Grupo Romero, con el propósito de ampliar de manera rápida y segura su cobertura de red a nivel internacional, concretamente, hacia los países de Ecuador, El Salvador, Colombia y Guatemala.

La necesidad tecnológica ha surgido como consecuencia inmediata de la rápida expansión que este importante grupo económico peruano ha tenido en los últimos años hacia el mercado internacional, lo cual trajo también consigo el aumento de la cantidad de usuarios y por ende, el aumento de los requerimientos informáticos.

El desarrollo del proyecto se ha fundamentado en una de las tecnologías de mayor auge en la actualidad, como es la implementación de VPNs basados en IPsec, para lo cual se ha recurrido a uno de los mayores fabricantes de equipos de redes a nivel mundial, como es la compañía Cisco System Inc., sobre cuya plataforma de equipos y teniendo como medio de enlace el Internet, ha sido posible desplegar la solución final con muy buenos resultados, no sólo en el aspecto de la conectividad de las sucursales involucradas, sino también en la protección de los datos cursados.

INDICE

INTRODUCCIÓN.

El vertiginoso crecimiento e interés de las empresas que se vienen produciendo en los últimos años respecto a la seguridad de sus redes y sistemas informáticos, ha sido uno los principales factores que ha llevado a exponer el presente tema, concretamente, en el enfoque relacionado con las Redes Privadas Virtuales, sobre el cual se expone la experiencia obtenida en el diseño e implementación de esta tecnología, dentro de la red corporativa del Grupo Romero en el Perú, que gracias a esta tecnología, a ha ampliado su cobertura de red a filiales del extranjero de manera rápida, segura y económica.

En la actualidad, los delitos informáticos se han incrementado enormemente y no es ajeno para la mayoría de nosotros toparnos casi a diario con indicios de ello, tales como por ejemplo, correos electrónicos falsos que llegan a nuestro buzón, supuestamente enviados por entidades reconocidas sobre todo de tipo financieras, invitándonos a proporcionarles datos personales o a ingresar a falsos enlaces que nos conducirán de manera inocente a proporcionarles el número de cuenta bancaria, clave de acceso, montos de ahorros, etc. Situaciones como éstas, son quizás los tipos de delitos informáticos que son los más perceptibles para el común de las personas; pero existen también por otro lado, los delitos informáticos que pasan totalmente desapercibidos al usuario común y ocurren únicamente dentro de una determinada red, donde delincuentes informáticos haciendo uso, ya sea de técnicas simples o complejas, interceptan datos desprotegidos que circulan por dicha red, pudiendo llegar a obtener información muy confidencial y relevante. Tales tipos de hechos son más propensos de ocurrir si la red por la cual transmiten los datos, son redes públicas, como el caso del Internet.

Por otro lado, con la tan conocida globalización a nivel mundial, ha llevado a las empresas a tener sus redes de datos conectadas a por lo menos, un punto de acceso a Internet, sobre el cual además de realizar operaciones sencillas como navegar o enviar correos, los usan también muchas veces para interconectar sus sucursales y abaratar costos, en lugar de pagar por enlaces dedicados. Esta necesidad de usar el Internet se hace aun más fuerte, cuando se requiere conectar ubicaciones remotas que se encuentran a grandes distancias, como el caso de sucursales internacionales, donde contratar un enlace dedicado elevaría los costos enormemente.

Si juntamos ambas situaciones, que por un lado se tiene delincuentes informáticos pululando en el Internet a la caza de datos desprotegidos y por otro lado, la alta necesidad que tienen las empresas de usar este medio para transmitir datos confidenciales, nos lleva inevitablemente a la conclusión de que todo dato enviado por una red debe ser protegido o encriptado antes de ser transmitido, sobre todo, si se usa para tal fin una red pública, tal como el Internet.

Tecnológicamente, esto puede ser llevado a cabo usando una Red Privada Virtual, más comúnmente conocida como VPN por sus siglas en inglés de Virtual Private Network. Para desplegar dicha tecnología existen diversos protocolos, dentro de los cuales el más conocido y uno de los más seguros es el protocolo IPSec. Este es el tema que se desarrollará en el presente informe, donde se expone de manera práctica el diseño e implementación de esta solución ejecutada para la red corporativa del Grupo Romero, que requería expandir sus sucursales a nivel internacional.

CAPITULO I
PLANTEAMIENTO DE INGENIERIA DEL PROBLEMA

1.1 Descripción del Problema

1.1.1 El Escenario

El escenario donde se presentó la necesidad tecnológica se sitúa en un consorcio de empresas que pertenecen al Grupo Romero, uno de los grupos económicos más importantes del país, al cual pertenecen diversas empresas que desarrollan variados rubros de negocios en diferentes sectores de la industria, tales como alimentos, logística, infraestructura, comercio, servicios y otros. Dicho conjunto de empresas, al estar todas regidas por un mismo grupo económico, mantienen un mismo sistema informático contable, por lo cual todas ellas se encuentran interconectadas mediante una misma red corporativa de datos y voz a nivel nacional. Aunque por otro lado, al tener diferentes rubros de negocio, cada una de las empresas cuenta con su propia sede central, sus propias sucursales, así como sus propios aplicativos de sistemas de negocios corriendo sobre la misma red común.

1.1.2 El Estado Inicial de la Red

Tecnológicamente, la red corporativa de voz y datos existente que une a todas las empresas ha sido implementada sobre la red IP/VPN MPLS de Telefónica del Perú a nivel nacional, sobre la cual se cursan diversos servicios de datos, tales como Correo Electrónico, SAP, AS400, Citrix, Internet, entre otros, así como también se tiene servicio de comunicación de voz sobre IP usando protocolo H323. Dichas sucursales interconectadas suman alrededor de 120 locales y constituyen una red de tipo full-mesh, es decir, todos los locales pueden comunicarse directamente con todos los locales de cualquier empresa, dependiendo únicamente de la red MPLS, mas no de un punto central o punto intermedio. (Ver Figura 1.1). Esta red corporativa está implementada con una plataforma de routers marca Cisco como equipo de acceso de usuario (CE), los cuales son de diferentes modelos, de acuerdo a las necesidades de cada local, aunque por lo general constan de una interface para conectarse a la red MPLS, que puede ser serial V.35 o FastEthernet; otra interface para conectarse a la red LAN de tipo FastEthernet,

una interface de backup RDSI, V.35 o FastEthemet y también de interfaces de voz que pueden ser de tipo E1, E&M o FXS.

Como se mencionó, dentro de la red existen servidores comunes denominados servidores corporativos, así como también servidores propios de cada empresa. Los servidores de datos que contienen aplicaciones comunes para todas las empresas, como el caso del AS400 y SAP, se encuentran ubicados físicamente en el centro de datos corporativo o nodo central, mientras que los servidores de aplicativos y de correo de cada empresa se ubican en sus propias sedes centrales. El servicio de navegación a Internet también es común para todas las empresas, por lo que se encuentra en modo centralizado, es decir, todos los locales del Grupo conectados a la red, acceden a este servicio por medio del nodo central corporativo, en donde se tiene la salida a Internet mediante un enlace de 10 Mbps. A esta salida a Internet corporativa se le añaden otros servicios, como protección perimetral vía firewall, antispam, webfiltering e IPS.

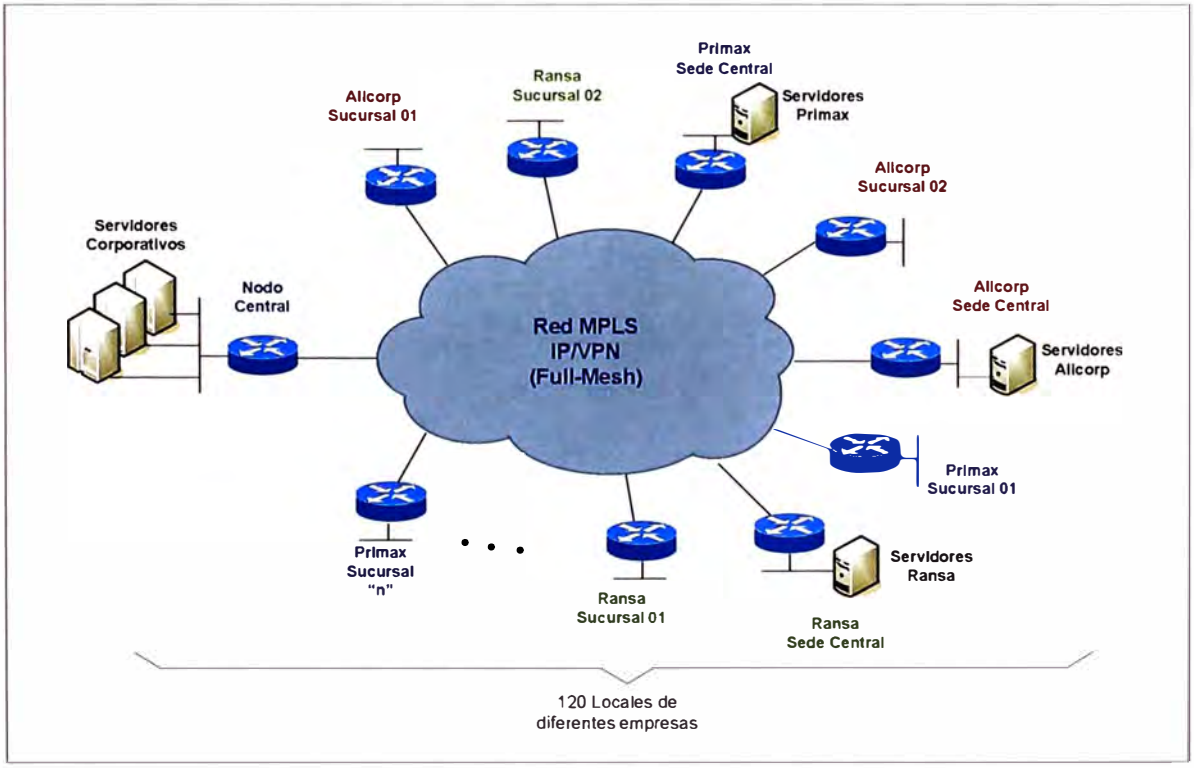


Figura 1.1 Topología de la Red WAN del Grupo Romero

Todos los segmentos de red de cada una de las sucursales conectadas a la red MPLS tienen direccionamiento IP de clase B, pero todas ellas se resumen por el segmento de red 10.0.0.0 /8, es decir, los segmentos de red señalados para cada local remoto son tales como:

- 10.1.0.0 /16
- 10.2.0.0/16

- 10.3.0.0/16, etc.

Así mismo, todos los router de acceso de usuario (CE) conectados a la red WAN IP/VPN, usan como protocolo de enrutamiento RIP y BGP, por medio de los cuales aprenden todas la rutas para llegar a un determinado punto de le red; así mismo, incorporan mediante los mismos protocolos una ruta default 0.0.0.0, que a través de los diferentes saltos de la nube MPLS lleva los paquetes que buscan destino desconocido hacia el nodo principal. De esta forma es que se encaminan todas las peticiones de tráfico hacia Internet, de las diferentes empresas hacia la única salida a Internet ubicada en el nodo central.

Dicha salida a Internet, además de ser usada para la navegación, sirve también para publicar ciertos servidores según los requerimientos de cada una de las empresas, a fin de que éstas puedan ser vistos desde fuera de la red privada, ya sea desde los pequeños locales del Grupo que no cuentan con enlace dedicado, desde empresas terceras o por usuarios remotos que trabajan desde algún punto conectado a Internet.

Respecto a la telefonía dentro de la red corporativa, se tiene una mixtura de centrales telefónicas en las diferentes empresas y sus sucursales del Grupo, que van desde centrales tradicionales TDM, de marcas tales como Nortel, Samsung, Norstar, Alcatel y Panasonic hasta centrales IP de marca Nortel y Cisco. Dichas centrales tienen diferentes capacidades de acuerdo a las funcionalidades requeridas en cada local y están conformadas por elementos que por lo general se agrupan en:

Anexos, que pueden ser de tipo analógicos, digitales o IP; la cantidad depende del tamaño de la sucursal

Líneas Troncales, que van conectadas a la red de telefonía pública y se usan para llamadas a terceros.

Líneas de Interconexión, que se usan para conectar la central al router y proveer de comunicación corporativa, pueden ser de tipo E1, E&M, o también líneas troncales; en las centrales IP se usan líneas conocidas como troncales IP y que van directamente conectadas a la red LAN.

Esta comunicación corporativa se da a través de la red de datos; cuando un usuario quiere llamar a otro anexo de la red de la compañía, marca desde su anexo un código para tomar línea corporativa (líneas de interconexión), es decir, salida hacia los canales de voz del router, luego marca el número de anexo destino y el router lo envía hacia su ubicación final. Cuando los usuarios se quieren comunicar entre anexos de la misma ubicación física y que dependen de la misma central, no necesitan marcar un código, sino llaman directamente marcando el anexo destino.

La comunicación de voz sobre la red de datos se da mediante protocolo H323 y dependiendo qué dispositivo origine la llamada, se tiene dos plataformas de comunicación de voz, la primera conformada por routers Cisco con canales de voz tradicionales (E1, E&M o FXS) y la segunda, conformada por Centrales IP de marca Nortel. Cuando se desea establecer una comunicación entre dos dispositivos de la misma plataforma, la llamada se establece directamente, pero cuando se desea establecer una comunicación entre dos dispositivos de diferentes plataformas, la llamada debe pasar por un punto de paso conformado por un router Cisco y una Central IP Nortel unidas por una interface E1 (Ver Figura 1.2). Esto de debe a que bajo H323 no se ha podido interconectar dispositivos Cisco con Nortel. El detalle de ese tema no es cubierto en el presente trabajo.

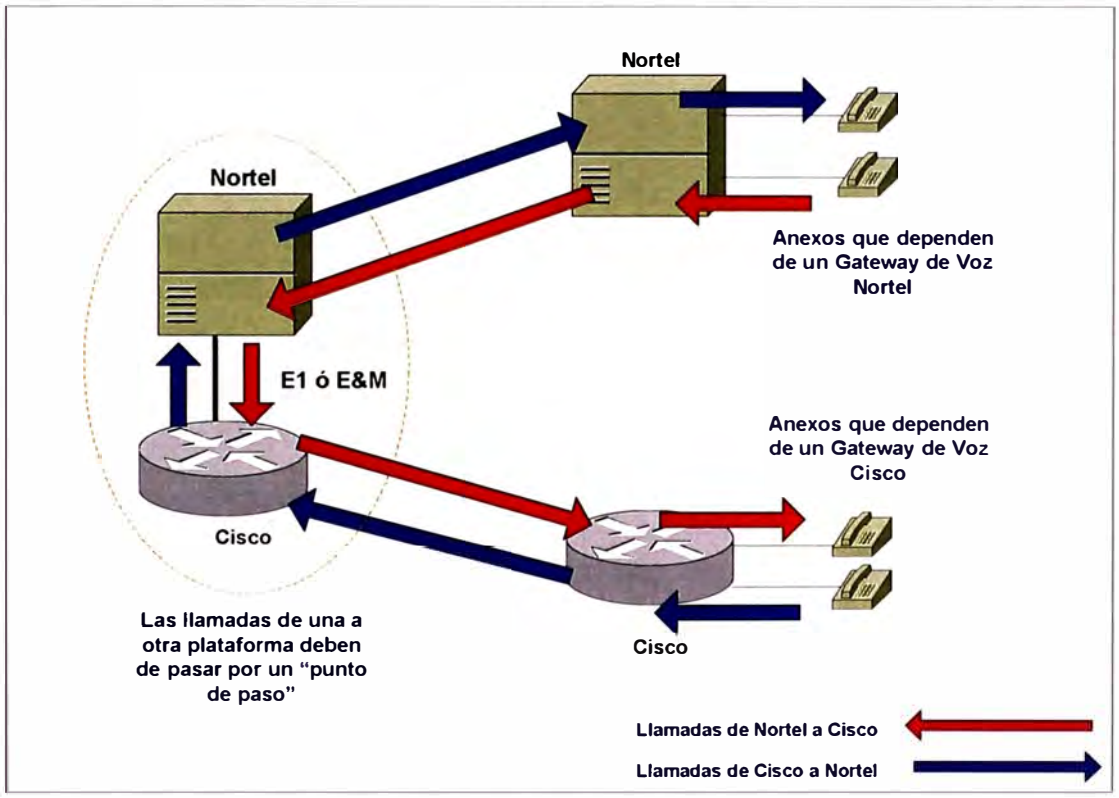


Figura 1.2 Tránsito de llamadas entre las plataformas Nortel y Cisco existentes.

Es importante mencionar además que cada una de las dos plataformas descritas hace uso de un Gatekeeper de su propia marca para manejar el plan de numeración de anexos corporativos. Dichos Gatekeepers se encuentran ubicados físicamente en el nodo central de la red.

Por otro lado, en el nodo central de la red corporativa se tenía ya operando un servicio de VPN, pero limitado a modo en acceso remoto, mediante el cual usuarios remotos que contaban con software cliente VPN en su PCs o PDAs, establecían una conexión hacia la red privada. Este servicio estaba siendo brindado por medio de un

equipo Concentrador VPN de marca Cisco modelo 3015, ubicado en el nodo central y que estaba conectado a la salida del Internet corporativo; este servicio generalmente era usado por personal de ventas que se movilizaba continuamente y necesitaba acceso seguro a la red, así como también por personal técnico que requería dar soporte desde una ubicación remota, como podía ser desde su domicilio o cualquier punto similar que tenga una salida a Internet; también tenían acceso a este servicio los gerentes de las empresas o algunos usuarios especiales que requerían este tipo de conexión. El segmento de red que se les asignó a estos usuarios remotos, es la 172.18.10.0/24 y 172.18.11.0/24. La cantidad total de usuarios que usaban este servicio sumaban alrededor de 80.

1.1.3 La Necesidad Tecnológica

Como se mencionó previamente, existían locales pequeños que ingresaban por medio de Internet a ciertos servidores publicados en el nodo central. Inicialmente este medio de acceso sólo era utilizado por empresas terceras y algunas sucursales pequeñas de provincia que no contaban con un enlace dedicado hacia la red corporativa, pero con el rápido crecimiento de varias empresas del Grupo y su expansión internacional, fueron utilizando esta modalidad de acceso los usuarios de sucursales ubicadas fuera del Perú, específicamente, las situadas en los países de Ecuador y El Salvador. Si bien inicialmente no se tuvo mayores problemas en usar este esquema, ya que la cantidad de usuarios que requerían ingresar a los servidores de Perú en cada local era pequeña, conforme aumentaron en número y volumen de tráfico, los requerimientos adicionales y la necesidad de tener una integración completa a la red se hizo muy necesaria. Bajo esta modalidad de acceso, los usuarios de estos locales sólo estaban limitados a ingresar a los servidores publicados, no podían ver otros servidores o dominios de la red corporativa, no tenían conexión al Directorio Activo ni tampoco podían ver directorios compartidos de otros usuarios, por lo que básicamente, el intercambio de archivos lo realizaban por medio de correo electrónico, con el consiguiente problema de saturar sus buzones de correo y discos duros, independientemente de la molestia en sí, de tener que generar los correos para cada solicitante que necesite el archivo. De la misma forma, tampoco podían ingresar a la intranet ni tener en línea información valiosa, como publicaciones corporativas, comunicados, encuestas electrónicas, acceso al directorio corporativo, entre otros.

Otro problema de gran envergadura, era el hecho de no poder tener comunicación de voz corporativa a través de la red: para comunicarse con las sedes centrales u otras sucursales de Perú, lo tenían que hacer por medio de la red de telefonía pública (PSTN),

con el consiguiente costo por llamadas de discado directo internacional. Este punto se hizo aun más notorio al crecer la cantidad de operaciones de las empresas y requerir una comunicación fluida con sus sedes centrales.

Así mismo, otro problema y sobre todo el más importante de todos, era el gran riesgo que estaba corriendo las empresas al estar cursando tráfico de datos entre sus sucursales remotas internacionales y la red privada de Perú, de forma totalmente desprotegida por medio del Internet. Como es sabido, el hecho de contar con un firewall en el nodo central, solamente protegía el ingreso o salida de conexiones mas no los paquetes de datos durante su curso, los cuales siguen diferentes trayectorias al viajar por la red pública Internet.

Como se mencionó, las sucursales que presentaban el problema descrito se encontraban ubicadas en los países de Ecuador y El Salvador; posteriormente el requerimiento tecnológico se amplían para sucursales ubicadas en Colombia y Guatemala, los cuales ingresaban también a los servidores centrales mediante una salida a Internet, con la particularidad de que de cierta manera, estaban algo más protegidos, pues las PCs y equipos de usuario tenían direcciones privadas y salían a Internet mediante un translación de direcciones que les hacía el router del proveedor. Las direcciones privadas que manejaban no tenían ninguna relación con las direcciones privadas de la red corporativa y solo tenían implicancia a nivel local. Tal es así, que en más de una sucursal las direcciones privadas se repetían.

En resumen, el problema presentado era la desintegración que tenían las sucursales remotas internacionales del Grupo Romero con la red corporativa existente, tanto en voz como en datos y a la vez el peligro en el que estaban inmersos, al estar cursando datos desprotegidos por medio del Internet (Ver Figura 1.3). Los locales remotos involucrados con tal problemática eran los que se muestran en la Tabla 1.1.

Tabla 1.1 Locales a ser integrados a la red corporativa

N°	Empresa	País	Ubicación	Ancho de Banda	Usuarios
1	Ransa	Ecuador	Guayaquil	256 Kbps	22
2	Ransa	Ecuador	Quito	256 Kbps	10
3	Ransa	Guatemala	Guatemala	1 Mbps	18
4	Ransa	El Salvador	Nejapa	1 Mbps	25
5	Ransa	El Salvador	Merliot	1 Mbps	70
6	Alicorp	Ecuador	Santa Leonor	1.2 Mbps	95
7	Alicorp	Ecuador	Quito	1.5 Mbps	66
8	Alicorp	Ecuador	Guayaquil	256 Kbps	12
9	Alicorp	Colombia	Bogota	512 Kbps	43
10	Primax	Ecuador	Guayaquil	1.5 Mbps	37

1.2 Objetivos del Trabajo

El objetivo del proyecto consistía en interconectar las sucursales remotas del Grupo Romero ubicadas en el extranjero, hacia la red nacional ya existente. Esta integración debería permitir cursar de manera protegida y segura todos los servicios, tanto de datos como de voz, haciendo uso para tal fin, la red Internet como medio de enlace.

Tal integración se debería ver reflejada en que los usuarios de los locales remotos internacionales puedan conectarse con toda la red privada de datos y por otro lado, tener comunicación de voz a nivel corporativo, lo cual les permita reducir los costos por llamadas internacionales.

Así mismo, la infraestructura desplegada debería tener la capacidad de crecimiento a futuro sin incurrir en mayores costos de inversión.

1.3 Evaluación del Problema

Si bien el problema presentado puede haberse catalogado como un conjunto de requerimientos de comunicación hasta cierto punto usuales y que de cierto modo eran consecuencia lógica del crecimiento de la red corporativa, se encontraba de por medio un problema que no era perceptible para el usuario final del sistema, pero que constituía el punto más importante de todos y era el de estar cursando tráfico de datos desprotegido por el Internet. Al analizar estos requerimientos y necesidades de comunicación, se anticipa que éstos podrían ser cubiertos con diferentes alternativas tecnológicas, pero dentro de las cuales debería tener especial ponderación la que contemplase la seguridad como uno de sus principales aspectos dentro del despliegue final.

En este punto, la seguridad de los datos de varias empresas del Grupo estaban en gran riesgo, que de haber ocurrido un incidente de interceptación de dicha información cursada, habría ocasionado cuantiosas pérdidas económicas. Es así que el problema de comunicación inicial y la necesidad de integración de las sucursales remotas, pusieron en evidencia la seguridad de la información, sobre la cual en la solución final se debería tener que cubrir, principalmente, tres aspectos importantes, como son:

- Confidencialidad, para asegurar que los datos no sean vistos por terceros con o sin intención de hacerlo.
- Integridad, para asegurar que los datos no sean modificados por personal no autorizado.
- Disponibilidad, para garantizar que los datos siempre estén disponibles cuando se soliciten por personal autorizado.

Así mismo, el problema de seguridad de datos cursados, nos hacía enfocar además, nuestra atención en la seguridad perimetral de los locales remotos, ya que éstos, en su mayoría, tenían una conexión directa a la red Internet sin ningún tipo de filtro de por medio. Como se sabe, cualquier computadora conectada a la Internet constituye un hueco de seguridad y está propenso a muchos tipos de ataques por parte de delincuentes informáticos que circulan en la Internet en búsqueda de redes vulnerables o desprotegidas.

Otra falencia en la que se venía cayendo como consecuencia de la falta de integración a la red corporativa de las sucursales remotas, era que éstas no contaban con atención del Help Desk Corporativo, al que sí tenían acceso el resto sucursales de todas las empresas. Por lo tanto, no tenían soporte técnico eficiente y directo para resolver sus problemas de hardware o software que se presentaban en sus equipos de oficina, como computadoras, impresoras, escaners, etc. Con lo cual tampoco tenían un sistema de control de incidentes, ni estadísticas qua ayuden a hacer un seguimiento de los eventos o a determinar recurrencia de fallas, tipos de averías por equipo, por usuario, etc., menos aun, índices que ayuden a minimizarlas.

Respecto al problema de integración a la red de voz corporativa, se debían tener presente que Alicorp estaba adquiriendo centrales IP Nortel para sus sucursales internacionales, lo cual facilitaba de cierto modo, la integración con la red de Perú, ya que si se resolvía del problema de integración de la red datos, la solución de voz se enfocaba básicamente, a la configuración de dichas centrales IP, puesto que a nivel de capa de red éstas eran como un dispositivo más conectado en la red LAN.

Otro factor a considerar en al solución del problema, era el factor tiempo, ya que la actividad de las operaciones de las sucursales remotas había ido en aumento y la necesidad de integración a la red corporativa era de mucha urgencia y necesitaba ser resuelta cuanto antes.

De la misma manera, un aspecto importante era el económico, ya que si bien no se tenía un tope de presupuesto, se debía minimizar los costos para la resolución de los problemas expuestos. En ese aspecto, se debería considerar los equipos con los que se contaba ya instalados en la red, a fin de incluirlos como parte de la solución final. Por el lado de los locales remotos, ninguno de ellos tenía equipos de comunicaciones propios como routers o firewall, tan solo contaban con switches para la red LAN y los routers que venían usando para la salida a Internet, eran arrendados al proveedor de servicios de Internet (ISP).

1.4 Limitaciones del Trabajo

Si bien es cierto, en teoría, bajo la solución final se podrían lograr un acceso total a la red privada levantando VPNs desde cualquier punto conectado a Internet, se debe tener en cuenta que la calidad y performance de los servicio de red cursados van a estar limitados por el desempeño de la red Internet, porque al ser éste un medio público, no se tiene control de los elementos intermedio para poder habilitar QoS de extremo a extremo, lo cual sí se lograría en un red totalmente controlada. En ese sentido, es posible dar ciertas prioridades a los paquetes al momento de ser enviados a la nube Internet, pero no se garantiza que éstos tengan un adecuado tratamiento en su trayecto, ya que éstos puedan ser encolados o descartados indebidamente por dispositivos intermedios que no manejen calidad de servicio o no reconozcan los paquetes marcados.

Un punto adicional que limita el buen desempeño constituyen los anchos de banda usados y el control de tráfico de navegación hacia Internet que se debe tener de los usuarios, que en muchos casos hacen uso indebido de este servicio usando aplicaciones de tipo P2P que saturan el enlace de acceso y dado que el VPN se monta sobre éste, se verá también afectado. De la misma forma y en modo paralelo, están los elementos de software indeseados que se instalan en las PCs, como los virus troyanos, spams, etc., que de manera similar a los programas P2P, van a congestionar el ancho de banda de acceso.

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1 Red Privada Virtual (VPN)

Una Red Privada Virtual, conocida comúnmente como VPN por sus siglas en inglés Virtual Private Network, es la tecnología que permite establecer un servicio de red privada sobre una infraestructura de red pública o compartida, tal como el Internet.

Para tal propósito, se puede hacer uso de diferentes protocolos, tales como IPSec, GRE, L2TP, MPLS, SSL, entre otros, aunque de todos ellos, los VPNs basados en IPsec son los más seguros y preferidos en las implementaciones actuales, como es el caso del proyecto descrito en el presente trabajo, por lo que nos enfocaremos en dicho protocolo.

2.1.1 Tipos de VPN

Fundamentalmente los VPN se pueden clasificar de acuerdo a las entidades involucradas para la conexión VPN, es así que tenemos tres tipos generales de VPN (1):

VPN acceso remoto

VPN Site-to-Site

VPN por Firewall

a. VPN Acceso Remoto

Un VPN Acceso Remoto es el que se establece bajo la modalidad de cliente servidor. Es decir, un cliente VPN remoto realiza una conexión hacia un servidor o Gateway VPN central con el cual establece la VPN. Son típicos de este tipo de conexiones, los caso donde los usuarios remotos que desde su casa u oficina pequeña se conectan a su sede principal para ingresar a la red como si estuviesen físicamente en la misma oficina central. Así mismo, usan esta modalidad usuarios móviles que desde sus PDAs o computadoras portátiles se conectan a su red privada mediante un VPN.

En el caso de Cisco, el software instalado en el equipo remoto es el denominado VPN Client, el cual no necesita licencia para ser instalado en el equipo del usuario.

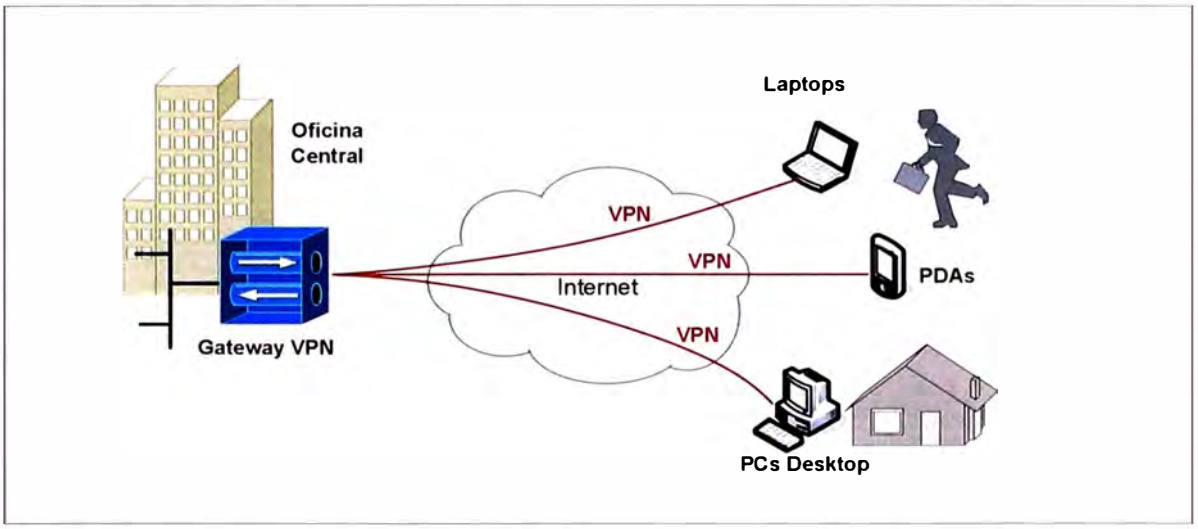


Figura 2.1 VPNs Acceso Remoto

b. VPN Site-to-Site

Es un tipo de conexión VPN que se establece entre dos Gateways VPN para proteger el tráfico entre dos o más redes, por lo que este tipo de conexiones se les conoce comúnmente como conexiones Lan-to-Lan o L2L. El proceso de protección y el transporte entre los dos dispositivos Gateways VPN es transparente para los equipos de los usuarios finales en los dos locales.

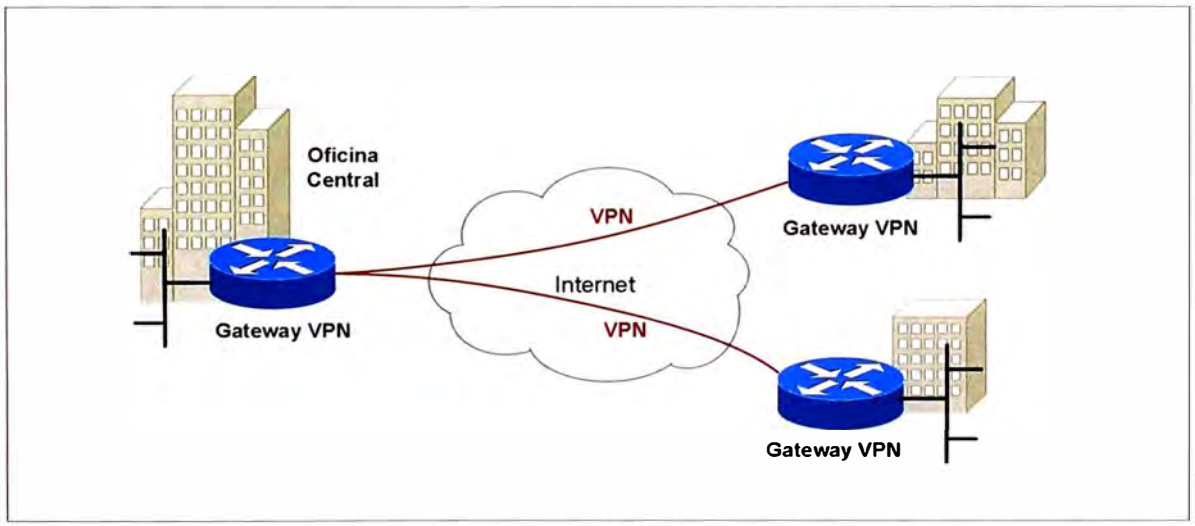


Figura 2.2 VPNs Site-to-Site (L2L)

c. VPN por Firewall

Este tipo de conexión VPN, es básicamente la misma que el VPN Site-to-Site con la particularidad que los Gateways VPN vienen a ser Firewalls.

2.1.2 Protocolos usados para implementar VPNs

Como ya se mencionó, los protocolos más usados para la implementación de VPNs son los siguientes: GRE, IPsec, PPTP, L2TP, MPLS y SSL.

Para establecer una conexión VPN, cada uno de ellos opera en diferentes niveles del modelo OSI, como se puede apreciar en la siguiente Figura 2.3, donde se muestran algunos ejemplos (2).

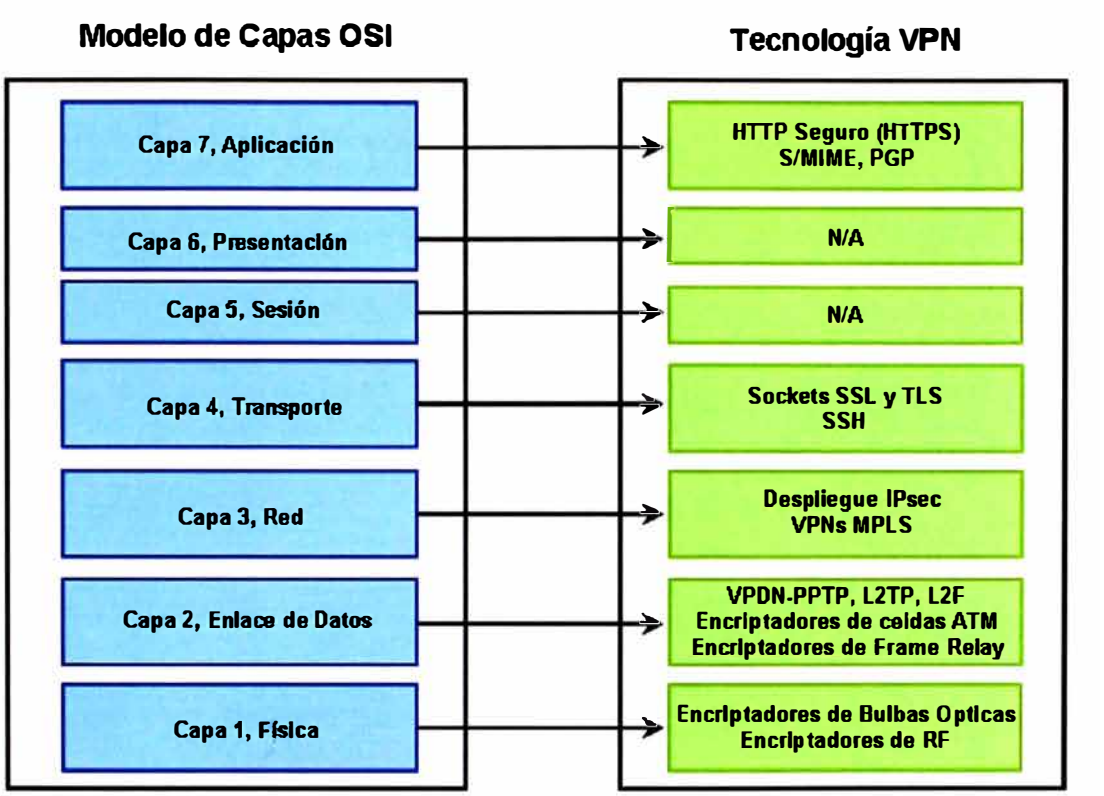


Figura 2.3 El Modelo OSI y la Tecnología VPN

2.2 IPSEC.-

IPSec (Internet Protocol Security) es un conjunto de estándares que fueron creados para proporcionar servicios de seguridad a la capa IP, dotándole de mecanismos de encriptación, los cuales se integran dentro de los paquetes IP, proveyéndoles de autenticidad, integridad y confidencialidad de datos. IPsec se acopla fácilmente con IP versión 4 y viene ya incorporado con IP versión 6. (3)

Una implementación de IPsec funciona en un host o en un security gateway (SG), proporcionando protección al tráfico IP. La protección ofrecida se basa en requerimientos definidos en el establecimiento de una "Base de Datos de Políticas de Seguridad" (SPD) y mantenidas por un usuario o administrador del sistema o por una aplicación, funcionando dentro de las restricciones ya establecidas.

Los servicios de seguridad IPsec se dan en la capa IP por medio de la selección de protocolos de seguridad apropiados, algoritmos criptográficos y claves criptográficas. IPsec puede ser usado para proteger una o más trayectorias entre un par de host, entre un par de gateways de seguridad o entre un gateway de seguridad y un host.

Los dos principales grupos de estándares que IPsec usa son:

ISAKMP/IKE/Oakley/SKEME. Estos estándares son usados para establecer una conexión de administración segura; determinan información para intercambio de claves para encriptación y usa firmas para autenticación de la conexión de administración. Esta conexión es usada para que los dos entes IPsec puedan intercambiar mensajes uno con otro.

AH y ESP. Estos estándares son usados para proveer protección a los datos de usuario. Estos pueden proveer confidencialidad (solo ESP), integridad de datos, autenticación de origen de datos y servicios anti réplica (4).

Antes de pasar a ver con más detalle estos protocolos, se debe conocer cuáles son los modos de conexión IPsec y qué servicios provee cada uno de ellos.

2.2.1 Modos IPsec

IPsec tiene los dos modos siguientes de enviar tráfico a través de una red:

Modo túnel

Modo transporte

Cada uno difiere en su aplicación así como en el promedio de cabecera adicionada al paquete original. Estos modos se describen a continuación.

a. Modo Túnel

El modo túnel trabaja encapsulando y protegiendo un paquete IP completo. Debido a que el modo túnel encapsula u oculta la cabecera IP del paquete inicial, una nueva cabecera IP se añade, de manera que el paquete puede ser enviado satisfactoriamente. El dispositivo de encriptación usa su propia IP para esta nueva cabecera. El modo túnel puede emplearse con cualquiera u ambos protocolos de seguridad IPsec (ESP y AH). En el modo túnel resulta en una expansión adicional del paquete de aproximadamente 20 bytes, debido a la nueva cabecera IP. El modo túnel es considerado mucho más seguro y flexible que el modo transporte, ya que encripta las direcciones IP origen y destino del paquete original, y oculta la información de la red desprotegida.

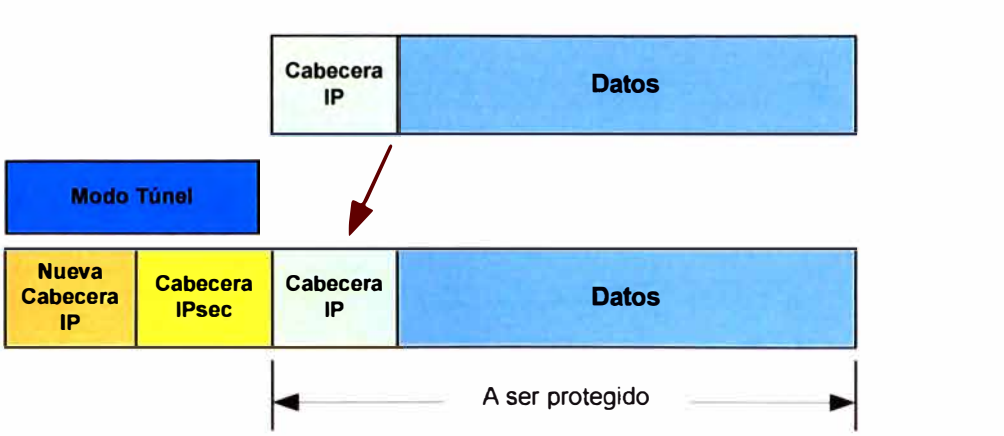


Figura 2.4 IPsec Modo Túnel

b. Modo Transporte

El modo transporte de IPsec trabaja insertando la cabecera AH o ESP entre la cabecera IP y el siguiente protocolo o la capa de transporte del paquete. Ambas direcciones IP de los dos nodos de red cuyo tráfico está siendo protegido por IPsec, son visibles en la cabecera IP del paquete luego de ser encriptado. Este modo de IPsec puede ser susceptible de ataques de análisis de tráfico. Sin embargo, debido a que no se adiciona una cabecera IP, esto resulta en una menor expansión del paquete. El modo transporte puede ser desplegado con los protocolos AH, ESP u ambos. El modo transporte puede ser usado con p2p GRE sobre IPsec, debido a que este diseño oculta las direcciones de las estaciones terminales adicionando su propia IP. Otra limitación del modo transporte, es que ésta no puede ser usada con traslaciones de direcciones (NAT) de paquetes entre entidades IPsec. También, para la mayoría de motores de encriptación por hardware, es menos eficiente encriptar en modo transporte que en modo túnel, debido a que el modo transporte requiere un desplazamiento de la cabecera IP para hacer espacio para la cabecera ESP o AH.

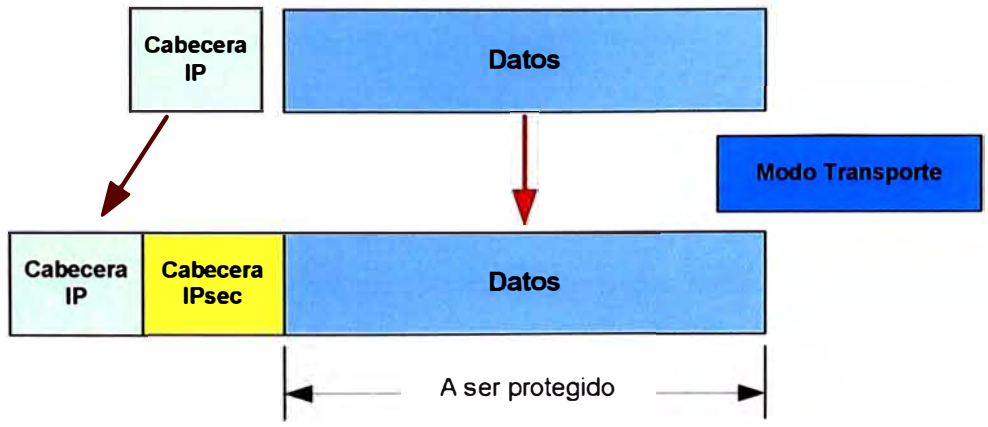


Figura 2.4 IPsec Modo Transporte

2.2.2 Protocolos de Seguridad en IPsec

IPsec usa dos protocolos para proveer servicios de seguridad de tráfico: Authentication Header (AH) y Encapsulating Security Payload (ESP). Las implementaciones con IPsec deben soportar ESP y pueden soportar AH, debido a que la experiencia ha mostrado que hay muy pocos contextos en los cuales ESP no puede proporcionar los requisitos de servicios de seguridad necesitados.

El IP Authenication Header (AH) ofrece verificación de integridad y autenticación de la data origen con la opción de habilitar características anti-replay.

El protocolo Encapsulating Security Payload (ESP) ofrece el mismo grupo de servicios y adicionalmente confidencialidad. El uso de ESP para proveer solamente confidencialidad sin integridad no es recomendada. Cuando se usa ESP sin habilitar la confidencialidad, existen ciertas disposiciones para la confidencialidad de flujo de tráfico limitado.

Tanto AH y ESP ofrecen control de acceso, realizado a través de la distribución de claves criptográficas y administración de flujo de tráfico, de acuerdo a la Base de Datos de Políticas de Seguridad (SPD).

Estos protocolos pueden ser aplicados individualmente o en combinación de uno con otro para proveer servicios de seguridad a IPV4 y IPV6. Sin embargo, la mayoría de los requerimientos de seguridad pueden ser satisfechas mediante el uso de ESP por si solo. Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En modo transporte, AH y ESP brinda protección, principalmente, para protocolos de los próximos niveles; en modo túnel AH y ESP son aplicados a paquetes IP completos.

a. Encapsulating Security Protocol (ESP)

La cabecera ESP (Protocolo IP 50) forma el núcleo del protocolo IPsec. Este protocolo junto con un grupo de parámetros de seguridad acordados o “transform set”, protegen los datos presentándolos indescifrables. Este protocolo encripta solo la porción de datos del paquete y usa otros algoritmos (HMAC) para realizar otras protecciones (integridad de datos, anti-replay, man-in-the-middle). Opcionalmente este puede también proveer autenticación de los datos protegidos. La Figura 2.5 ilustra como ESP encapsula un paquete IP.

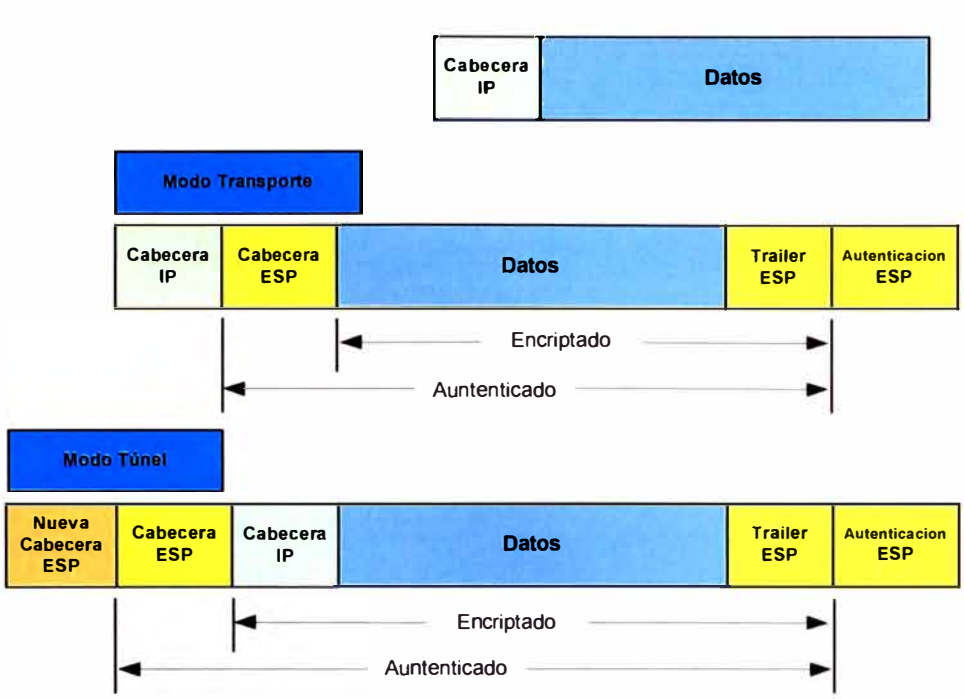


Figura 2.5 Protocolo ESP

b. Authentication Header (AH)

El protocolo AH (Protocolo IP 51) forma la otra parte de IPsec. El AH no encripta datos en el sentido usual de ocultarlos, sino que les adiciona una marca de seguridad para evidenciar si estos han sido leídos. Este también protege los campos no variables en la cabecera IP que transporta los datos, los cuales incluyen los campos de direcciones de la cabecera IP. Cuando existe un requerimiento de confidencialidad de datos de por medio, no debería usarse el protocolo AH solo, sino en combinación con ESP. La Figura 2.6 ilustra como AH encapsula un paquete IP.

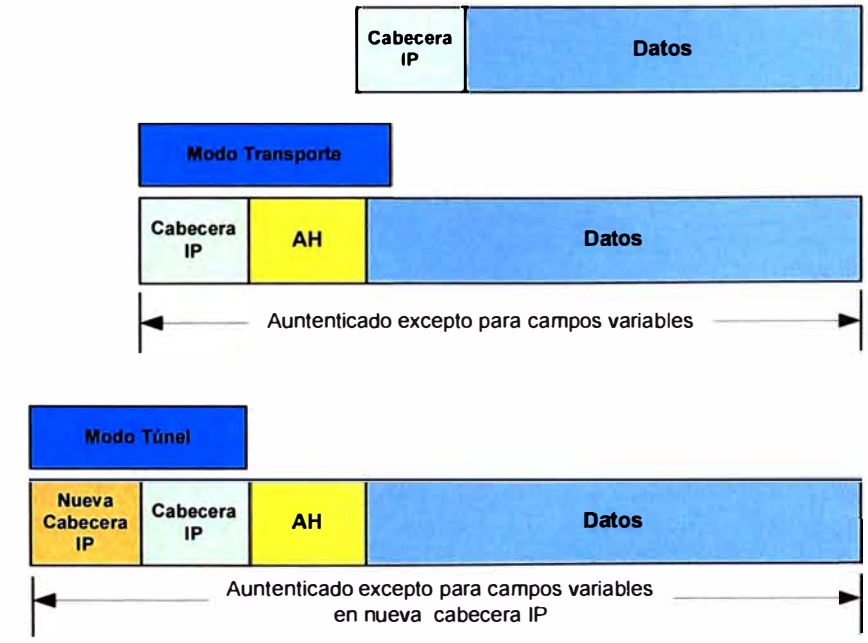


Figura 2.6 Protocolo AH

c. Usando ESP y AH juntos

Es posible usar ESP y AH juntos sobre la misma Asociación de Seguridad (SA) IPsec. ESP incluye la misma autenticación que AH, así como proveer protección y encriptación de datos.

2.2.3 Internet Key Exchange

Para implementar una solución de VPN con encriptación, es necesario que se realicen cambios periódicos de claves de encriptación de sesión. Una falla para cambiar estas claves hace al VPN susceptible de ataques de desencriptación por fuerza bruta. IPsec soluciona este problema con el uso del protocolo IKE, el cual a su vez hace uso de otros dos protocolos para autenticar al otro ente que es parte de la encriptación y generar las claves. IKE usa un algoritmo matemático llamado intercambio Diffie-Hellman para generar claves de sesión simétrica a ser usada por los dos entes encriptadores. IKE también maneja la negociación de otros parámetros de seguridad, tales como los datos ha ser protegidos, la fortaleza de las claves, el método de generación de claves a ser usado y si los paquetes están protegidos de anti réplica. ISAKMP normalmente usa puerto UDP, 500 tanto en el origen como en el destino.

a. Asociaciones de Seguridad (SA)

Una Asociación de Seguridad o Security Association (SA) es un acuerdo entre dos entes que intervienen en una comunicación encriptada. Este acuerdo incluye el tipo y la consistencia del algoritmo de encriptación usado para proteger los datos. El SA incluye el método y la consistencia de la autenticación de datos y el método para crear nuevas claves para tal protección de datos.

Cada SA posee un valor de período de vida (lifetime) para el cual un SA se considera válido. El valor de período de vida es medido, tanto en tiempo (segundos) como en volumen (bytes) y es negociado durante la creación de un SA. Estos dos valores de período de vida son comparados y acordados al menor valor. Bajo circunstancias normales, el valor de período de vida expira en el límite de tiempo antes que el límite de volumen. Así, si un paquete de interés cae en un SA dentro de los últimos 120 segundos de período de vida de un SA activo, se invoca al proceso de revalidación de clave. Luego el proceso de revalidación de clave establece otro SA antes de que el SA existente sea borrado. El resultado es una suave transición hacia el nuevo SA con una pérdida de paquetes mínima.

Asociación de Seguridad ISAKMP

Un ISAKMP SA es un simple canal de negociación segura bi-direccional usado por ambos entes de encriptación para comunicar parámetros de seguridad importantes hacia el otro par de la comunicación, tales como los parámetros de seguridad para el IPsec SA (data túnel).

En Cisco IOS, la política ISAKMP SA tiene como valor por defecto del período de vida de 86400 segundos sin límite por volumen cursado.

Asociación de Seguridad IPsec (Data Tunnel)

Un IPsec SA es un canal de comunicación uni-direccional entre un ente encriptador y otro. Los datos actuales de usuario solo atraviesan un IPsec SA y nunca sobre un ISAKMP SA. Cada lado del IPsec túnel tiene un par de IPsec SAs por conexión; uno al remoto y otro desde el remoto. Esta información del par IPsec SA es grabado localmente en la base de datos SA.

En Cisco IOS, la política IPsec SA tiene como valor por defecto de período de vida de 3600 segundos con un límite de volumen de 4,608,000 Kbytes.

b. IKE Fase Uno

El IKE fase uno es la negociación inicial de un ISAKMP SA bi-direccional ente dos crypto peers, frecuentemente referido como modo principal (main mode). IKE Fase Uno se inicia con una autenticación, en la cual cada crypto peer verifica su identidad con el otro. Una vez autenticados los crypto peers, acuerdan el algoritmo de encriptación, el método hash, y otros parámetros descritos en las siguientes secciones para construir el ISAKMP SA. La conversación entre los dos crypto peers puede estar sujeta a espionaje con un mínimo riesgo de que las claves sean descifradas. El ISAKMP SA es usado por el proceso IKE para negociar los parámetros de seguridad para los IPsec SA. La información del ISAKMP SA es grabado localmente en la base de datos SA de cada crypto peer. La Tabla 2.1 ilustra los diversos parámetros de seguridad definidos en las siguientes secciones.

Pre-Shared Keys

PSK son una cadena de caracteres predefinidos administrativamente en cada Crypto Peer y usadas para identificarse el uno con el otro. Usando el PSK, los dos crypto peers son capaces de negociar y establecer un ISAKMP SA. Un PSK usualmente contiene una dirección IP de host o una subset y una máscara que es considerada válida

para tal particular PSK. Un "wildcard PSK" es un tipo especial de PSK, cuya red y máscara pueden ser cualquier dirección IP.

Tabla 2.1 Parámetros de Seguridad ISAKMP SA.

Default en IOS Cisco	**Autenticación**	**Encriptación**	**HMAC**	**Diffie-Hellman**	**Periodo de vida**	**NAT-T**
Parámetros ISAKMP SA	Firmas RSA (PKI) (default)	DES (default)	SHA-1 (default)	Gupo1 (default)	86,400 segundos Sin límite de volumen (default)	Habilitado (default)
	PSK	3DES	MD5	Grupo 2	Definible por usuario	No habilitado
	RSA nonce	AES 128		Grupo 5		
		AES 192				
		AES 256				

Métodos de Autenticación

IKE fase uno tiene tres posibles métodos de autenticación: Pre-shared KEY (PSK), Public Key Infrastructure (PKI) usando certificado digital X.509 y encriptación RSA. En la presente solo se describen el PSK, pero el diseño es factible con cualquiera de estos métodos de autenticación.

Algoritmos de Encriptación

La encriptación usa diversos algoritmos para realizar esta función. En el núcleo del algoritmo de encriptación se encuentra una clave secreta compartida para autenticar cada peer. Luego de autenticados, se introducen los datos en texto claro en el algoritmo en bloques de tamaño fijo y convertido a texto encriptado. El texto encriptado es transmitido al crypto peer usando ESP. El peer recibe el paquete ESP, extrae el texto encriptado, lo corre a través del algoritmo de desencriptación y saca una salida de texto claro idéntico al que ingreso en el peer de encriptación.

Cisco IOS soporta algoritmos de encriptación DES, 3DES, AES 128, AES 192 y AES 256, con DES asignado como valor por defecto.

Código de Autenticación de Mensajes Hashed (HMAC)

Los principales algoritmos de hash usados por main mode, son funciones criptográficamente seguras, como son Message Digest 5 (MD5) y Secure Hash Algorithm 1 (SHA1). Los algoritmos de hashing se han convertido en Hashed Message Authentication Codes (HMAC), los cuales se combinan demostrando la seguridad de los algoritmos de hashing con funciones de encriptación adicionales. El hash producido es

encriptado con la clave privada del origen, resultando en un chequeo de clave como salida.

Diffie-Hellman.

Diffie-Hellman es un método de encriptación de clave pública que proporciona una forma para que dos crypto peers establezcan una clave secreta compartida que solo ellos dos conocen, mientras están comunicándose por un canal inseguro.

Con Diffie-Hellman, cada peer genera un par de claves pública y privada. La clave privada generada por cada peer es mantenida en secreto y nunca compartida. La clave pública es calculada a partir de la clave privada por cada peer y es intercambiada sobre el canal inseguro. Cada peer combina la clava pública de la otra con su propia clave privada y computa el mismo número secreto compartido. El número secreto compartido es luego convertido en una clave secreta compartida. La clave secreta compartida nunca es intercambiada sobre el canal inseguro.

c. IKE Fase Dos

En IKE Fase Dos, los IPsec SAs son negociados por el proceso IKE usando la ISAKMP SA bi-direcional, a menudo referido como modo rápido o quick mode. Los IPsec SAs son unidireccionales en naturaleza, provocando un intercambio de clave separado para los datos que fluye en cada dirección. Una de las ventajas de esta estrategia es doblar el promedio de trabajo requerido por un espía para recuperar con éxito ambos lados de una conversación. Durante el proceso de negociación en modo rápido, los crypto peer acuerdan los conjuntos de transformación o transform sets, métodos hash y otros parámetros. La Tabla 2 ilustra los diversos parámetros de seguridad.

Tabla 2.1 Parámetros de Seguridad IPsec SA.

Default en IOS Cisco	**Encriptación**	**HMAC**	**PFS**	**Período de vida**	**Modo IPsec**
Parámetros IPsec SA	DES (default)	SHA-1 (default)	Desabilitado (default)	3600 segundos 4´608,000 Kbytes (default)	Modo Túnel (default)
	3 DES	MD5	Grupo 1	Definible por usuario	Modo Transporte
	AES 128		Grupo 2		
	AES 192		Grupo 5		
	AES 256				

Algoritmos de Encriptación

Como en el modo principal, el modo rápido usa un algoritmo de encriptación para establecer los IPsec SAs. El algoritmo de encriptación negociado por el proceso en modo rápido puede ser el mismo o diferente del proceso en modo principal. Cisco IOS soporta algoritmos de encriptación DES, 3DES, AES 128, AES 192 y AES 256, con DES asignado como valor por defecto.

Hashed Message Authentication Codes (Hash)

Como en modo principal, el modo rápido usa un HMAC para establecer los IPsec SAs. El HMAC negociado por el proceso de modo rápido puede ser el mismo o diferente del de modo principal. Tanto MD5 y SHA-1 son soportados con Cisco IOS, con SHA-1 asignado como valor por defecto.

Perfect Forward Secrecy

Si Perfect Fordward Secrecy (PFS) es especificado en las políticas IPsec, un nuevo intercambio Diffie-Hellman se lleva a acabo con cada negociación en modo rápido, proporcionando material con claves que tiene gran entropía (key material life), por lo tanto, una mayor resistencia a los ataques criptográficos. Cada intercambio Diffie-Hellman requiere grandes cálculos exponenciales, incrementando así el uso de CPU y exigentes costos de performance.

En PFS (Diffie-Hellman), los grupos 1, 2 y 3 son soportados con Cisco IOS. PFS es deshabilitado por default. Grupo1 tiene un tamaño de clave de 768 bits, Grupo 2 tiene un tamaño de clave de 1024 bits, y Grupo 5 tiene un tamaño de clave de 1536 bits (5).

2.2.4 Estándares IPsec

La estructura de IPsec está definida en el RFC 4301, sin embargo la implementación de IPsec es definida a lo largo de otros RFCs adicionales, los que se indican a continuación (6):

RFC 4301 Este RFC define el role que el IPsec cumple y un resumen de cómo trabaja. (Reemplazó al RFC2401)

RFC 4302 Este RFC es uno de los dos que define cómo son protegidos los datos de usuario. Este define el protocolo Authentication Header (AH) y puede autenticar y verificar la integridad de los paquetes. (Reemplazó al RFC2402)

RFC 4303 Este RFC define el protocolo Encapsulation Security Payload (ESP) para proveer confidencialidad, autenticación e integridad de paquetes para conexiones de datos. (Reemplazó al RFC2406)

RFC 2403 Este RFC define el uso de MD5 como una función HMAC en conexiones de datos IPsec.

RFC 2404 Este RFC define el uso de SHA-1 como una función HMAC de conexiones de datos IPsec.

RFC 2405 Este RFC define el uso de DES como un algoritmo de encriptación para conexiones de datos.

RFC 4306 Este RFC define el protocolo Internet Key Exchange, el cual es usado para negociar y autenticar información de claves para proteger las conexiones. (Reemplaza a RFCs 2407, 2408 y 2409)

Adicionalmente, existen otros RFCs definidos para IPsec, pero los que se han mencionado son los principales. La lista completa de RFCs pueden ser encontrados en la página web de la IETF (http://www.ietf.org).

CAPITULO III
DISEÑO E IMPLEMENTACIÓN DE VPNs CON ENCRIPTACIÓN IPSEC

3.1 Alternativas Previas de Solución

Una vez que ya se tenía consolidada la necesidad existente y teniendo claro los objetivos buscados, se pasaron a revisar rápidamente alternativas que puedan dar solución a los problemas presentados.

La primera alternativa surge casi de manera inmediata y era el de contratar enlaces dedicados internacionales para conectar cada uno de los locales hacia el nodo central del Grupo en Perú y de esta forma, puedan tener en cada una de las sucursales todos los servicios con los que se contaba en la red que ya opera a nivel nacional. Se solicitaron algunas propuestas técnicas y económicas a algunos proveedores de este tipo de servicio, tales como Telefónica Internacional, Infonet, Equant e Impsat. Como es lógico con este tipo de solución, sí se lograba una integración completa a la red corporativa y se tendría un comunicación privada y segura, pero luego de una rápida evaluación esta forma de conexión fue puesta en espera por el alto costo de inversión que significa contratar este tipo de enlaces, tanto en el pago por instalación inicial como en la renta mensual. Adicionalmente, se encontró la desventaja que ciertos proveedores de este servicio de enlaces dedicados no contaban con los correspondientes permisos de regulación de telecomunicaciones en algunos países para cursar tráfico de voz sobre enlaces de datos, lo cual limitaba la solución y por lo tanto, no se lograría cubrir la totalidad de los objetivos planteados.

Como segunda opción, se tenía la alternativa de crear portales seguros para cada uno de los servidores ubicado en Perú y publicarlos en Internet, mediante el cual las sucursales remotas accedieran a realizar sus operaciones. Esto resultaba una alternativa más económica que la primera, pero tenía la gran limitante de que solamente se iba poder acceder a ciertos servidores de datos y que además, para poder llegar a su implementación, tenía que pasar por un fase previa de validación, diseño y desarrollo de cada uno ellos, lo cual dilataba el tiempo en que se podía tener la solución. Así mismo, otra desventaja de esta alternativa era que el servicio de voz corporativa quedaría restringido, por lo que para realizar las llamadas se tendría que seguir haciendo uso de la de telefonía pública, es decir, mediante Discado Directo Internacional, lo cual generaría

costos adicionales que se iban a seguir asumiendo de manera permanente cada vez que se realicen las llamadas, con lo cual los objetivos trazados no podían ser cumplidos en su totalidad.

Como tercera alternativa, surge la opción de replicar la misma solución VPN en modo acceso remoto que se tenía para las pequeñas sucursales en el Perú y para acceso de terceros, la cual era el de instalar software con clientes VPN en cada una de las PCs de la sucursal que deseaban acceder a la red privada. Esta solución tenía la ventaja de ser relativamente rápida para ser implementada y con la cual el usuario, por un lado lograría poder ver a toda la red corporativa, y por otro lado, proteger todas las transacciones de datos que realice desde su PC a los servidores o dispositivos de la red interna, los paquetes iban a ser encriptados y protegidos por el software VPN. La desventaja de esta alternativa era que no se iba a contar con comunicación de voz corporativa, por lo que no se lograría alcanzar los objetivos en este aspecto. Otro inconveniente presentado, era que la cantidad máxima de sesiones VPN en modo acceso remoto que soporta el concentrador Cisco VPN 3015 es 100 y dado que en ese momento ya se tenían alrededor de 80 sesiones simultáneas casi permanentes, al adicionar este servicio para todas las PCs remotas de los locales internacionales, la capacidad del Concentrador VPN iba a desbordar rápidamente y por lo tanto, tampoco se tendría una solución flexible y con capacidad de crecimiento futuro.

Como consecuencia natural de las alternativas anteriores, surge la cuarta alternativa, que era el de realizar conexiones VPN en modo Lan-to-Lan entre el nodo central y cada una de las sucursales remotas. Esta solución les permitiría a dichos locales tener conexión a toda la red privada de manera segura y protegida, con lo cual todos sus usuarios podrían acceder a todos los servidores o equipos de la red corporativa y tener todos los servicios de datos y voz, tal como si estuviesen conectados mediante enlaces dedicados. Si bien es cierto que esto implicaría un costo inicial de implementación por el equipamiento de hardware requerido, éste se compensaría rápidamente con un retorno de inversión en pocos meses, debido a que en este caso ya no se contratarían líneas dedicadas, sino solamente se haría uso de las líneas de acceso a Internet con las cuales ya venían operando hasta el momento. Así mismo, dado que con esta solución se emulaba tener circuitos dedicados, se podría fácilmente integrarlos a la red de voz corporativa, tan solo adicionando el hardware necesario, ya sea en los mismos equipos que haría la VPN, disponiendo de gateways de voz o usando Centrales IP. Esta implementación les permitiría lograr grandes ahorros por costos de llamadas internacionales que se venían dando para comunicarse con las sucursales de Perú.

Además, esta solución tenía la ventaja de que no sería necesario adquirir equipamiento adicional en el lado central, puesto que se podía usar el concentrador VPN 3015 existente. A diferencia de la anterior alternativa, en este caso, por cada sesión VPN Lan-to-Lan del concentrador VPN viajaría la comunicación de todas las PCs de la sucursal remota, con lo cual solo se usaría una licencia IPsec del concentrador VPN por cada local remoto.

3.2 Descripción del Proyecto Ejecutado

Luego de evaluadas las alternativas presentadas, se pudo concluir que la más adecuada para alcanzar los objetivos propuestos y resolver los problemas de comunicación existentes, era la implementación de conexiones VPN en modo Lan-to-Lan con cada una de las sucursales remotas.

Por lo tanto, luego que se recabó información detallada de la red existente que ya fue descrita en el Capitulo I, se pasó a desarrollar dicha solución siguiendo básicamente las siguientes etapas:

Diseño y Planeamiento

Implementación

Verificación y Afinamiento

Los cuales se pasan a explicar a continuación:

3.2.1 Diseño y Planeamiento

En primer lugar, se parte del hecho de que ya se contaba en el nodo central con el equipo concentrador VPN de marca Cisco modelo VPN 3015, el cual como ya se dijo venían operando para dar servicio de VPNs en modo acceso remoto a usuarios, quienes mediante un software cliente de Cisco establecían una conexión VPN a la red privada, como se ve en la Figura 3.1

Estos usuarios, generalmente eran personal móvil de las áreas de ventas, soporte técnico o algunos usuarios de empresas terceras que necesitaban ingresar a los servidores de algunas de las empresas del Grupo; así mismo, también tenían acceso algunos usuarios especiales que contaban con autorización para conectarse a la red privada. Esta situación marcó el punto de partida, ya que se deseaba aprovechar este equipo concentrador VPN existente para recibir también las conexiones VPN L2L desde los locales remotos.

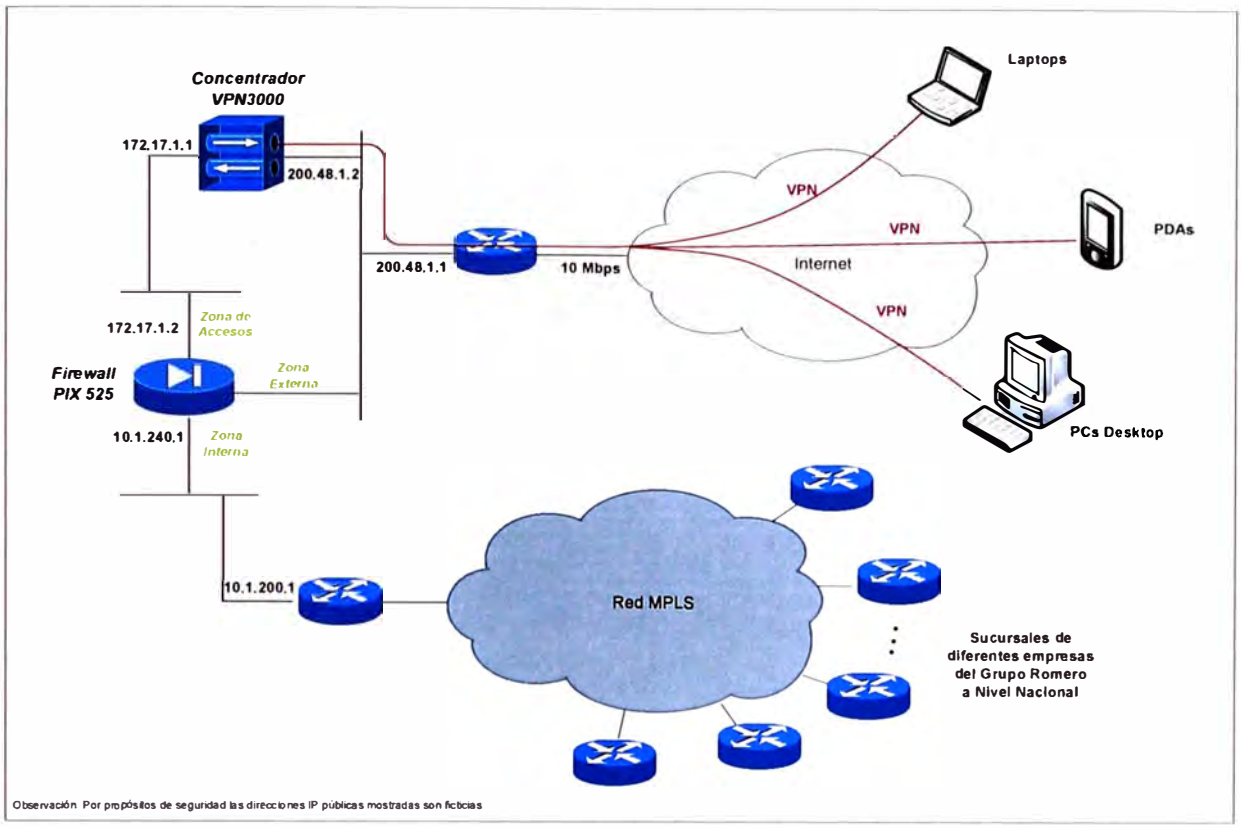


Figura 3.1 Plataforma VPN inicial que solo cubría modo acceso remoto

Lo que se debía tener en cuenta era que la cantidad máxima de sesiones IPsec que soportaba dicho equipo concentrador era de 100 y hasta ese momento ya se tenía inscrito 80 usuarios para acceso remoto VPN, con lo cual el número de conexiones en determinado momento podía superar la capacidad del equipo y por otro lado, la capacidad de crecimiento para futuras conexiones sería limitada. Por tal motivo, si se deseaba seguir usando dicho equipo, se le debería realizar un upgrade de hardware, añadiéndole un módulo SEP (Scalable Encryption Processing) para subir a un modelo VPN 3030, el cual permitiría tener hasta 1500 sesiones IPsec simultáneas, como se muestra en detalle en el anexo A.3. Otra ventaja de realizar este upgrade, sería que con el módulo SEP la encriptación se realizaría por hardware y ya no mediante software, como venía sucediendo con el concentrador VPN 3015. Este aspecto era muy importante, pues se sabe que el proceso de encriptación por hardware es más rápido que el que se realiza por software y considerando que se necesitaba pasar voz sobre el enlace, sería muy útil para reducir el retardo de los paquetes.

Por otro lado, se sabía que por información del fabricante Cisco. que sus concentradores VPN podrían establecer conexiones VPN con diversos fabricantes de equipos similares, pero se determinó que a fin de facilitar la interconexión, el dispositivo Gateway VPN que se use en las sucursales sea también de marca Cisco.

En ese sentido y de acuerdo a las opciones que brindaba Cisco, se podría usar en el local remoto uno de las siguientes tipos de equipos:

Concentrador VPN Serie 3000

Router Cisco con IOS para VPN

Firewall PIX o ASA

El primero de ellos quedó descartado porque era un dispositivo básicamente orientado para ubicarlo en un nodo central mas que en una oficina remota y además, porque no manejaba canales de voz y se conocía que era más costoso comparado con las otras dos opciones. Según las recomendaciones que hace Cisco en sus manuales de información técnica, la forma más eficiente de realizar una conexión VPN L2L es por medio de sus routers, por lo que se concluyó que éste sería el tipo de dispositivo indicado para ser usado en las sucursales remotas de las empresas para la implementación; los routers tenían además la ventaja de poder incorporarles los canales de voz para el manejo de las llamadas corporativas. En el caso de Ransa y Primax, esta opción fue aceptada sin mayor inconveniente, pero en el caso de Alicorp, esta empresa quería darle mayor prioridad a la seguridad, por lo que preferían usar un Firewall para establecer el VPN en lugar de router, además de que en dicha empresa no necesitarían routers con canales de voz, puesto que como ya se mencionó, estaban adquiriendo centrales telefónicas IP, las cuales enviaría las llamadas directamente por la red de datos que se implemente. En vista de ello, se tuvo que considerar la solución con ambos tipos de dispositivos, tanto router como firewall para operar como dispositivo Gateway VPN en los locales remotos.

Luego de elegido el tipo de dispositivo a usar en los locales remotos para establecer los VPNs, se pasó a determinar el modelo a usar en cada clase, para lo cual era preciso saber cuántas interfaces y de qué tipo se necesitaría en cada local remoto. Es así que básicamente se necesitaba que el equipo tenga 2 interfaces Ethernet, una para conectarse hacia el router de salida del ISP y la otra para conectarse hacia la red LAN interna de la sucursal. Para los casos donde se usaría un router (Ransa y Primax), éste debía tener además 2 interfaces de voz FXS, donde conectar los aparatos telefónicos para las llamadas por la red corporativa; en los casos donde se usaría Firewalls (Alicorp), la voz se manejaría directamente desde las centrales IP. Con estas consideraciones y teniendo en cuenta el throughput que nos ofrecen los diferentes modelo de equipos, finalmente los elegidos para la implementación del VPN en las sucursales remotas fueron los routers Cisco 2801 y para los locales que usarían Firewalls el modelo PIX 506E. El anexo A muestra la relación completa de los modelos de dispositivos que ofrece Cisco para este fin y una comparación de sus capacidades.

Otro punto a considerar en el diseño de los VPNs, es el tipo de conectividad o topología de conexiones VPN L2L que se va a tener entre los locales de la red involucrada. Se sabía que cada uno de los locales remotos requería, principalmente, tener conexión hacia el nodo central de Perú por medio del cual y a través de la red nacional llegaba a su oficina principal, pero dado que por otro lado también era necesario que tengan conectividad entre algunas sucursales internacionales de la misma empresa, básicamente se llegó a conformar el diseño como una red en modo Hub-and-Spoke, con ciertas conexiones adicionales. Es decir, que todos y cada uno de los Gateway VPN remotos establecería una conexión VPN hacia el Concentrador del nodo central en Perú y adicionalmente, según se requiera, se deberían establecer otras conexiones VPN entre dos o más sucursales determinadas de la misma empresa. La forma en que finalmente quedaron conformadas las conexiones VPN se muestra en la Figura 3.3.

Como siguiente punto, se debería determinar el tipo de tráfico que sería protegido o enviado por la conexión VPN y dado que lo que se requería era que la sucursal remota vea toda la red privada sin restricción de segmentos, puertos o aplicaciones, se concluía que el tráfico a ser protegido debería ser todo lo que se curse a nivel de direcciones privadas, mientras que el tráfico que la sucursal haga hacia o desde Internet debería ser enviado a la salida a la nube sin encriptación, es decir, por fuera del túnel, en otras palabras, la navegación y salida a la Internet de cada sucursal remota se debería dar directamente por su propio enlace mas no por medio de la salida de Internet corporativa que se tenía en el nodo central de Perú. Para este propósito, los dispositivos VPN de cada local remoto, ya sea router o firewall, serían configurados para realizar la separación del tráfico, enviando la comunicación privada por la conexión VPN y el tráfico a Internet directamente a la nube mediante un NAT, tal como se muestra en la Figura 3.2.

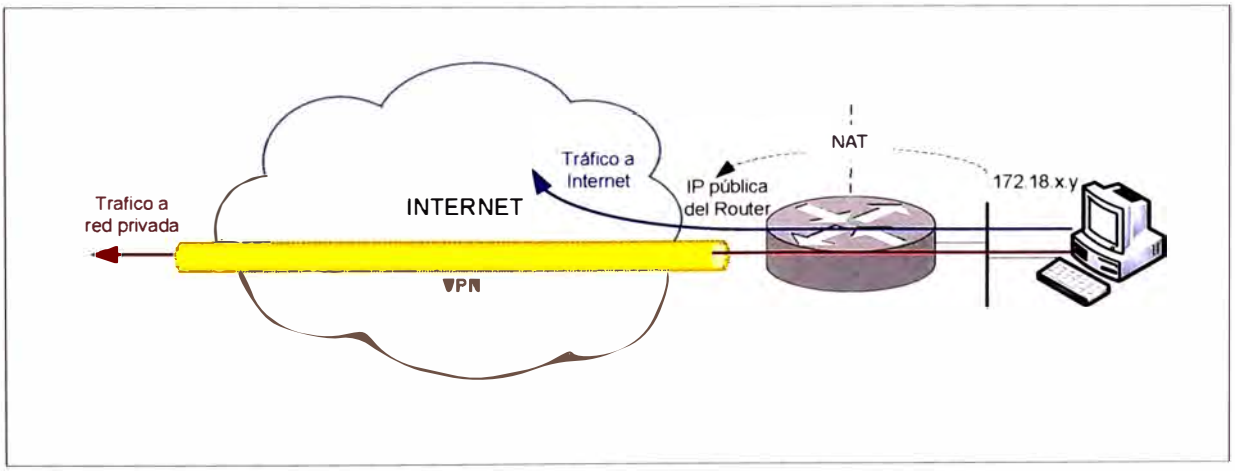


Figura 3.2 Separación de tráfico que debe hacer el Gateway VPN (Router o Firewall)

Luego de definido los dispositivos a usarse y el sentido de flujo de tráfico, se pasó a definir un plan de direccionamiento IP privado para cada una de las sucursales y dado que ya se venía usando el segmento IP 172.18.10.0/24 y 172.18.11.0/24 para los VPNs en modo acceso remoto, se optó por usar clases similares, sobre todo para mantener un orden en el enrutamiento y debido también a que en el Firewall de seguridad perimetral ubicado en el nodo central se tenían bien diferenciado el direccionamiento de sus zonas y la zona de accesos por donde ingresarían los VPN L2L tenía la ruta 172.18.0.0 ya configurada, de tal manera que se les asignó los siguientes segmentos de red según las empresas:

Red Ransa: 172.18.100.0/24

Red Primax: 172.18.120.0/24

Red Alicorp: 172.18.150.0/24

Cada una de dichas redes luego serían segmentadas para asignárselos a cada uno de los locales remotos de cada empresa, teniendo en cuenta el número de host existentes en cada local. A medida que iban ingresando las sucursales remotas por medio de VPNs, se les fue dando subrangos de dichas clases, esto, a fin de facilitar la administración y gestión de la red. Es así que se tuvo las siguientes redes mostradas en la tabla 3.1.

Tabla 3.1 Direcciones de red asignadas para cada uno de los locales remotos.

N°	Empresa	País	Ubicación	Red	Mascara
1	Ransa	Ecuador	Guayaquil	172.18.100.0	255.255.255.224
2	Ransa	Ecuador	Quito	172.18.100.64	255.255.255.240
3	Ransa	Guatemala	Guatemala	172.18.100.96	255.255.255.224
4	Ransa	El Salvador	Nejapa	172.18.100.128	255.255.255.224
5	Ransa	El Salvador	Merliot	172.18.101.0	255.255.255.0
6	Alicorp	Ecuador	Santa Leonor	172.18.150.0	255.255.255.128
7	Alicorp	Ecuador	Quito	172.18.151.0	255.255.255.128
8	Alicorp	Ecuador	Guayaquil	172.18.151.128	255.255.255.224
9	Alicorp	Colombia	Bogota	172.18.150.128	255.255.255.192
10	Primax	Ecuador	Guayaquil	172.18.120.0	255.255.255.192

Como siguiente punto del diseño se debería determinar los parámetros a ser configurados en los Gateway VPN para establecer las conexiones VPN. Como se menciona en el título del presente trabajo y en la introducción del mismo, el protocolo que se ha usado par implementar los VPNs a sido IPsec, debido principalmente a:

Es uno de los protocolos más difundidos para las implementaciones de VPN Lan-to-Lan.

- Tal protocolo realiza la protección de los paquetes a nivel de red, lo que da la ventaja de poder proteger cualquier protocolo de las capas superiores.
- El equipo concentrador VPN 3000 maneja solamente IPsec para conexiones de tipo L2L.

Por lo tanto, se debía definir ahora los parámetros IPsec a configurarse.

En primer lugar, se debería especificar las redes entre las que se tenía que establecer las conexiones IPsec, en el caso de esta implementación, dichas conexiones se establecerían entre la red privada del Grupo y la red privada de la sucursal remota.

Se debe tener en cuenta que tales segmentos de red se definen en los dos equipos entre los que hace el túnel VPN, pero se debe tomar como referencia el equipo que se está configurando, es decir, por ejemplo para el caso del VPN con Ransa Guayaquil se tenía de la siguiente forma:

En el Router de Ransa Guayaquil:

- Red local: 172.18.100.0 Máscara 255.255.255.224
- Red remota: 10.0.0.0 Máscara 255.0.0.0

En el Concentrador VPN 3000 del Nodo Central:

- Red local: 10.0.0.0 Máscara 255.0.0.0
- Red remota: 172.18.100.0 Mascara 255.255.255.224

Por lo tanto, para dicha sucursal el tráfico que fluya entre estas dos redes sería encriptado y enviado por la conexión VPN. Este proceso en los Routers y Firewall Cisco se define generalmente mediante listas de acceso (ACLs) y el Concentrado VPN mediante la opción de Listas de Red (Network List). Esta definición de redes es muy importante y se debe tener especial cuidado al configurarlas, pues una diferencia en la declaración de ellas en los Gateways VPN puede ocasionar que la conexión VPN no levante.

Luego pasamos a determinar cómo se protegerá a la conexión de administración (ISAKMP/IKE Fase 1) y cómo se protegerá a la conexión de datos (ISAKMP/IKE Fase 2). Para definir los parámetros de esta parte debemos tener en cuenta que en cualquier nivel, cuanto más complejo y seguro sea el protocolo elegido, mayor será también el uso de los recursos del dispositivo Gateway VPN. Es decir, cuanto más seguro y menos vulnerable sea nuestra conexión VPN, el consumo de CPU y memoria será también más alto, por lo cual se debe proceder con cautela y llegar a un buen equilibrio entre ambos aspectos. Lógicamente no existe una regla precisa para alcanzar tal balance, pero si no se está seguro de la capacidad del equipamiento, se recomienda empezar eligiendo los parámetros de encriptación menos complejos.

En el Anexo B se muestra un diagrama de flujo que puede ayudar cuando se realiza el diseño de esta parte de la implementación. Para el caso de nuestra solución desarrollada, los Routers y Firewalls venían con cantidad de memoria bastante encima del promedio por lo que eligieron los siguientes parámetros generales:

IKE Fase 1

- Tipo de Autenticación de dispositivo: pre-shared key
- Función HMAC: MD5
- Algoritmo de encriptación: 3DES
- Grupo Diffie-Helman: 2
- Período de vida de conexión: 86400 segundos (default)

IKE Fase 2

- Tráfico a ser protegido (ACLs): Depende de cada ubicación
- IPsec peer: Dirección IP del otro extremo del VPN
- Protocolo de Seguridad: ESP
- Función HMAC: MD5
- Algoritmo de encriptación: 3DES
- Modo de conexión: Túnel
- Período de vida de conexión: 4608000 Kbytes. (default)

Para poder definir estos parámetros, así como en otros casos, es importante tener presente cómo se establece una conexión IPsec, la cual sigue, básicamente, la siguiente secuencia:

- Se necesita que alguien active el proceso de conexión IPsec. Esto ocurre cuando uno de los Gateway requiere enviar tráfico que necesita ser encriptado con destino hacia el otro Gateway IPsec que se encuentra en el otro extremo.
- Si aun no existe conexión VPN, IPsec usará ISAKMP/IKE Fase 1 para establecer una conexión de administración segura, la cual es usada para que los dos Gateway puedan comunicarse entre ellos por un canal seguro, y a su vez, puedan establecer canales de datos seguros.
- A través de una conexión segura, los dos Gateways IPsec negociarán los parámetros de seguridad que serán usados para establecer las conexiones de datos seguro, las cuales son usadas para transmitir datos de usuario.
- Una vez que las conexiones de datos han sido establecidas, los Gateways IPsec pueden usarlos para cursar datos de usuario de manera segura.

Tanto la conexión de administración como las de datos, tiene un período de vida asociados con ellos. Esto asegura que el intercambio de claves se vuelva a generar cada cierto tiempo para proveer mayor seguridad, en caso de que alguien esté intentando vulnerar dichas claves de seguridad. Cuando se alcanza el período de vida de la conexión, ésta es desconectada. Si luego se requiere enviar datos, la conexión se restablecerá dinámicamente.

Respecto a la solución de comunicación de voz corporativa, en el caso de las sucursales de Ransa y Primax los routers Gateways VPN funcionarían también como Gateways de voz, por lo que fueron adquiridos con 2 canales de voz FXS, con el propósito de ser conectados directamente a aparatos telefónicos, los que funcionarían como anexos corporativos o en algunos casos, para ser conectados a sus respectivas centrales telefónicas ya existentes vía puertos troncales de éstas.

En el caso de Alicorp, como se mencionó anteriormente, esta empresa estaba adquiriendo para sus sucursales internacionales, centrales telefónicas IP de marca Nortel modelo BCP50 y BCM400, por lo que para la integración de éstas a la red corporativa sólo bastaba que tengan conectividad a nivel IP con el gatekeeper Nortel de su sede central y también con las demás centrales IP que ya tenían operando en Perú.

Como se mencionó anteriormente, la red corporativa de voz en Perú estaba constituida por una mixtura de routers Cisco y Centrales IP Nortel, cada uno con su propio gatekeeper centralizado, ambas plataformas en protocolo H323, pero que solamente se comunicaban directamente entre dispositivos de la misma marca. Para comunicación desde una sucursal con router Cisco hacia una con central IP Nortel o viceversa se hacía uso de puntos de paso, que consistían de un router y una central unidos por interfaces de tipo E1.

Para la incorporación de las sucursales a la red de voz corporativa, en primer lugar, se debió definir el plan de numeración de anexos a seguir, el cual tuvo que basarse según el plan de numeración corporativo que ya existía en la red nacional. Luego se revisó qué gateway de voz se iba a usar para generar o recibir las llamadas de voz sobre IP, las cuales además, debían usar protocolo H323, a fin de que puedan interactuar con la red de voz ya existente. En ese contexto se tenían dos formas de interconexión: el caso de Ransa y Primax, que usarían el router de VPN para operar también las llamadas actuando como gateway de voz, mediante 2 canales FXS y el caso de Alicorp, el cual tendría centrales telefónicas IP para generar o recibir las llamadas en H323. Respecto a la numeración de anexos, para el caso de Alicorp se definió un rango completo de anexos, ya que además requerían tener una marcación transparente, es decir, cuando los llamen desde otra sede debería timbrar directamente en el anexo destino.

Por lo tanto, se definió el plan de numeración que se muestra en la Tabla 3.2 y el diseño de la solución finalmente quedó plasmado como se muestra en el diagrama adjunto de la Figura 3.3

Tabla 3.2 Rangos de anexos asignados a los locales remotos

N°	Empresa	País	Ubicación	Rango de Anexos	Canales de voz
1	Ransa	Ecuador	Guayaquil	2282 -2283	2 FXS
2	Ransa	Ecuador	Quito	2284 – 2285	2 FXS
3	Ransa	Guatemala	Guatemala	2286 – 2287	2 FXS
4	Ransa	El Salvador	Nejapa	2288 – 2289	2 FXS
5	Ransa	El Salvador	Merliot	2280 – 2281	2 FXS
6	Alicorp	Ecuador	Santa Leonor	5600 – 5699	4 IP Trunk
7	Alicorp	Ecuador	Quito	5700 – 5799	4 IP Trunk
8	Alicorp	Ecuador	Guayaquil	5800 – 5819	4 IP Trunk
9	Alicorp	Colombia	Bogota	5820 – 5821	2 FXS
10	Primax	Ecuador	Guayaquil	3307 – 3308	2 FXS

Se debe notar que la cantidad de canales de voz simultáneos que pueden tener en cada local en el caso de FXS, se refiere a lo permitido por el hardware del router, mientras que en le caso de IP Trunk se refiere a la cantidad de canales simultáneos que puede transmitir la central IP hacia otra central o gateway de voz.

3.2.2 Implementación

En esta etapa de la ejecución del proyecto, se verificó cualquier pequeño detalle que haya pasado por alto en alguna de las etapas previas y se determinó cómo, dónde y de qué manera se desplegaría el desarrollo de la solución. Se debe tener en cuenta que en esta etapa se tiene la última oportunidad de identificar algún riesgo que se pueden tener al implantar la solución dentro de la red existente.

De esta forma, en el desarrollo de la implementación, básicamente, se ha seguido la siguiente secuencia:

a. Instalación y configuración básica de Gateway VPN remoto
b. Configuración de VPN L2L entre Concentrador VPN3000 y Gateway VPN
c. Migración de red pública a red privada
d. Integración de la sucursal remota a la red de voz corporativa

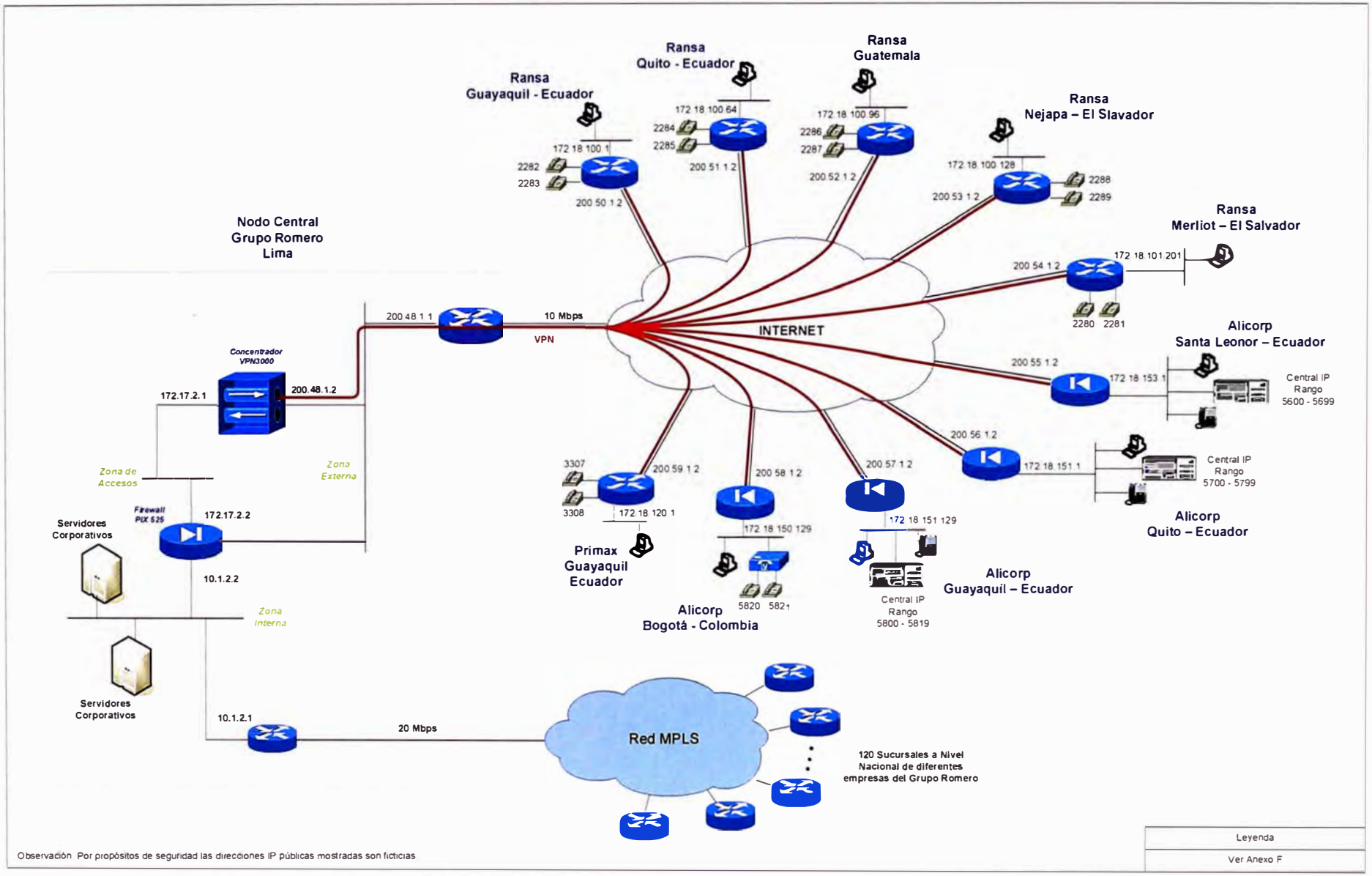


Figura 3.3 Solución de VPN L2L propuesta

a. Instalación y configuración básica de Gateway VPN remoto

La primera tarea desarrollada durante el despliegue de la solución, fue la instalación y configuración básica del dispositivo VPN de la sucursal. Esta labor se ejecutó de manera remota desde Perú, básicamente, por un tema de tiempo y presupuesto. Es así que tan solo se contó con la ayuda de una persona de apoyo en cada una de las sucursales. Para ejecutar esta labor también fue necesario tomar en cuenta que los trabajos que se realizarían deberían impactar lo menos posible en la continuidad de las operaciones de la sucursal, ya que si bien en cierto modo, hasta ese momento los usuarios sólo accedían a los servidores centrales por medio del Internet, las transacciones eran casi continuas, sobre todo en los locales de almacenes de Ransa y distribuidoras de Alicorp.

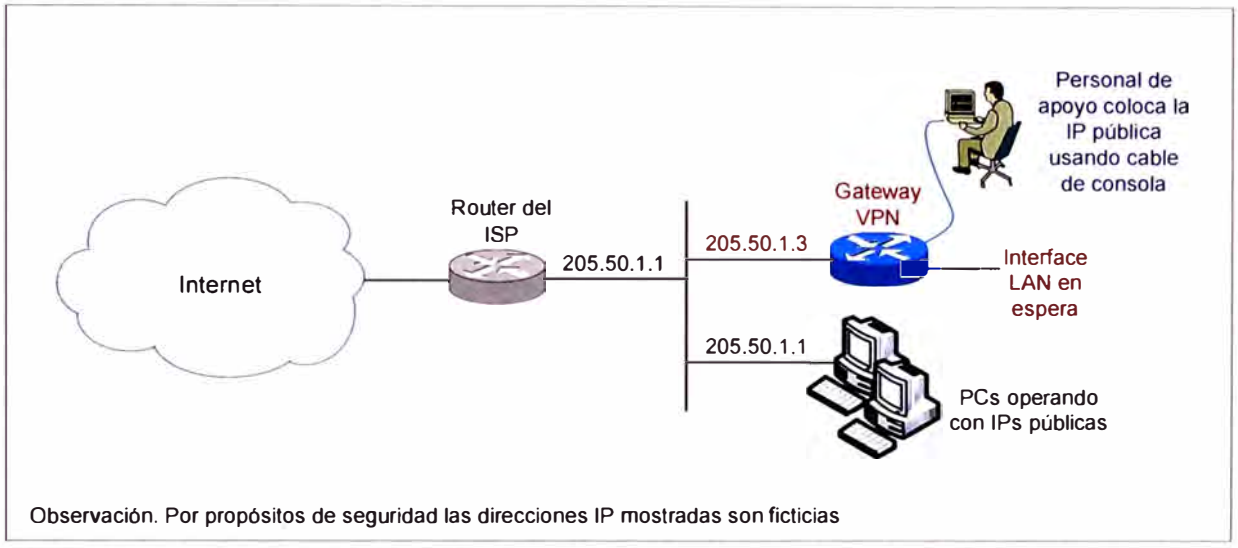


Figura 3.4 Instalación inicial de Gateway VPN en el local remoto

Bajo esta premisa y sin hacer ningún cambio en la red, se colocó el Gateway VPN (router o firewall) en la red LAN de la sucursal, tal igual como si fuese un dispositivo más de esa red, configurándole tan sólo una dirección IP (pública) del rango correspondiente a tal segmento. Para el caso de los locales que usaron el router Cisco 2801 como Gateway VPN, se eligió la interface Fastethernet 0/1 para ser usada para dicho fin, denominándola a su vez interface externa, mientras que la interface Fastethernet 0/0, a la cual se le denominó interface interna, quedó en espera para recibir la conexión de la nueva red LAN privada, como se muestra en la Figura 3.4.

En el caso de los locales de Alicorp que usaron como dispositivo VPN a un Firewall Cisco PIX 506E, se usó la interface denominada como externa (outside) para conectarlo a la LAN existente y configurarle una dirección IP pública, mientras que la interface denominada como interna (inside) quedó en espera de recibir la nueva red LAN privada.

Una vez dispuesto el Gateway VPN de esta manera, ya se pudo tomar control remoto de dicho dispositivo desde Perú y realizar el resto de la configuración avanzada, que además del VPN L2L, consistió en hablitar las funcionalidades de enrutamiento, firewall o listas de acceso para protección perimetral.

b. Configuración de VPN L2L entre Concentrador VPN3000 y Gateway VPN

Teniendo ya el control del dispositivo de la sucursal en modo remoto, se pasó a realizar la configuración del VPN L2L propiamente dicho y enlazarlo con el Concentrador VPN 3015 del Nodo central de Perú.

Según los parámetros dados en la etapa de diseño, se pasó a configurar los dispositivos VPN, a fin de establecer las conexiones VPN L2L, tanto en el concentrador VPN 3015 como en el dispositivo VPN remoto (Router o Firewall).

Considerando que estos equipos ya tienen la configuración básica de red, en general, para establecer el túnel IPsec, se siguen las siguientes secuencias de configuración en cada uno de ellos:

b.1 Concentrador VPN 3000:

En este caso, antes de proceder a la configuración, se realizó el upgrade de hardware, instalándole el módulo SEP para subir del modelo 3015 que se tenía al modelo 3030, luego se siguió, en general, con los siguientes pasos:

- Crear los "Network List" donde se especifica las redes ha ser protegidas. Se debe inscribir tanto la red del lado local como del lado remoto.
- Verificar si existe como predefinido el conjunto de parámetros para IKE Fase 1 que necesitamos, de lo contrario, crear dicho conjunto en "IKE Proposals"
- Crear un nueva conexión Lan-to-Lan, ingresando a "IPsec Lan-to-Lan", dentro de la cual se definirán:
    - Parámetros de configuración básica L2L
    - Peer o Gateway VPN del otro extremo del túnel
    - Información sobre autenticación del dispositivo
    - Políticas de la conexión
    - Opciones de enrutamiento
    - Redes local y remota
- Verificar las Asociaciones de Seguridad creadas.

b.2 Router Cisco 2801

- Definir políticas para IKE fase 1, donde se indican los parámetros para proteger la conexión de administración IPsec. Se configura ingresando dentro del nivel la línea de comando "crypto isakmp"
- Definir el tráfico que necesita ser protegido; esto se realiza mediante la configuración de listas de acceso (ACL).
- Definir cómo se protegerá el tráfico de la conexión de datos IKE fase 2. Esto se realiza mediante definición de un conjunto de parámetros denominados "transform sets".
- Definir a dónde debería enviarse el tráfico, interrelacionando a su vez los ACL, transform sets e interface por donde se establecerá el IPsec VPN.

b.3 Firewall Cisco Pix 506 E

- Especificar listas de acceso que permitan establecer la conexión VPN
- Definir políticas para IKE fase 1, donde se indican los parámetros para proteger la conexión de administración IPsec.
- Especificar el tráfico a ser protegido mediante listas de acceso.
- Definir cómo se protegerá el tráfico de la conexión de datos IKE fase 2. Esto se realiza mediante definición de un conjunto de parámetros denominados "transform sets".
- Definir a dónde debería enviarse el tráfico, interrelacionando a su vez los ACL, transform sets e interface por donde se establecerá el IPsec VPN.

Un ejemplo de configuración entre un Concentrador VPN 3000 y un router Cisco se muestra en detalle en el Anexo D.

Así mismo, los procedimientos detallados de configuración de estos equipos se describen en los enlaces externos del fabricante Cisco indicados a continuación:

VPN L2L entre un Concentrador VPN 3000 y un router Cisco:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008009482e.shtml

VPN L2L entre un Concentrador VPN 3000 y un Firewall Cisco PIX:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a008064a06f.shtml

c. Migración hacia la nueva red privada

Luego de establecido ya la conexión VPN entre el nodo central y la sucursal remota, se procedió a pasar todos los dispositivos de la red LAN pública hacia la nueva red interna que ahora era privada y se le colocó el direccionamiento señalado en la Tabla 3.1. Dado el planeamiento realizado que se viene describiendo, esta migración resultó sencilla y con tiempos muertos de comunicación mínimos, que básicamente era el tiempo que se demoraba en cambiarle de dirección IP a la PC y pasar el cable de red al nuevo segmento, teniendo además, la ventaja de poder hacerlo paulatinamente de PC en PC, tal como se muestra en la Figura 3.5. A medida que se iba migrando cada host, también se realizaban pruebas de comunicación de datos hacia sus diferentes sucursales de Perú, que antes de implementar el VPN no podían ser vistos.

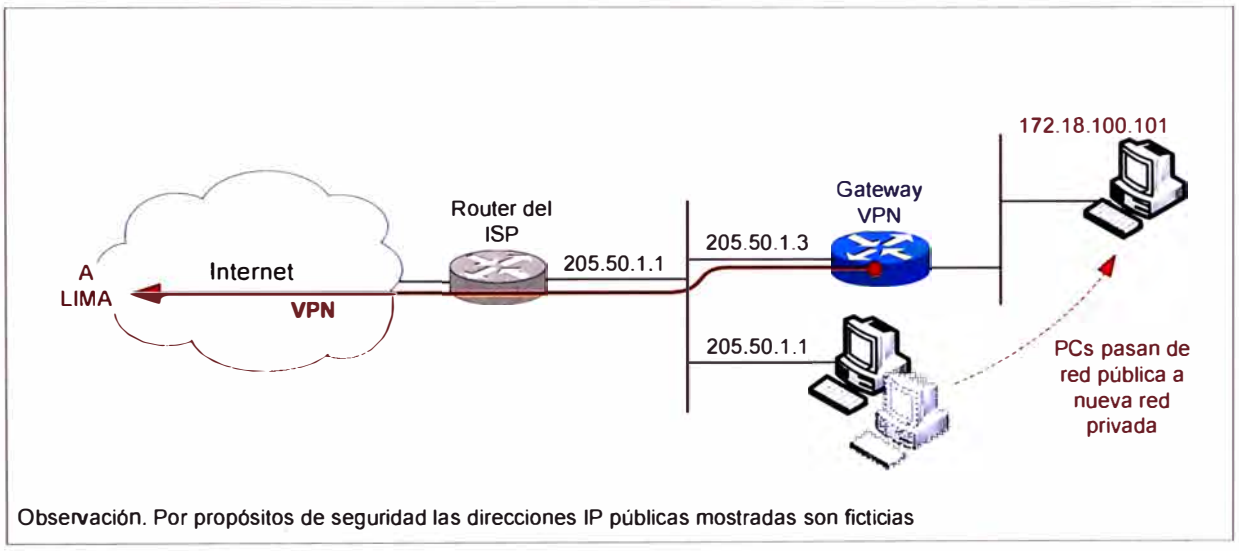


Figura 3.5 Cambio paulatino de las PCs de la pública a la nueva red privada

d. Integración de la sucursal remota a la red de voz corporativa

Una vez que ya se tenía operando el VPN y con las PCs del local remoto cursando tráfico privado, seguro y protegido, se pasó a incorporar la sucursal a la red de voz corporativa, para lo cual, según el plan de numeración asignado, se configuró los canales de voz del router o la central IP, según sea el caso. Para realizar esta labor fue necesario coordinar con el soporte técnico de las centrales telefónicas.

En el caso de los locales de Ransa y Primax, cuyos Gateway VPN eran los routers Cisco 2801 con 2 canales de voz FXS, se conectaron directamente a dichos puertos 2 aparatos telefónicos análogos y se procedió a configurar dichos puertos según la numeración de anexos asignados en la Tabla 3.2; así mismo, dado que el router ya pertenecía a la red privada, se realizó el enrutamiento de voz correspondiente hacia el resto de la red de voz corporativa. (Figura 3.6)

Como se mencionó en la situación inicial de la red, todos los routers de voz Cisco existentes se registran en un Gatekeeper Cisco ubicado en el nodo central de la red, el cual maneja el plan de numeración corporativo. Es así que cada vez que el router remoto quiere realizar una llamada, hace la consulta al Gatekeeper para ver a dónde envía la llamada. Para el caso de las sucursales internacionales, no se ha hecho uso de dicho Gatekeeper para evitar un retardo prolongado en el establecimiento de las llamadas; en su lugar se ha configurado el router Cisco con tablas de enrutamiento de voz internas denominadas "dial-peer".

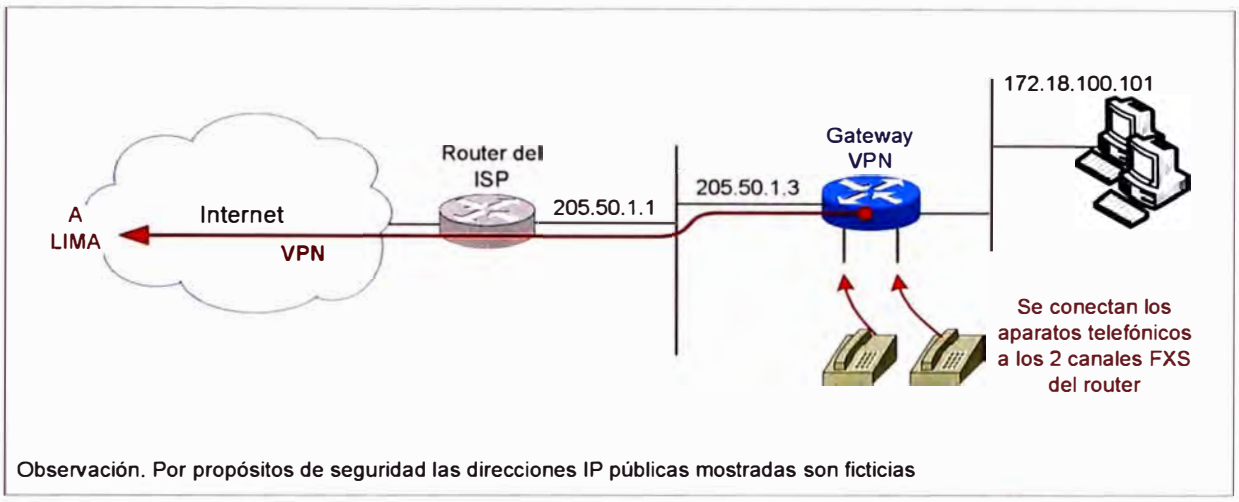


Figura 3.6 Modo de conexión de canales de voz en Ransa y Primax

Para el caso de Alicorp, donde se tenía planificado la instalación de Centrales IP, se conectó este dispositivo en la red LAN con una dirección IP privada del nuevo segmento de red; lo propio se hizo con los teléfonos IP que se instalaron en cada uno de dichos locales, como se muestra en la Figura 3.7.

Figura 3.7 Modo de conexión de canales de voz en Alicorp

Esta etapa de instalación de Centrales IP formó parte de otro proyecto, por lo que no se entra en mayor detalle al respecto, pero es importante mencionar que al igual que los routers Cisco, se determinó que las Centrales IP también hagan uso de sus tablas de enrutamiento de voz internas en lugar de usar el Gatekeeper central de Perú, a fin de evitar una mayor demora en el tiempo de establecimiento de las llamadas.

3.2.3 Verificación y Afinamiento

Luego de implementadas las conexiones VPN, se realizaron las verificaciones correspondientes, tanto a nivel de los Gateway VPN que intervienen en la conexión como también realizando pruebas a nivel de usuario desde su PCs hacia los servidores o viceversa.

Tanto el Concentrador VPN, el router y el firewall tienen internamente componentes que ayudan a verificar la operatividad del las conexiones VPN así como también a realizar diagnósticos, si es que fueran necesarios.

Tomando el caso de la primera implementación de VPN L2L realizada, que es el caso de Ransa Guayaquil, se muestran algunas de las pantallas de verificación que se pueden obtener.

En el lado de concentrador VPN 3000, se pude apreciar la conexión VPN establecida, donde a su vez se muestra tanto la sesión IKE (Fase 1) y las sesiones IPsec (Fase 2). Ver Figura 3.9.

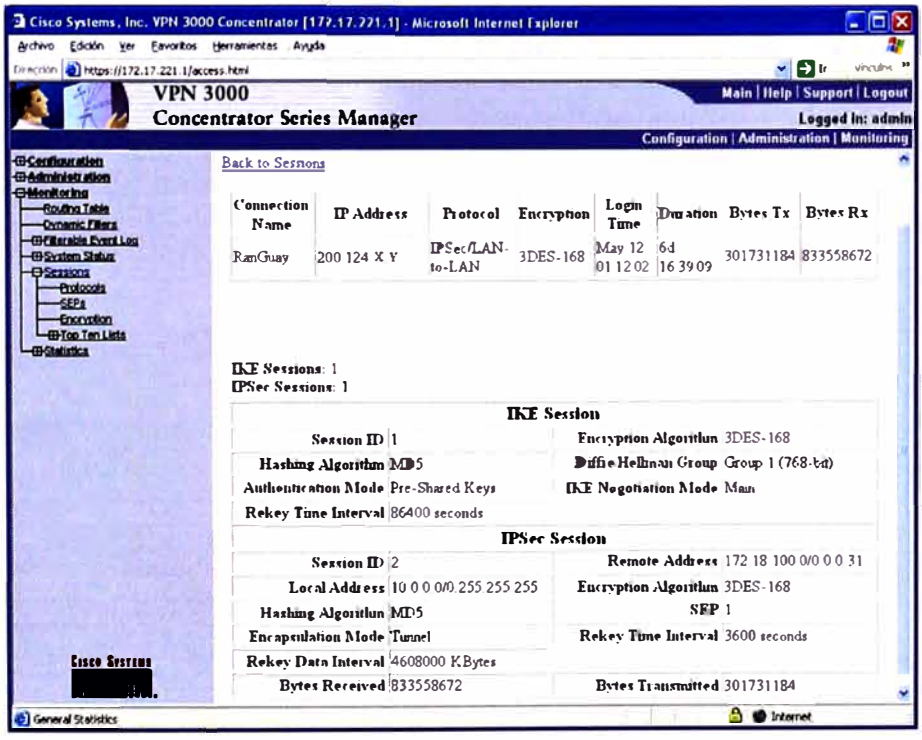


Figura 3.9 Monitoreo de conexión VPN en el Concentrador 3030

Así mismo, del lado del router remoto se pueden apreciar también ambas Fases. Ver Figuras 3.10 y 3.11

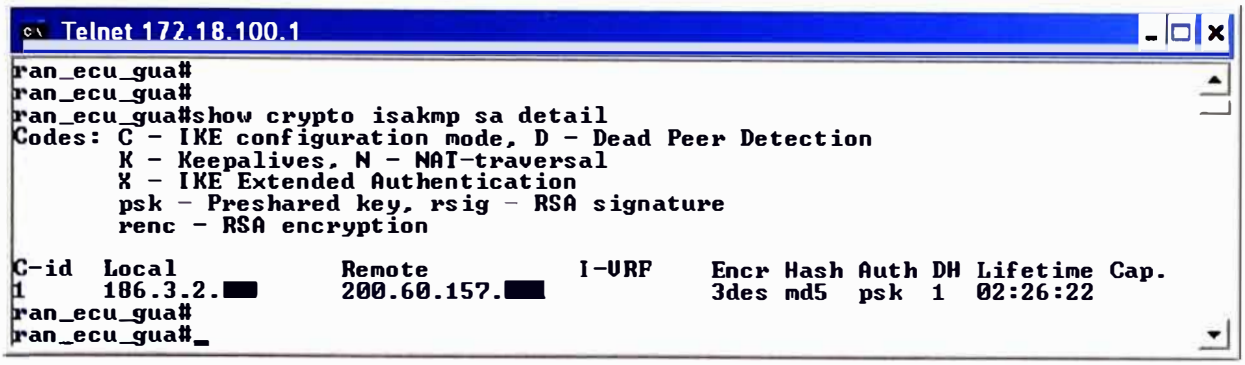


Figura 3.10 Monitoreo de conexión VPN en el router Cisco 2801 de Ransa Guayaquil

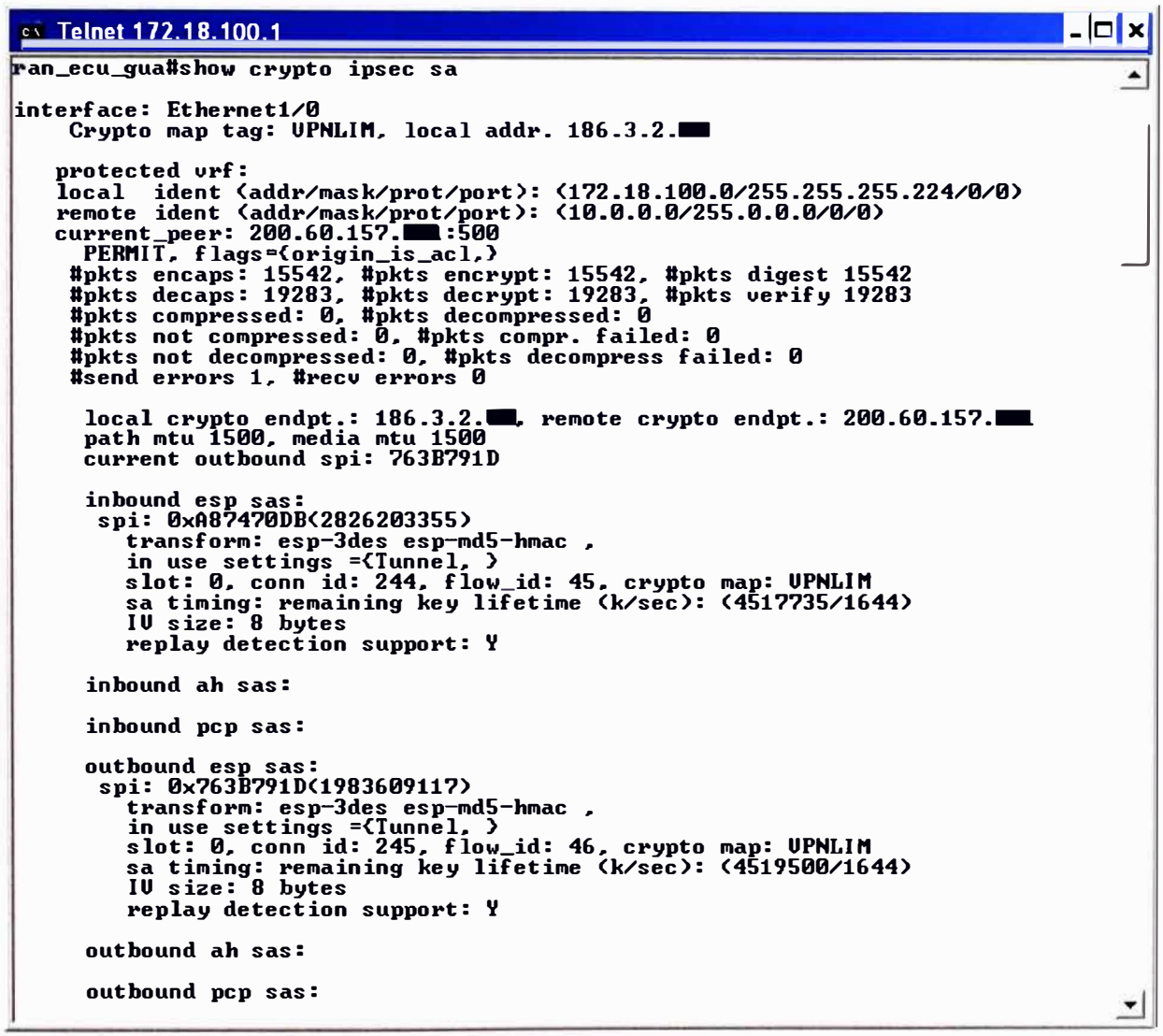


Figura 3.11 Monitoreo de conexión VPN en el router Cisco 2801 de Ransa Guayaquil

De esta forma, conforme las empresas fueron haciendo uso del nuevo servicio VPN Lan-to-Lan, se fue monitoreando el comportamiento y se determinó realizar algunas mejoras entres cuales estuvieron:

- Se contrató un nuevo enlace a Internet en el nodo central, usándolo exclusivamente para las conexiones VPN, tanto en modo acceso remoto como los de modo L2L. De esta forma, se evitó de cierto manera, que el tráfico de navegación que era de categoría ocio o entretenimiento, afectase la comunicación que se cursaba netamente del negocio de la empresas, ya que experiencias previas demostraban que malos hábitos de los usuarios en el uso de la red Internet, como son el uso de programas P2P o equipos infectados con virus informáticos producían saturación de los enlaces o generaban ráfagas de tráfico que volvían lentas las comunicaciones de datos y entrecortes de las llamadas de voz.
- Se incorporó firewalls Cisco modelo PIX 506E para seguridad perimetral en los locales de Ransa, ya que tenían algunos problemas con el control de la navegación que realizaban sus usuarios de la sucursales remotas. Este dispositivo fue instalado en serie y detrás del router gateway VPN, es decir, directamente a la red LAN interna, donde mediante filtros y listas de acceso controlaba la salida a Internet de las PCs; así mismo, dicho firewall no realizaba NAT de las direcciones privadas, ya que éstas debían llegar como tal al router gateway VPN para poder ver toda la red privada.
- Finalmente, para mejorar y agilizar la comunicación en general, se subió las velocidades de los locales remotos que tenían los anchos de banda más bajos, puesto que al contar ya con red privada, el volumen de tráfico e intercambio de información con la sucursales de Perú había tenido un crecimiento significativo, tanto en datos como en llamadas de voz que antes no había.

3.3 Recursos Humanos y Equipamiento

3.3.1 Recursos Humanos e Infraestructura

El despliegue del proyecto en sus fases de diseño e implantación ha sido, básicamente, ejecutada por un solo especialista del área de comunicaciones del Grupo Romero, ya que no ha sido necesario desplazarse a las ubicaciones remotas para la configuración de los equipos, puesto que al contar con personal de apoyo en dichas sucursales, se les ha dado instrucciones precisas para realizar la instalación, configuración básica y pruebas, tanto de los routers como de los firewalls; una vez hecho esto y teniendo la administración remota desde Perú, estos dispositivos han sido configurados completamente en todos los niveles necesarios restantes, tales como

enrutamiento, seguridad, VPN, voz, etc. Para la configuración de las centrales telefónicas tradicionales si ha sido necesario contratar un proveedor externo que brinde el soporte que se requería para conectarlo al router. De manera similar, para la configuración de las centrales IP ha intervenido personal externo, pero dado que estas eran nuevas, ya venían con instalación y configuración incluida, pero como se mencionó anteriormente, estos trabajos pertenecían ya a otro proyecto.

Así mismo, previamente para la etapa de adquisición de equipamiento, se realizaron solicitudes de cotización a proveedores locales de Cisco en cada país, lo que fue realizado por las respectivas áreas de adquisiciones de cada empresa y validado técnicamente por el área de comunicaciones de Grupo. Una ventaja de adquirir los equipos a nivel local en cada país, es que los tiempos de reemplazo por garantía son más cortos, así como también, poder contar con una rápida asistencia técnica ante eventuales fallas. En algunos casos, la cotización del equipamiento fue solicitada con instalación y configuración básica incluida, ya que el personal de apoyo de esas sucursales no tenía los conocimientos de nivel técnico para realizarlo. Como dichas solicitudes de cotización habían sido validadas técnicamente, luego recibidas las respuestas, cada empresa decidió la compra de la que económicamente era la más conveniente.

Un punto importante previo a la implementación, es la verificación de facilidades o requisitos necesarios que se deben contar en los locales remotos involucrados antes de la instalación de los equipos de comunicaciones, entre ellos, los más importantes son el sistema eléctrico y las condiciones físicas o ambientales.

En cada sucursal, el sistema eléctrico fue verificado y corregido por un proveedor local antes de la instalación del equipamiento de comunicaciones. Primero se solicitó un informe donde dicho proveedor da cuenta del estado de las instalaciones eléctricas encontradas, el estado del pozo a tierra y el sistema de protección eléctrica, tales como estabilizador, UPS y transformador de aislamiento, así como también señala lo necesario para corregir y adecuar dichos elementos. Una vez evaluado estos resultados, se validó los costos con el área de sistemas de cada empresa y luego se pidió al proveedor para que proceda ha realizar las correcciones indicadas.

Así mismo, se solicita a un proveedor similar que realice la verificación de las condiciones ambientales y físicas adecuadas, para la instalación de equipos de comunicaciones, así como el cableado de red necesario. En los locales donde las instalaciones eran casi nuevas, se realizó la inclusión de un gabinete o rack de comunicaciones, así como del sistema de ventilación mediante aire acondicionado para rack de comunicaciones. En el caso de las otras instalaciones ya existentes, dicho

proveedor realiza las verificaciones que los mencionados elementos estén adecuados para los equipos de comunicaciones a instalarse.

3.3.2 Equipamiento Utilizado

Los equipos usados para el desarrollo del presente proyecto son los que se describen a continuación

a. Concentrador Cisco VPN 3015
b. Router Cisco 2801
c. Firewall Cisco PIX 506E

a. Concentrador Cisco VPN 3000

Los concentradores Cisco de la serie 3000 son dispositivos Gateway VPNs que manejan técnicas avanzadas de autenticación y encriptación para proteger un cierto tipo de tráfico de datos determinado. Estos concentradores se fabricaron inicialmente para manejar gran número de sesiones VPN para acceso remoto, pero también soportan de muy buena forma, conexiones VPN L2L.

Los modelos de la serie 3000 se dividen en: 3005, 3015,3020, 3030, 3060 y 3080. De todos ellos, la serie 3005 y 3015 son los únicos que realizan las funciones VPN vía software, mientras que el resto de la serie lo realiza por hardware, usando para ello, módulos SEP (Scalable Encryptation Process),.los que son escalables y pueden adicionarse fácilmente para incrementar capacidad y throughput. Toda esta serie de concentradores tienen software actualizable y usan procesador Motorota PowerPC, NVRAM y Memoria Flash. Como se mencionó anteriormente, la implementación realizada se ha llevado a cabo usando un concentrador Cisco 3015, que fue migrado a un modelo 3030 mediante la adición de un módulo SEP, principalmente, para aumentar su capacidad de sesiones IPsec.

Básicamente, el hardware externo entre el 3015 y 3030 es el mismo, pues el 3015 puede ser actualizado a 3030 ó 3060, adicionándole uno o dos módulos SEP, respectivamente, aunque por default viene sin módulo SEP. En el Anexo A, Tabla A.3, puede verse un comparativo de estos modelos. Una vista de frente del equipo Concentrador VPN 3000 se muestra en la Figura 3.12.

Así mismo, como se puede ver en la Figura 3.13, este equipo consta de 3 interfaces Ethernet 10/100 que están claramente identificadas como: Privada, Pública y Externa. La interface privada conecta a la red interna, la interface pública conecta hacia el mundo exterior (usualmente Internet) y la interface externa conecta a una DMZ o la red

de otra compañía. En el caso del presente proyecto, ésta última interface no venía siendo usada.

Figura 3.12 Concentrador Cisco VPN 3000.

Además, se puede observar que es factible usar una fuente de alimentación modular adicional para respaldo de la principal. Es recomendable que si se desea alta disponibilidad, ambas fuentes de alimentación deben conectarse a redes eléctricas independientes.

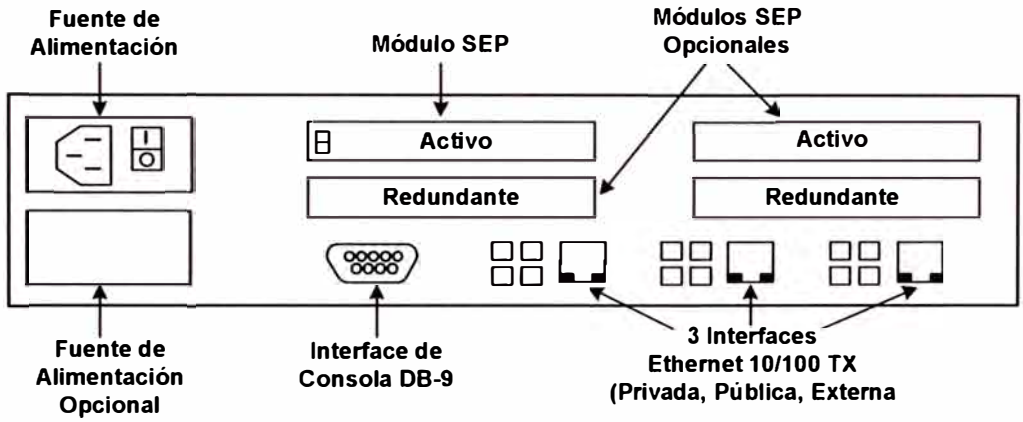


Figura 3.13 Panel posterior del Concentrador Cisco 3015 y 3030.

Dentro de todos los dispositivos Gateways VPN de Cisco, la serie de concentradores es la que mejor se desempeña en el mercado. Este tipo de dispositivos, actualmente han sido descontinuados por Cisco y reemplazados por los Cisco ASA.

b. Router Cisco 2801

Los Routers Cisco son otros dispositivos que pueden operar como Gateway VPN para dar protección de paquetes a determinado tráfico de red, además de otras funcionalidades, como enrutamiento, seguridad, calidad de servicio entre otros. Para desarrollar las funciones de encriptación y autenticación de datos, lo pueden realizar,

tanto por software IOS (Internet Operating System) o por hardware, mediante una tarjeta de encriptación. Para el caso del proyecto desarrollado, se ha usado un router Cisco modelo 2801 (Figura 3.14) con una tarjeta AIM-VPN, que ha sido instalado en locales remotos. La Figura 3.15 muestra el panel frontal de dicho equipo con la explicación correspondiente en la Tabla 3.3. Así mismo, las especificaciones técnicas de dicho equipo se muestran en el Anexo C.

Existen diferentes modelos de routers Cisco; hay uno para cada necesidad o situación. Una comparativa entre los diferentes modelos de routers que pueden realizar las funciones de Gateway VPN se muestran en el Anexo A.

Figura 3.14 Router Cisco 2801.

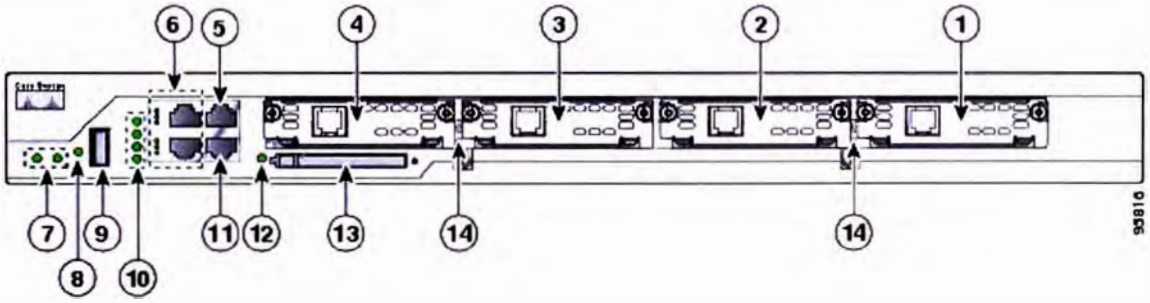


Figura 3.15 Panel frontal del Cisco 2801.

Tabla 3.3 Descripción de panel frontal correspondiente a la Figura 3.9

1	Slot 0 (VIC o VWIC, solo para voz)	**8**	LED de Fuente de Alimentación Auxiliar (AUX/PWR) LED
2	Slot 1 (WIC, VIC, VWIC o HWIC)	**9**	Puerto USB
3	Slot 2 (WIC, VIC o VWIC)	**10**	LEDs AIM/PVDM
4	Slot 3 (WIC, VIC, VWIC o HWIC)	**11**	Puerto auxiliar
5	Puerto de consola	**12**	LED de Compact flash (CF)
6	Puertos Fast Ethernet y sus LEDs	**13**	Slot para memoria externa CompactFlash
7	Sistema de LEDs	**14**	Guía de tarjetas central removible para permitir instalación de HWIC doble ancho

c. Firewall Cisco PIX 506E

El modelo usado para el presente proyecto es el Cisco PIX 506E, el cual además de tener funciones de VPN, puede realizar NAT dinámico, Proxy Server, filtrado de paquetes, firewall, entre otros. Físicamente, consta de 2 interfaces FastEthernet: una interface de consola y un puerto USB para uso futuro (Figura 3.16).

Este equipo está básicamente orientado a oficinas remotas, dado su tamaño compacto (Figura 3.17), pero que mantiene las mejores características de performance y disponibilidad que otros equipos de series similares. Así mismo, posee administración remota mediante interface gráfica vía web, para facilitar gestión a distancia o mediante interface de comandos por conexión a consola local.

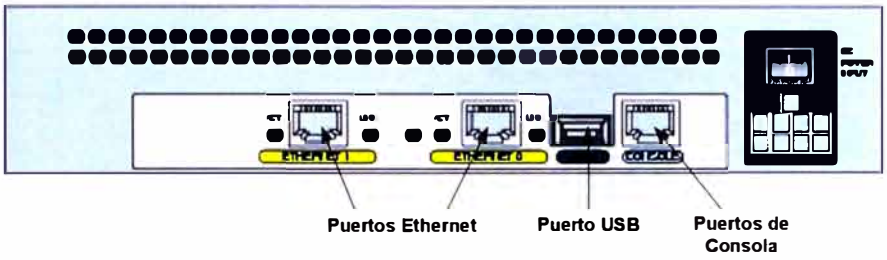


Figura 3.16 Panel posterior del PIX506E

Dentro de las funcionalidades de VPN, cumple completamente los estándares IKE e IPsec. Así mismo, soporta encriptación de datos con DES-56 bits, 3DES-168 bits y AES-256 bits.

Figura 3.17 Firewall Cisco PIX506E

Además, posee otras características, tales como:

- Provee seguridad perimetral para prevenir acceso a red no autorizado
- Usa el Algoritmo de Seguridad Adaptiva de Cisco para brindar un servicio de firewall de inspección de estado.
- Integra más de dos docenas de motores de inspección especializadas para protocolos, tales como http, FTP, SMTP, DNS, SNMP, SQL, NFS, H323, SIP, etc.

Se integra fácilmente con servicios AAA via TACACS+ y RADIUS.

Proporciona flexibilidad adicional cuando se definen políticas de seguridad, integrándose fácilmente a redes LAN con switches, mediante la creación de interfaces lógicas sobre VLANs IEEE 802.1q.

Puede operar como Servidor o Cliente DHCP, obteniendo una dirección IP por la interface outside desde el proveedor de servicio o entregando parámetros de red por una o más interfaces, permitiendo a otros dispositivos obtener direcciones IP dinámicamente.

Soporta servicios de bridge IPsec, habilitando a que un dispositivo ubicado detrás del Cisco PIX pueda establecer un túnel VPN a través del Firewall hacia otro peer VPN.

CAPITULO IV
BENEFICIOS OBTENIDOS Y COSTOS

4.1 Descripción de los resultados alcanzados

Con la implementación de la solución de VPN Lan-to-Lan en las diferentes sucursales internacionales de las empresas del Grupo Romero, se lograron obtener los siguientes resultados:

- Los usuarios de las sucursales remotas ya tienen conectividad con todos los servidores de la red de datos y con los permisos respectivos pueden acceder a todas sus aplicaciones.
- Las redes remotas internacionales se encuentran totalmente integradas a la red corporativa de Perú, con lo cual se constituye en una sola plataforma de comunicaciones, con la consecuente simplificación para los administradores de sistemas de las empresas del Grupo. Así mismo, al estar dichas sucursales conectadas a la red privada, cuentan con soporte integral por parte la Mesa de Ayuda corporativa, con lo cual pueden a su vez, tener un registro y seguimiento de todos lo eventos que suceden con sus equipos de oficina, como con servidores y servicios brindados por la red de voz y datos.
- La incorporación de las sucursales internacionales a la red de voz corporativa, ha logrado una importante reducción de costos por llamadas internacionales en los que venían incurriendo, reduciendo dicho rubro del presupuesto de las empresas, prácticamente, al mínimo. Ha sido posible mediante esta solución que usuarios de las sucursales remotas, además de poder comunicarse con sus similares en Perú, puedan también a través de dicha red de voz tener la opción de ser enrutados para tomar línea de la red pública de Lima, haciendo uso para ello, de la central telefónica de su sede principal en Perú, con lo cual sus llamadas a terceros se realizan a costo de llamada local.
- Los usuarios han liberado sus buzones de correo que venían saturándose constantemente, puesto que ahora ya no comparten sus archivos entre ellos enviándolos por correo electrónico, sino por medio de carpetas compartidas de sus PCs o colocándolos en el servidor FTP de la compañía, al cual todos ya pueden tener acceso.

- Finalmente, el logro más importante ha sido que los datos cursados por medio de la Internet entre las sucursales remotas internacionales y sus sedes centrales de cada una de las empresas en el Perú, viajan totalmente protegidos y seguros, libre de ser interceptados o modificados durante el trayecto.

4.2 Costos del proyecto y tiempo de ejecución

4.2.1 Costos

El presente proyecto no ha tenido un presupuesto definido con antelación a su realización, ya que debido a la coyuntura en que se encontraba la situación de las redes remotas internacionales, se debería resolver el problema en el menor tiempo posible, simplemente considerando la mejor alternativa de solución y que a la vez sea la de menor inversión económica.

Es así que el despliegue del proyecto ha incurrido de manera aproximada dentro los costos más significativos siguientes:

a. Costos por única vez (Iniciales)

Son costos que se refieren a los gastos realizados, principalmente, para la implementación de la solución por lo cual han sido desembolsados por única vez; dentro de estos están, el costo de los equipos adquiridos y el soporte técnico necesitado, el que básicamente, ha sido para la configuración de los puertos de voz de las centrales telefónicas que se conectaron a los routers. Como ya se explicó previamente, el resto del equipamiento ha sido configurado de manera remota desde Lima.

a.1 Equipamiento

Descripción	Precio ($)
Router Cisco 2801 con 2 FXS para Ransa Guayaquil	8500
Router Cisco 2801 con 2 FXS para Ransa Quito	8500
Router Cisco 2801 con 2 FXS para Ransa Guatemala	8500
Router Cisco 2801 con 2 FXS para Ransa Nejapa	8500
Router Cisco 2801 con 2 FXS para Ransa Merliot	8500
Firewall Pix 506E Alicorp Santa Leonor	3500
Firewall Pix 506E Alicorp Quito	3500
Firewall Pix 506E Alicorp Guayaquil	3500
Firewall Pix 506E Alicorp Bogotá	3500
Router Cisco 2801 con 2 FXS para Primax Guayaquil	8500
Módulo SEP para Cisco VPN3000	1500
Total Equipamiento	**66500**

a.2 Soporte Técnico

Descripción	Precio ($)
Configuración de central telefónica Rasa Guayaquil	350
Configuración de central telefónica Rasa Quito	350
Configuración de central telefónica Rasa Guatemala	350
Configuración de central telefónica Rasa Nejapa	350
Configuración de central telefónica Rasa Merliot	350
Total Soporte Técnico	**1750**

a.3 Enlaces

En cuanto a los enlaces, no ha habido costo inicial, ya que todos los locales contaban con acceso a Internet a diferentes velocidades cada uno de ellos, tal como se mostró en la tabla 1.1.

b. Costos Mensuales

Estos costos son los que se refieren básicamente a la renta mensual de los enlaces, ya que todo el equipamiento fue comprado y el soporte técnico se realiza desde el nodo central de Lima.

Descripción	Precio ($)
Enlace Internet de 256 Kbps para Ransa Guayaquil	400
Enlace Internet de 256 Kbps para Ransa Quito	400
Enlace Internet de 1 Mbps para Ransa Guatemala	1600
Enlace Internet de 1 Mbps para Ransa Nejapa	1700
Enlace Internet de 1 Mbps para Ransa Merliot	1700
Enlace Internet de 1.2 Mbps para Alicorp Santa Leonor	1300
Enlace Internet de 1.5 Mbps para Alicorp Quito	1600
Enlace Internet de 256 Kbps para Alicorp Guayaquil	400
Enlace Internet de 512 Kbps para Alicorp Bogotá	700
Enlace Internet de 1.5 Mbps para Primax Guayaquil	1200
Total Enlaces	**11000**

4.2.2 Tiempo de Ejecución

Como se mencionó en un inicio, los locales con problemas, en primer lugar, fueron las sucursales de Ransa ubicadas en Ecuador y El Salvador, con dos locales en cada uno esos países; posteriormente se presentó el requerimiento adicional de otros 6 locales, entre ellos, 1 de Ransa en Guatemala, 4 de Alicorp en Ecuador y 1 de Primax también en Ecuador.

Es decir, el desarrollo completo de toda la red de VPNs L2L mostrada en el presente trabajo, se ha venido dando en demanda de lo que las empresas lo solicitaban, es así que desde que se instaló el primer VPN con Ransa Guayaquil hasta el último que fue el de Alicorp Guayaquil, transcurrió aproximadamente, en total, 2 años.

El despliegue del primer VPN L2L con Ransa Guayaquil tomó alrededor de 8 semanas, básicamente, debido a que era la primera implementación de este tipo en la red del Grupo y como tal, debía validarse y verificarse todos los parámetros, a fin de obtener un patrón general para las demás configuraciones futuras. Así mismo, un lapso importante de tiempo lo constituyó la adquisición de los equipos, pues los tiempos de entrega que manejan los diversos proveedores son de 30 a 40 días.

Básicamente, los tiempos fueron divididos de la siguiente manera:

- Recolección de información: 1 semana
- Diseño de la solución : 1semana
- Adquisición de equipos: 4 semanas
- Implementación: 1 semana
- Pruebas y verificaciones: 3 días
- Afinamiento: 3 días

Tiempo total aproximado en la ejecución del primer VPN: 8 semanas

En el caso de las siguientes implementaciones de VPNs L2L con las otras sucursales, el tiempo total de ejecución logró reducir como sigue:

- Recolección de información: 1 semana
- Diseño de la solución : 1 día
- Adquisición de equipos: 2 semanas
- Implementación: 2 días
- Pruebas y verificaciones: 1 día
- Afinamiento: 1 día

Tiempo total aproximado en la ejecución de los demás VPNs: 4 semanas

La reducción del tiempo de ejecución, comparado con el de la primera VPN implementada, se debió básicamente, al conocimiento previo adquirido, tanto para el proceso de desarrollo de la implementación completa, así como en el aspecto técnico relacionado con los equipos de comunicaciones.

En el caso de los procesos, se logró negociar con los proveedores desde un inicio y antes de la adquisición, para que éstos entreguen equipos provisionales mientras llegaba el equipo nuevo definitivo que se estaba comprando. En el caso del aspecto técnico, ya se tenía una plantilla general de las configuraciones para levantar

rápidamente las conexiones VPN L2L aplicadas, tanto a los routers o firewalls, así como también en las centrales telefónicas o canales de voz.

CONCLUSIONES Y RECOMENDACIONES

1. Se ha comprobado que los VPN basados en IPsec pueden ser fácilmente implementados en cualquier lugar donde se tenga una conexión de acceso a Internet disponible, por lo tanto, ofrecen un alto grado de flexibilidad para interconectar sucursales remotas, aun en lugares donde no se cuenta con otro tipo de servicio de enlace dedicado.
2. Se ha determinado que para que las conexiones VPN L2L sobre Internet operen de manera eficiente, deben ir acompañados de un esquema de políticas de seguridad bien definidos, que elimine eventos indeseados o malas prácticas de los usuarios que afecten a las líneas de acceso a Internet, sobre los cuales se está implementando las conexiones VPN.
3. Se recomienda que para desplegar soluciones de VPN, donde se tiene que cursar tráfico sensible al retardo, tal como comunicaciones de voz, se usen dispositivos que realicen la función de encriptación por hardware en lugar de software.
4. Se recomienda que en implementaciones donde se usen routers como Gateway VPN, se incluyan adicionalmente, firewalls de seguridad perimetral, a fin de tener una salida de tráfico controlada, principalmente, cuando el medio de acceso es por Internet. Esto ha sido plasmado en los locales donde inicialmente sólo se instalaron routers, por lo que luego fue necesario adicionarle firewalls de seguridad perimetral.
5. Se recomienda en implementaciones de VPN L2L por Internet con topología Hub-and-Spoke, mantener el acceso del nodo central, únicamente para tráfico de las conexiones VPN. Esto mejora el rendimiento de la tecnología, sobre todo, cuando sobre ellas se cursa tráfico de voz sobre IP.
6. Las VPNs basadas en IPsec, han servido como una herramienta tecnológica valiosa para que las empresas del Grupo Romero sigan creciendo y desarrollando sus operaciones de manera eficiente y segura y, con la experiencia alcanzada, puedan ahora expandir su crecimiento a cualquier ubicación a nivel global.

ANEXO A
CUADROS COMPARATIVOS DE EQUIPOS CISCO

CUADROS COMPARATIVOS DE EQUIPOS CISCO

Tabla A.1. Comparación de Routers Cisco con funcionalidad para VPN.

Router Model	Location	VPN Sessions	VPN Throughput (in Mbps)
SOHO 90 series	SOHO	8	3DES: 1
830 series	SOHO	10	3DES: 7; AES: 2
850 series	SOHO or small branch office	5	3DES and AES: 8
870 series	SOHO or small branch office	10	3DES and AES: 30
1700 w/VPN module	Small branch office	100	3DES: 15
1841 w/AIM-VPN BP II Plus	Small to medium branch office	800	3DES and AES: 95
2600XM w/AIM-VPN/ BP II module	Medium branch office	800	3DES: 22; AES: 22
2691 w/AIM-VPN/EP II module	Medium branch office	800	3DES: 150; AES: 150
2621, 3640, or 3660 with hardware card	Medium branch office		3DES: 32 Mbps
2800s w/AIM-VPN/EP II-Plus	Enterprise branch office	1,500	3DES and AES: 145
3725 w/AIM-VPN/EP II module	Enterprise branch office	800	3DES: 186; AES: 186
3745 w/AIM-VPN/HP II module	Enterprise branch office	2,000	3DES: 190; AES: 190
3825 w/AIM-VPN/ EP II-Plus	Enterprise branch or regional office	2,000	3DES and AES: 175
3845 w/AIM-VPN/ HP II-Plus	Enterprise branch or regional office	2,500	3DES and AES: 185
7100 w/SM-VAM	Enterprise branch or regional office	3,000	3DES: 145; AES: N/A
7200 w/one ISA module	Enterprise branch or regional office	2,000	3DES: 90; AES: N/A
7200VXR w/one SA-VAM2+ module	Enterprise edge	5,000	3DES: 260; AES: 280
7300 w/one SA-VAM2+	Enterprise edge	5,000	3DES: 370; AES: 370
7400 w/one SA-VAM	Enterprise edge	5,000	3DES: 145; AES: N/A
7600 or Catalyst 6500 w/one VPN Service Module (VPNSM)	Enterprise data center	8,000	3DES: 1,900; AES: N/A

Tabla A.2. Comparación de modelos Cisco PIX y sus capacidades.

Specification	501	506E	515E	525	535
Firewall throughput in Mbps	60	100	190	330	1,650
Failover/redundancy support	N	N	Y	Y	Y
3DES throughput in Mbps (software/VAC+)	3	15	20/130	70/145	50/425
AES-128 throughput in Mbps (software/VAC+)	4.5	30	45/130	65/135	110/495
AES-256 throughput in Mbps (software/VAC+)	3.4	25	35/130	50/135	90/425
Maximum VPN peers	10	25	2,000	2,000	2,000

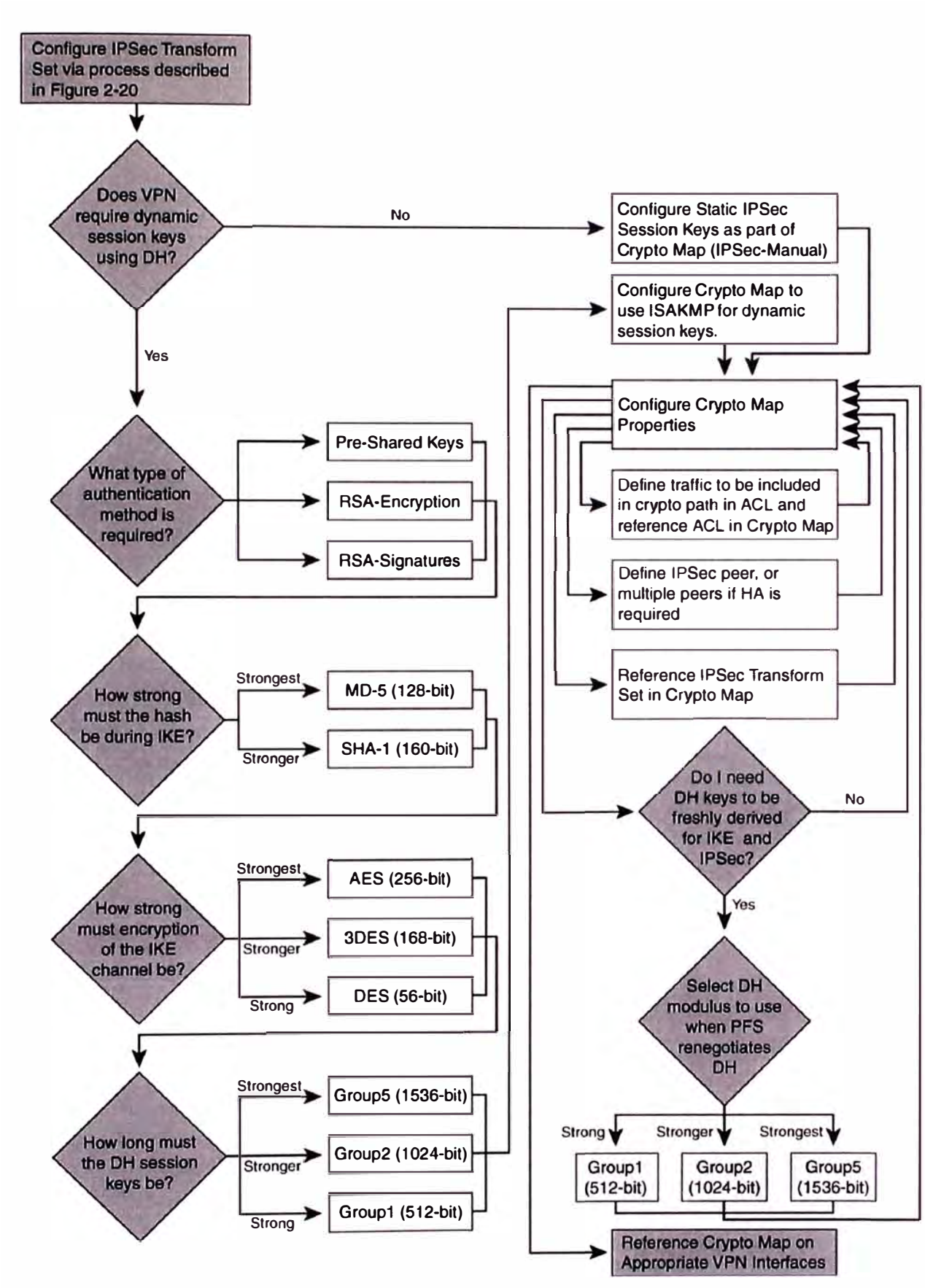
Tabla A.3. Comparación de modelos de Concentradores VPN Serie 3000.

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous IPsec Users*	200	100	750	1500	5000	10000
Simultaneous SSL VPN (Clientless) Users**	50	75	200	500	500	500
Máximum LAN-to-LAN Sessions	100	100	250	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware	Hardware
Available Expansión Slots	0	4	1 (redundancy option)	3 (redundancy option)	2 (redundancy option)	0 (fully redundant)
Encryption Module (SEP)	0	0	1	1	2	4
Redundant SEP	-	-	Optional	Optional	Optional	Yes
System Memory	32/64 MB (fixed)	128 MB	256 MB	512 MB	512 MB	512 MB
Hardware Configuration	1U	Scalable 2U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Optional	Optional	Optional	Optional	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

ANEXO B

PROCESO DE CONFIGURACIÓN DE ALTO NIVEL PARA VPNs IPsec

PROCESO DE CONFIGURACIÓN DE ALTO NIVEL PARA VPNs IPsec



ANEXO C
ESPECIFICACIONES TÉCNICAS DE EQUIPOS USADOS

C1.- ESPECIFICACIONES TÉCNICAS DE CONCENTRADOR CISCO VPN 3030

Hardware	
Processor	Motorola PowerPC processor
Memory	• Redundant system images (Flash) • Variable memory options (Figure 6)
Encryption	• Cisco VPN 3005, 3015: Software • Cisco VPN 3020, 3030, 3060, and 3080: Hardware
Embedded LAN Interfaces	• Cisco VPN 3005: Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted, and DMZ)
Instrumentation	• Cisco VPN 3005: Unit status indicator (front panel); status LEDs for Ethernet ports (rear panel) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Status LEDs for system, expansion modules, power supplies, Ethernet modules, and fan (front panel); status LEDs for Ethernet modules, expansion modules, and power supplies (rear panel) • Cisco VPN 3015, 3020, 3030, 3060, and 3080: Activity monitor displays the number of sessions, aggregate throughput, or CPU utilization, and is push-button selectable
Software	
Client Software Compatibility	• Cisco SSL VPN Client for network-layer connectivity using an SSL-capable Web browser on remote system • Cisco IPsec VPN Client for Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X 10.2, 10.3, and 10.4, including centralized split-tunneling control and data compression • Microsoft PPTP, Microsoft Point-to-Point Encryption (MPPE), and Microsoft Point-to-Point Compression (MPPC); Microsoft Challenge Handshake Authentication Protocol (MSCHAP) v1 and v2; and Extensible Authentication Protocol (EAP) and RADIUS passthrough for EAP-Transport Layer Security (EAP-TLS) and EAP-Generic Token Card (EAP-GTC) support • Microsoft L2TP and IPsec for Windows 2000 and XP, including Windows XP Dynamic Host Control Protocol (DHCP) option for route population • Microsoft L2TP and IPsec for Windows 98, ME, and NT Workstation 4.0
Tunneling Protocols	• Cisco SSL VPN (HTTPS/SSL-based) • IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with autodetection and fragmentation avoidance), IPsec/TCP • Support for Cisco EasyVPN (client and network extension mode)
Encryption/Authentication	• IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128/192/256-bit) with Message Digest Algorithm 5 (MD5) or Secure Hashing Algorithm (SHA); or MPPE using 40/128-bit RC4
Key Management	• Internet Key Exchange (IKE) • Diffie-Hellman (DH) groups 1, 2, 5, and 7 (ECDH)

	• RSA certificates (SSL and IPsec)
Routing	• Routing Initiation Protocol (RIP), RIPv2, Open Shortest Path First (OSPF), Reverse Route Injection (RRI), static routing, automatic endpoint discovery, NAT, and Classless Interdomain Routing (CIDR) • IPsec fragmentation policy control, including support for Path Maximum Transmission Unit (MTU) Discovery (PMTUD) • Interface MTU control
Third-Party Compatibility	iPass Ready, Funk Steel-Belted RADIUS, Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, and SA Keon
High Availability	• Virtual Router Redundancy Protocol (VRRP) for multichassis redundancy and multichassis failover • Remote-access load-balancing clusters supporting both SSL and IPsec connections • Destination pooling for client-based failover, re-establishment, and connection re-establishment • Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015, 3020, 3030, 3060, and 3080 models)
Management	
Configuraron	• Embedded management interface is accessible through console port, Telnet, SSHv1, and HTTPS • Administrator access is configurable for five levels of authorization; authentication can be performed externally through TACACS+ • Role-based management policy separates functions for service provider and end-user management • Monitoring • Event logging and notification through e-mail (SMTP) • Automatic FTP backup of event logs • Simple Network Management Protocol (SNMP) MIB-II support • Configurable SNMP traps • Syslog output • System status • Session data (including client assign IP, encryption type connection duration, client OS, and client version) • General statistics
Security	
Authentication and Accounting Servers	• Support for redundant external authentication servers, including: - RADIUS - Kerberos/Active Directory authentication - Microsoft NT Domain authentication - Microsoft NT Domain authentication with password expiration (MSCHAPv2); IPsec only
RSA Security Dynamics (SecurID Ready), Including Native Support for RSA 5 (Load Balancing, Resiliency)	• User authorization through Lightweight Directory Access Protocol (LDAP) or RADIUS • Internal authentication server for up to 100 users • X.509v3 digital certificates, including certificate revocation list (CRL)/LDAP and CRL/HTTP, CRL caching, and backup CRL distribution point support

	• RADIUS accounting • TACACS+ administrative user authentication
Internet-Based Packet Filtering	• Source and destination IP address • Port and protocol type • Fragment protection • FTP session filtering • Site-to-site filters and NAT (for overlapping address space)
Policy Management	• By individual user or group - Filter profiles (defined internally or externally) - Idle and maximum session timeouts - Time and day access control - Tunneling protocol and security authorization profiles - IP pool and servers - Authentication pool and servers
Certification	Federal Information Processing Standards (FIPS) 140-2 Level 2 (3.6), FIPS 140-1 Level 2 (3.1), and VPNC

C.2.- ESPECIFICACIONES TÉCNICAS DE ROUTER CISCO 2801

Description	Specification
Dimensions (H x W x D)	1.72 x 17.49 x 16.5 in. (4.4 x 44.4 x 41.9 cm).
Weight	10.9 lb (4.9 kg) with standard power supply if fully populated with modules 13.71 lb (6.2 kg) with inline power supply if fully populated with modules
AC input power • Input voltage • Frequency • Input current • Inrush surge current	 100 to 240 VAC, autoranging 47 to 63 Hz 2 A (5 A for IP phone support) 50 A maximum, one cycle (-48V power included)
Power consumption	105 W with standard power supply (maximum) 130 W with inline power supply and 12 IP phones (maximum)
Console and auxiliary ports	RJ-45 connector
Operating humidity	5 to 95%, noncondensing
Operating temperature	32 to 104·F (0 to 40·C)
Nonoperating temperature	-4 to 149·F (-20 to 65·C)
Noise level, standard power supply	39 dBA for local temperatures < 90·F (32·C) 47 dBA for local temperatures between 90·F and 116·F (47·F) 52.6 dBA for temperatures above 116·F (47·F)
Noise level, inline power supply	44 dBA for local temperatures < 90·F (32·C) 50 dBA for local temperatures between 90·F and 116·F (47·F) 53 dBA for temperatures above 116·F (47·F)
Safety compliance	UL 60950; CAN/CSA C22.2 No. 60950-00; IEC 60950; EN 60950-1; AS/NZS 60950

	For detailed compliance information, refer to the *Cisco 2800 and Cisco 3800 Series Integrated Services Routers Regulatory Compliance and Safety Information* document.
Immunity compliance	EN300386; EN55024/CISPR24; EN50082-1; EN61000-6-2 For detailed compliance information, refer to the *Cisco 2800 and Cisco 3800 Series Integrated Services Routers Regulatory Compliance and Safety Information* document.
EMC compliance	FCC Part 15; ICES-003 Class A; EN55022 Class A; CISPR22 Class A; AS/NZS 3548 Class A; VCCI Class A; EN 300386; EN61000-3-3; EN61000-3-2 For detailed compliance information, refer to the *Cisco 2800 and Cisco 3800 Series Integrated Services Routers Regulatory Compliance and Safety Information* document.

C.3.- ESPECIFICACIONES TÉCNICAS DE FIREWALL CISCO PIX 506E

Feature	**Specifications**
Software Licenses	• 3DES/AES and DES Encryption Licenses • The Cisco PIX 506E Security Appliance has two optional encryption licenses- one license (PIX-506-SW-3DES) enables 168-bit 3DES and up to 256-bit AES encryption, the other license (PIX-VPN-DES) enables 56-bit DES encryption. Both are available either at the time of ordering the Cisco PIX 506E Security Appliance, or can be obtained subsequently through Cisco.com. Note that an encryption license must be installed to activate encryption services which are required before using certain features including VPN and secure remote management.
Performance Summary	• Cleartext throughput: Up to 100 Mbps • Concurrent connections: 25,000 • 56-bit DES IPSec VPN throughput: Up to 20 Mbps • 168-bit 3DES IPSec VPN throughput: Up to 16 Mbps • 128-bit AES IPSec VPN throughput: Up to 30 Mbps • 256-bit AES IPSec VPN throughput: Up to 25 Mbps • Simultaneous VPN peers: 25* * Maximum number of simultaneous site-to-site or remote access IKE Security Associations (SAs) supported
Technical Specifications	• Processor: 300-MHz Intel Celeron Processor • Random access memory: 32 MB of SDRAM • Flash memory: 8 MB • Cache: 128 KB level 2 at 300 MHz • System bus: Single 32-bit, 33-MHz PCI
Environmental Operating Ranges	• Operating • Temperature: 23 to 104°F (-5 to 40°C) • Relative humidity: 10 to 95 percent, noncondensing • Altitude: 0 to 6500 feet (2000 m) • Shock: 250 G, < 2 ms • Vibration: 0.41 Grms2 (5 to 500 Hz) random input

	• Nonoperating • Temperature: -13 to 158°F (-25 to 70°C) • Relative humidity: 10 to 95 percent, noncondensing • Altitude: 0 to 15000 feet (4570 m) • Shock: 60 G, 11 ms • Vibration: 0.41 Grms2 (5 to 500 Hz) random input
Power	• Autoswitching: 100V to 240V RMS • Current: 0.7 - 0.4[a] • Frequency: 50-60 Hz, single phase • Heat dissipation PIX 506E chassis: 102.4 BTU/hr, full power usage (30W) • Heat dissipation PIX 506E plus power adapter: 204.6 BTU/hr, full power usage (60 VA)
Physical Specifications	• Dimensions and Weight Specifications • Dimensions (H x W x D): 1.72 x 8.5 x 11.8 in. (4.37 x 21.59 x 29.97 cm) • Weight: 6 lb (2.71 kg) • Interfaces • Console port: RS-232, 9600 bps, RJ-45 • Outside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ-45 • Inside: Integrated 10/100 Fast Ethernet port, auto-negotiate (half/full duplex), RJ-45
Regulatory and Standards Compliance	• Regulatory Compliance • Products bear CE Marking indicating compliance with the 89/366/EEC and 73/23/EEC directives, which includes the following safety and EMC standards. • Safety • UL 1950, CAN/CSA-C22.2 No. 950, EN 60950, IEC 60950, IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, 21 CFR 1040 • Electromagnetic Compatibility (EMC) • FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A with UTP Class B with STP, CISPR22 Class A with UTP Class B with STP, AS/NZS 3548 Class A with UTP Class B with STP, VCCI Class A with UTP Class B with STP, EN55024, ETS 300 386-2, EN50082-1, EN61000-3-2, EN61000-3-3

ANEXO D

EJEMPLO DE CONFIGURACIÓN DE UNA VPN ENTRE DISPOSITIVOS CISCO

EJEMPLO DE CONFIGURACIÓN VPN ENTRE UN CONCENTRADOR VPN 3000 Y UN ROUTER CISCO

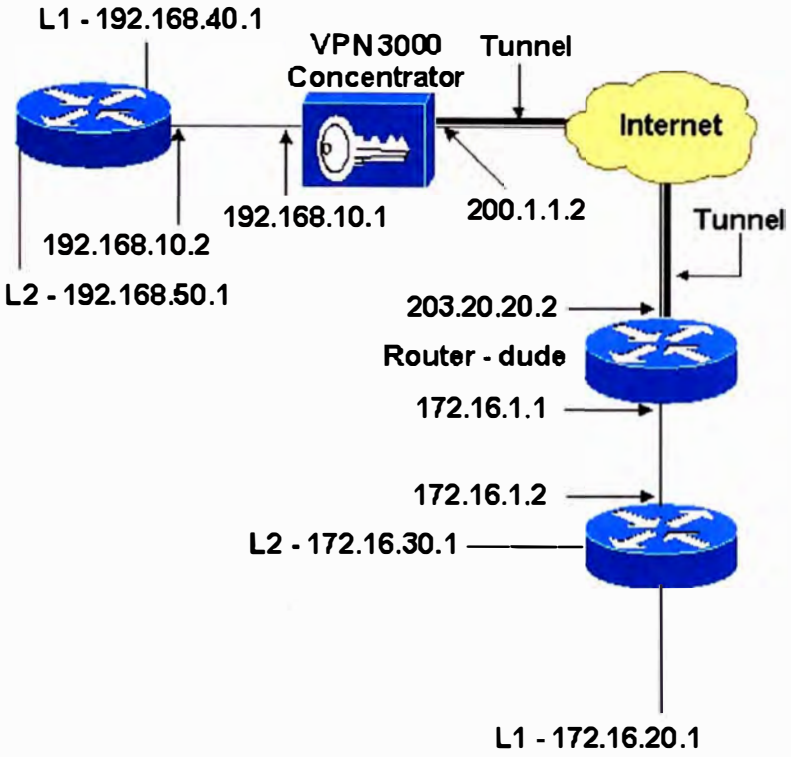
Componentes Usados

Router Cisco 2611 con Cisco IOS Software Release 12.3(1)a

Concentrador Cisco VPN 3000 con 4.0.1.B

Diagrama de Red

Este ejemplo se basa en el siguiente diagrama de red.



Configuraciones

Este ejemplo usa las siguientes configuraciones:

Configuración de Router
version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname dude ! memory-size iomem 15 ip subnet-zero

```
!
ip audit notify log
ip audit po max-events 100
!
!--- IKE policies.
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco123 address 200.1.1.2
!
!--- IPsec policies.
crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
set peer 200.1.1.2
set transform-set to_vpn
!

!--- Traffic to encrypt.
match address 101
!
interface Ethernet0/0
ip address 203.20.20.2 255.255.255.0
ip nat outside
half-duplex
crypto map to_vpn
!
interface Ethernet0/1
ip address 172.16.1.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!
!--- Traffic to encrypt.
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
```

```
!--- Traffic to except from the NAT process.
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
End
```

Configuración del Concentrador VPN

Asumiendo que el Concentrador VPN tiene ya configuración básica de interfaces, direcciones IP, default gateway, etc.

Ingresamos al equipo por medio de interface gráfica de usuario (GUI)

1.- Elegir **Configuration > Interfaces** para revisar las interfaces luego de ingresar a la GUI.

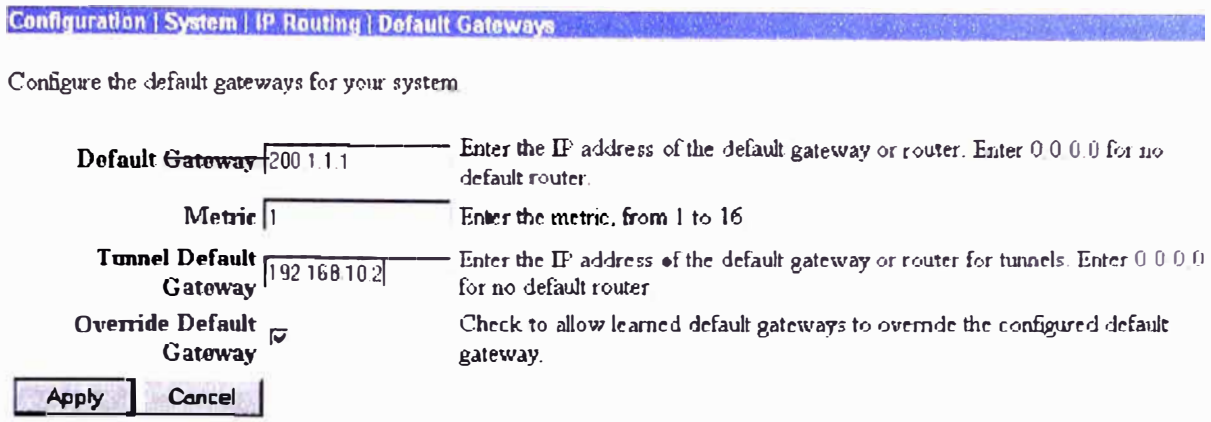
This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies

In the table below, or in the picture, select and click the interface you want to configure

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

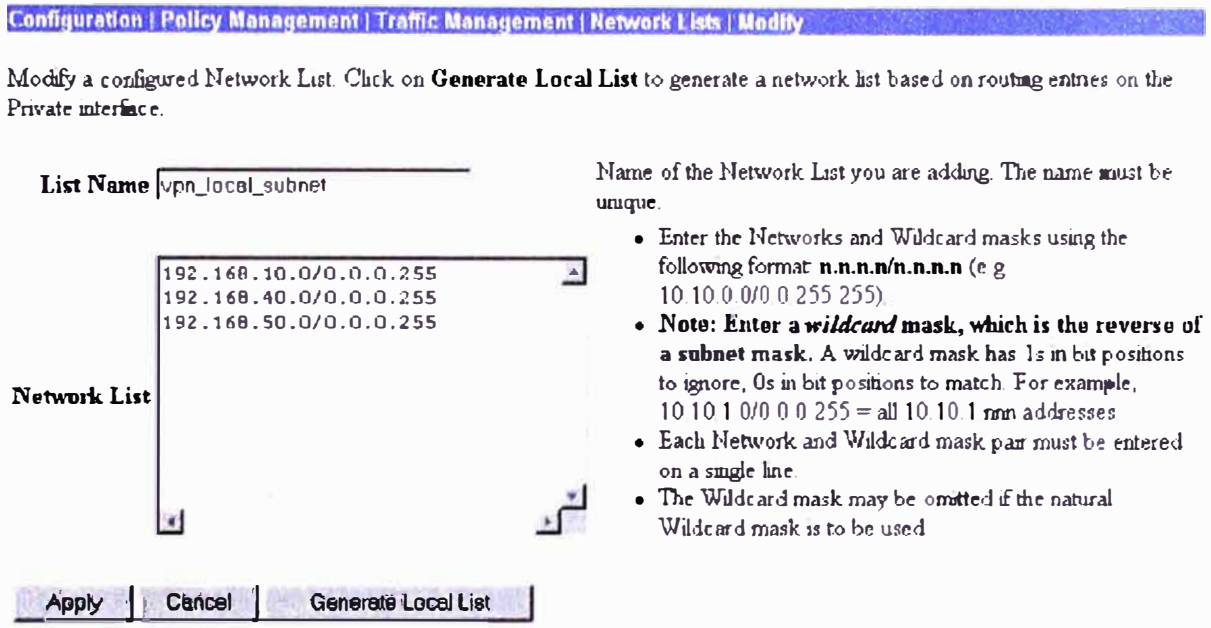
- Power Supplies

2.- Elegir **Configuration > System > IP Routing > Default Gateways** para configurar el Default (Internet) Gateway y el Default Túnel (inside) Gateway para IPsec.

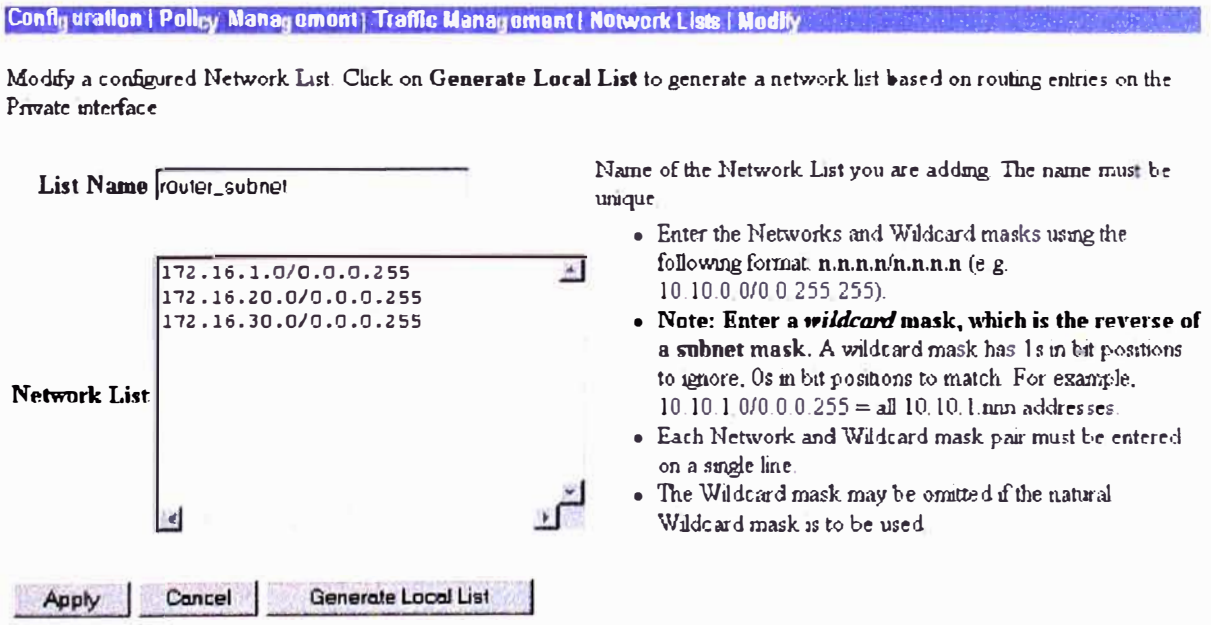


3.- Elegir **Configuration > Policy Management > Network Lists** para crear las listas de red que definirán el tráfico a ser encriptado.

Estas son las Redes Locales:

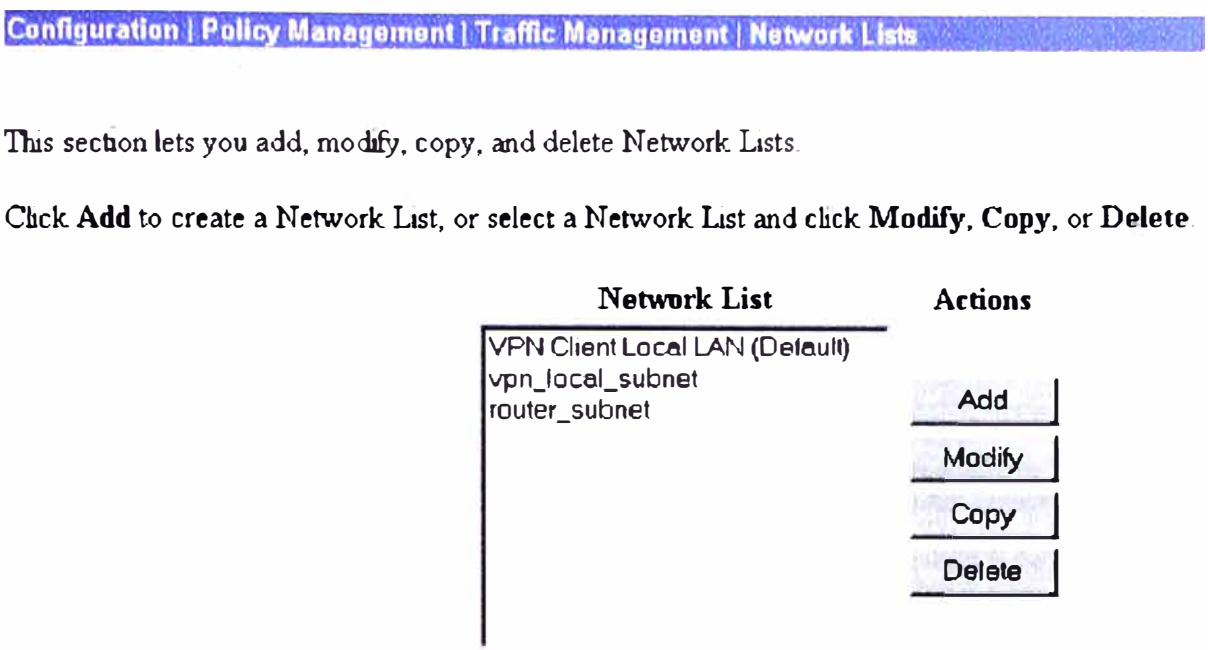


Estas son las redes remotas:

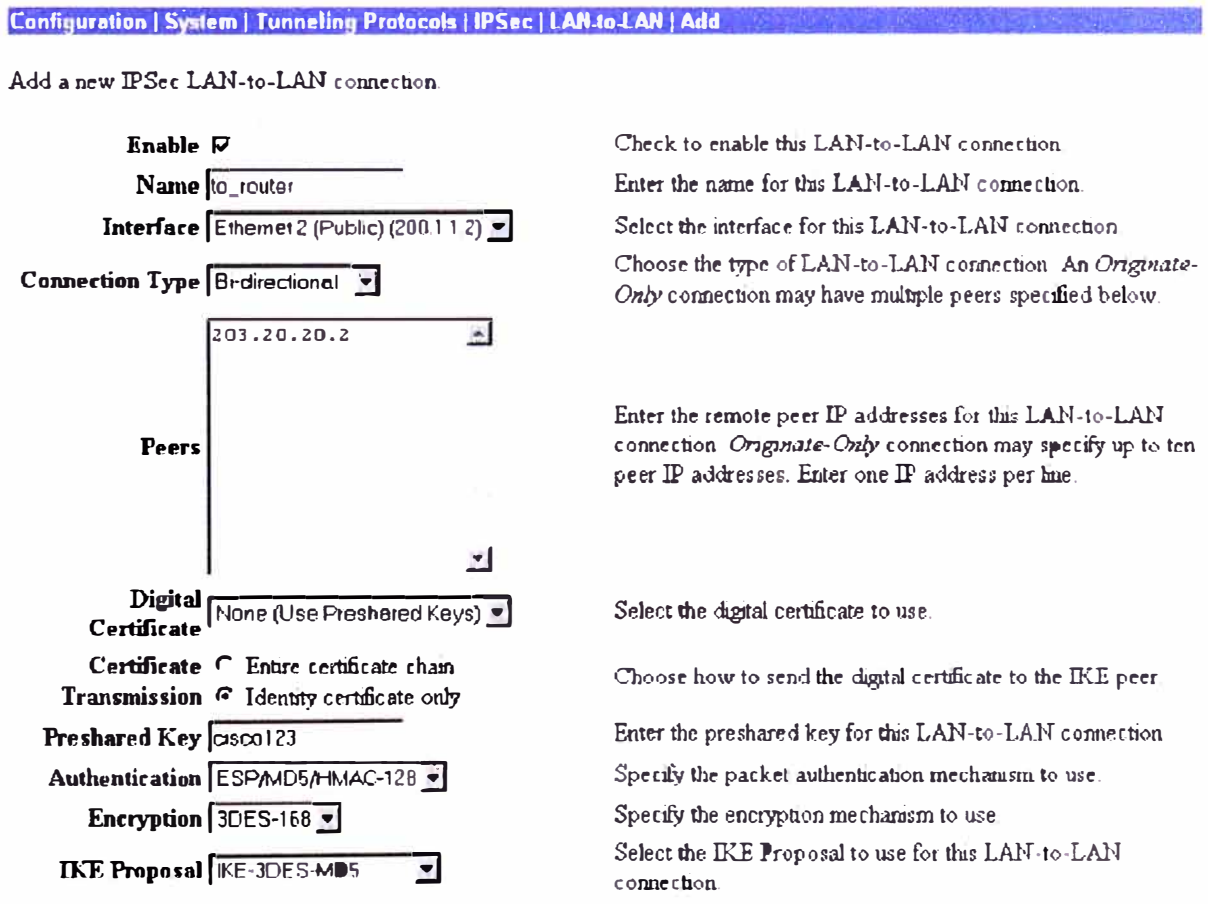


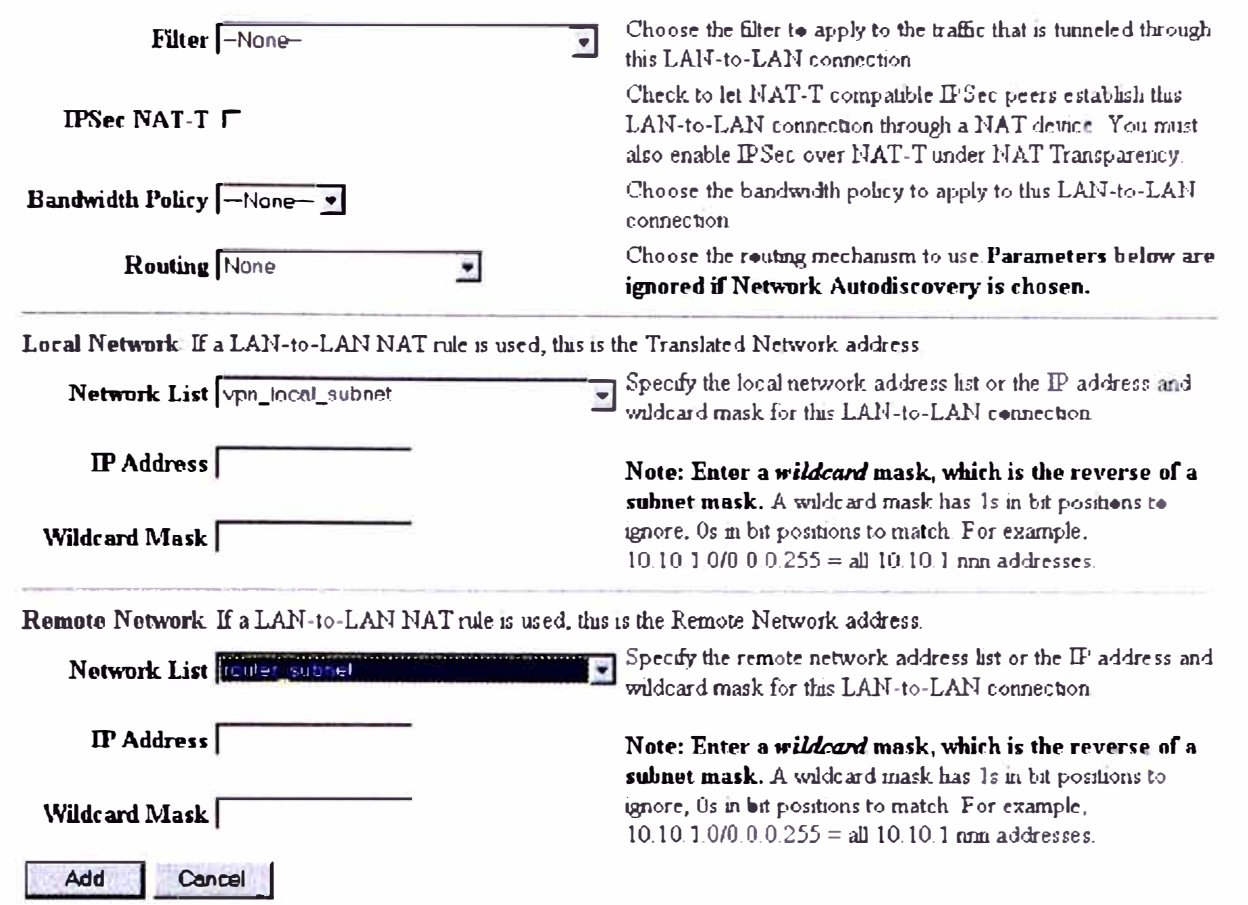
4.- Luego de completadas, hay dos network lists:

Nota: Si el túnel IPsec no levanta, verifique si el tráfico de interés coincide en ambos lados. El tráfico de interés es definido por access list en los routers y en los PIX.

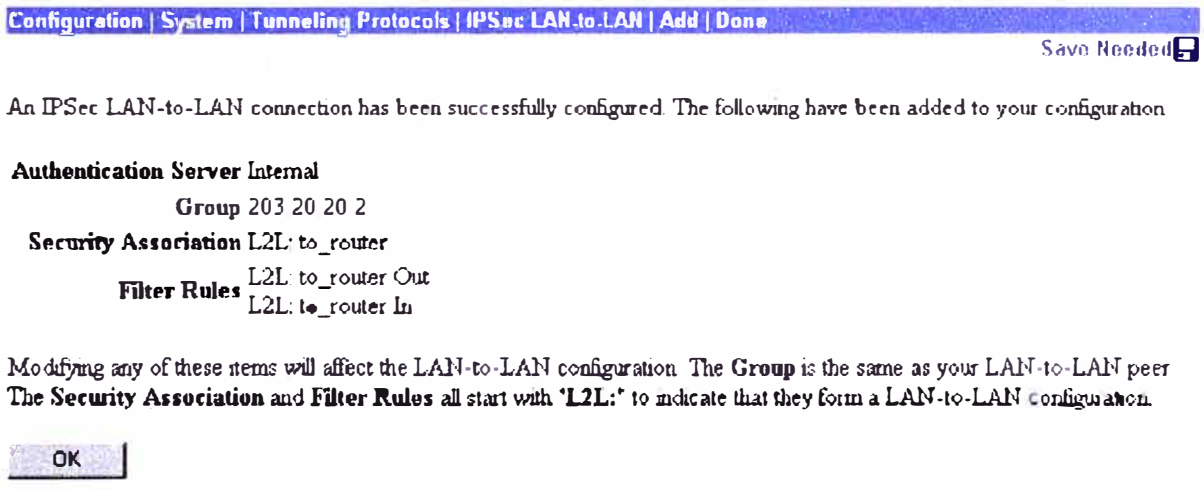


5.- Elegir **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** y definer el tunnel Lan-to-LAN

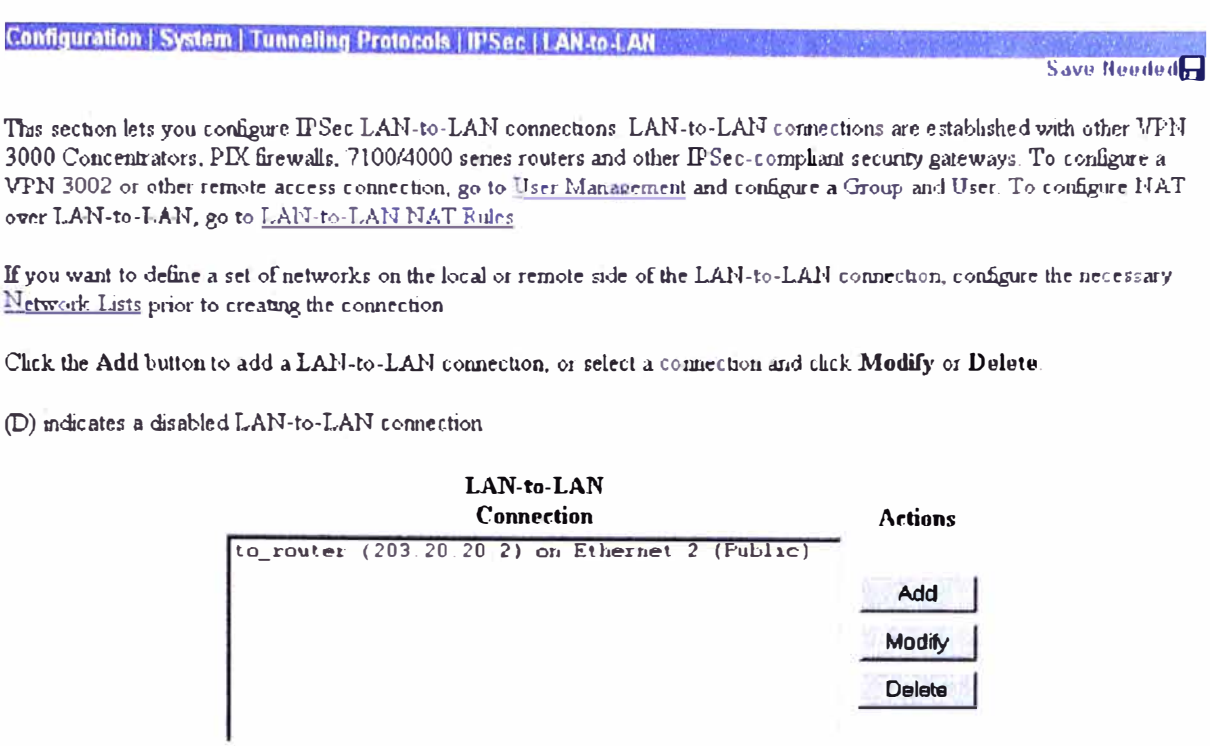




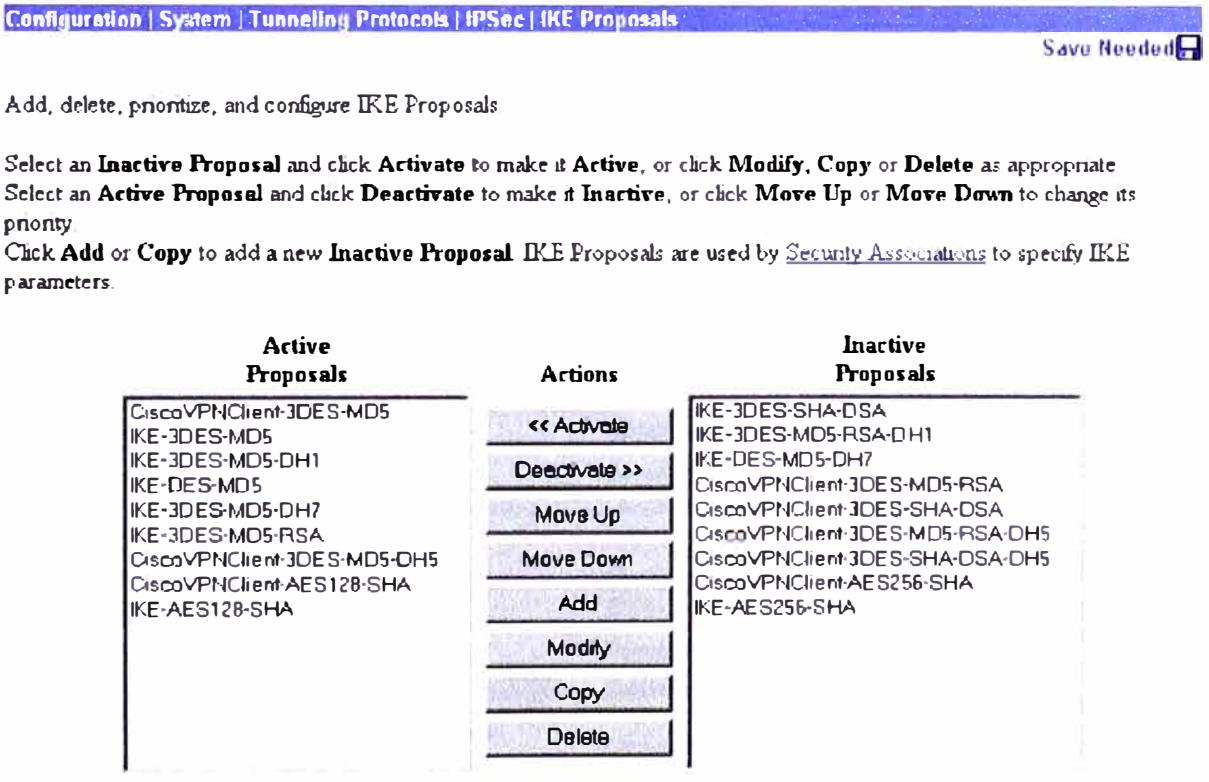
6.- Luego de aplicar **Apply**, esta ventana aparecerá con al configuración que ha sido automáticamente creada como resultado de la configuración del túnel LAN-to-LAN



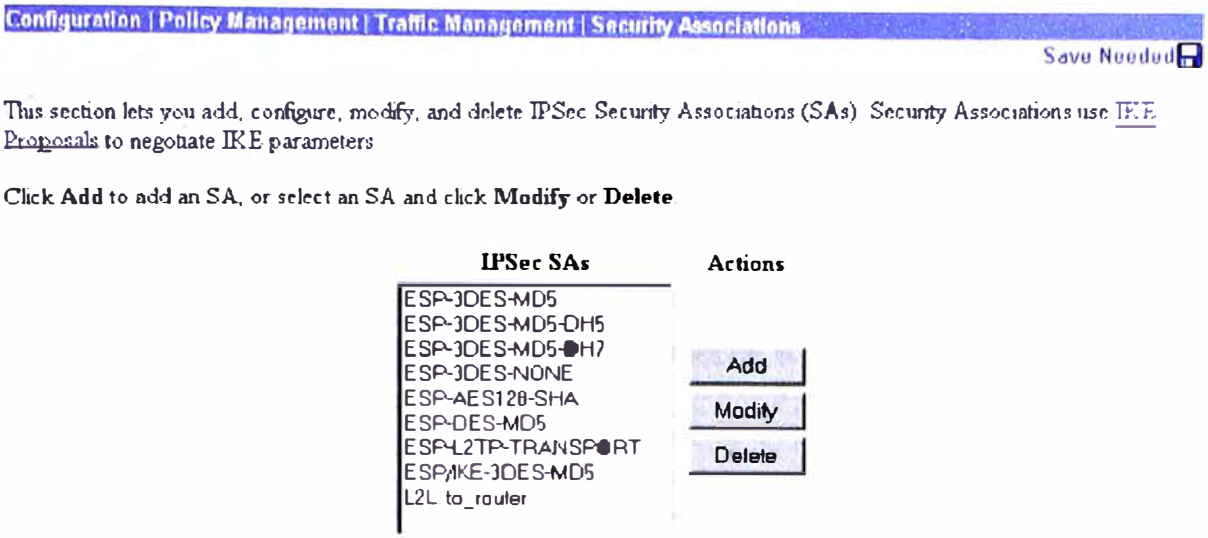
Estos parámetros IPsec LAN-to-LAN previamente creados, pueden ser vistos o modificados en **Configuration> System > Tunneling Protocols > IPSec LAN−to−LAN**.



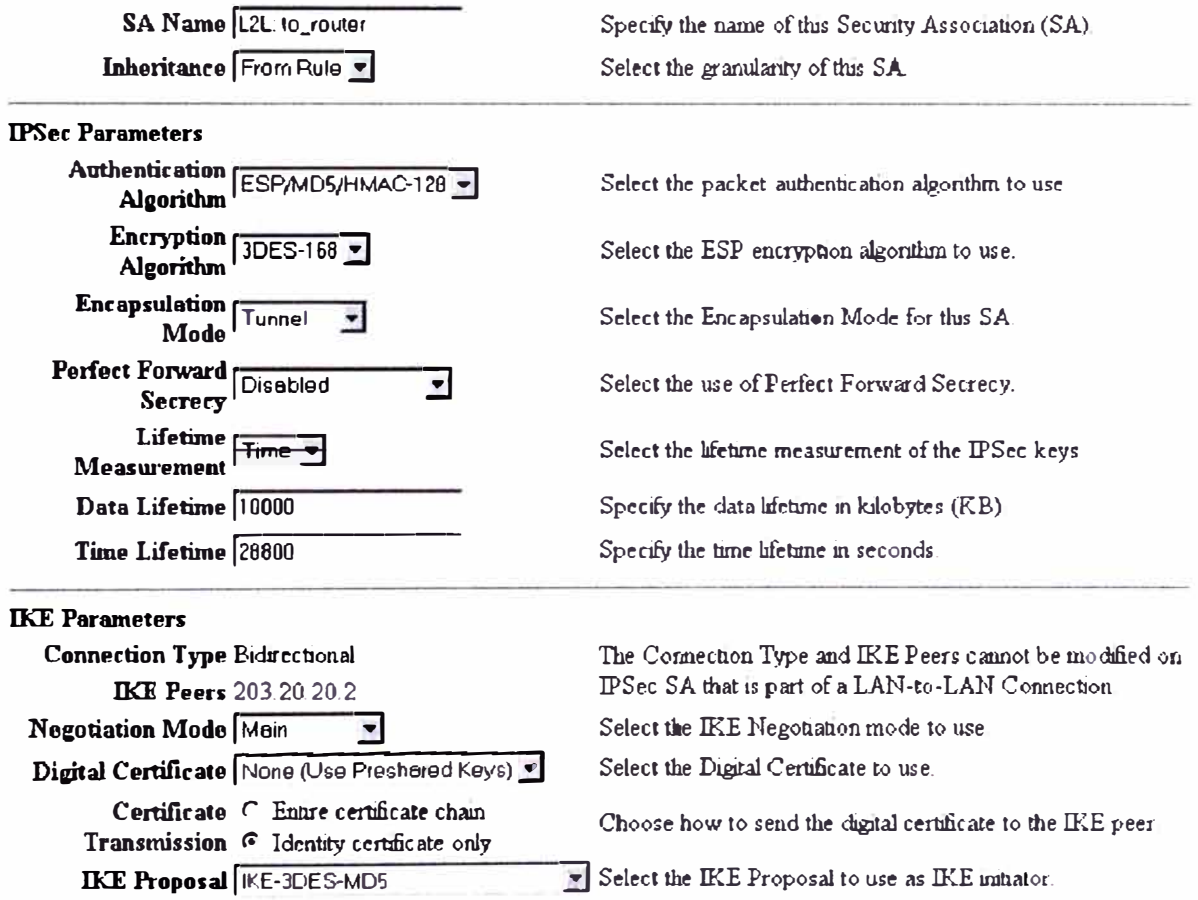
7.- Elegir **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** para confirmar la propuesta IKE active



8.- Elegir **Configuration > Policy Management > Traffic Management > Security Associations** par ver la lista de Asociaciones de Seguridad (SAs)



9.- Dar click en el nombre de la Asociación de Seguridad, y luego clic en **Modify** Para verificar estos parámetros



Verificaciones

Mostramos la lista y opciones de comandos que se pueden usar para verificar si la configuración trabaja apropiadamente.

En el Router

- **show crypto ipsec sa:** Muestra la configuración usada por el actual SA
- **show crypto isakmp sa:** Muestra todos los actuales IKE SAs en un peer
- **show crypto engine connection active:** Muestra las conexiones de sesiones encriptadas actuales para todos los motores de encriptación.

En el Concentrador

Elegir **Configuration** > **System** > **Events** > **Classes** > **Modify** para activar el logging

Estas son las opciones disponibles:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Severity to Log = 1−13

Severity to Console = 1−3

Seleccionar: **Monitoring** > **Event Log** para visualizar el log de eventos.

ANEXO E

LEYENDA DE ICONOS USADOS EN LOS DIAGRAMAS DE RED

LEYENDA DE ICONOS USADOS EN LOS DIAGRAMAS DE RED


Router Cisco


Firewall Cisco


Concentrador Cisco VPN 3000


Servidor


Central IP Nortel BCM


Central TDM Nortel


Adaptador de Teléfonos Análogos Cisco ATA 186


Computadora Personal Desktop


Computadora Personal Laptop


Computadora Personal de Mano (PDA)


Teléfono Analógico


Teléfono IP


Red de Área Local (LAN)

Línea de Enlace Digital de Datos

Conexión VPN


Nube de Red


Nube de Red

ANEXO F
GLOSARIO DE TÉRMINOS

GLOSARIO DE TERMINOS

- 3DES.- Triple Data Encryption Standard. Algoritmo de cifrado de bloques de claves simétricas, que cifra los datos tres veces, con una clave de 56 bits distinta cada vez (168 bits para claves).
- Antispam.- Dispositivo usado para proteger una red determinada de ataques provenientes vía correo electrónico.
- ACL.- Access Control List. Lista o base de datos que define las redes o los recursos a los que pueden tener acceso otras determinadas redes o usuarios.
- AES.- Advanced Encryption Standard. Algoritmo de cifrado de bloques de claves simétricas.
- AH.- Authentication Header. Protocolo IPSec antiguo que en la mayoría de las redes, es menos importante que ESP. AH proporciona servicios de autenticación, aunque no de cifrado. Su función es asegurar la compatibilidad con homólogos IPSec que no admiten ESP, que suministra tanto autenticación como cifrado
- AS/400.- Application System/400. Serie de minicomputadores de IBM, introducida en 1988, que reemplaza las primeras series System/36 y System/38.
- BGP.- Border Gateway Protocol. Protocolo de enrutamiento utilizado entre sistemas autónomos.
- CE.- Customer Equipment. Equipo en instalaciones de cliente.
- DES.- Data Encryption Standard. Norma de cifrado de datos. Utiliza una clave de 56 bits para el cifrado de bloques de claves simétricas.
- DHCP.- Dynamic Host Configuration Protocol. Es un protocolo que usan dispositivos de red para obtener de manera automática, parámetros de red, como dirección IP, default, gateway, DNS, etc., los cuales son proporcionados por un servidor que contiene una base de datos para tal fin.
- E&M.- Ear and Mouth. Es un tipo de señalización utilizada para sistema de transmisión de voz que usa hilos separados para la señalización y la comunicación de voz. El hilo "M" (Mouth – boca) transmite las señales al otro extremo del circuito, mientras que "E" (Ear – oído) las recibe.
- E1.- Es un formato de transmisión digital tanto para datos como para voz, consta de 30 canales para transmisión de voz o datos.
- Encriptación.- Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor.

- ESP.- Encapsulating Security Payload. Carga útil de seguridad encapsulada. Protocolo IPsec que proporciona confidencialidad e integridad de datos.
- Firewall.- Es un elemento de hardware o software utilizado para separar dos o más redes, con el propósito de controlar el tráfico que circula entre ellas, permitiéndolas o negándolas.
- FTP.- File Transfer Protocol. Protocolo de Transferencia de Archivos, que permite a un cliente descargar archivos de un servidor previa verificación por usuario y clave de acceso.
- FXS.- Foreign Exchange Station. Es la interface de un dispositivo de VoIP que permite conectarlo directamente a teléfonos, faxes y puertos troncales en centrales PBX.
- Gateway VPN.- Dispositivo de red que establece una conexión VPN con otro similar ubicado en el otro extremo de la comunicación.
- GRE.- Generic Routing Encapsulation. Es un protocolo para implementar VPNs, el cual se basa en tomar el paquete de un protocolo, encapsularlo en un paquete IP y transportarlo a través de un backbone IP.
- H323.- Es un estándar que especifica los componentes, protocolos y procedimientos que proveen servicios de comunicación multimedia sobre redes de conmutación de paquetes.
- Hash.- Función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc. Los valores hash se utilizan para comprobar la integridad de los datos que se envían a través de canales no seguros.
- HMAC.- Message Authentication Code. Código de autenticación de mensajes basado en funciones hash criptográficas. HMAC puede usarse con cualquier función hash criptográfica iterativa, como por ejemplo, MD5, SHA-1 combinada con una clave compartida secreta. La fuerza criptográfica de HMAC dependerá de las propiedades de la función hash subyacente.
- IKE.- Internet Key Exchange. Se trata de un estándar de protocolo de gestión de claves usado junto con IPSec y otros estándares. Se puede configurar IPSec sin IKE, aunque lo mejora proporcionando funciones adicionales, flexibilidad y facilidad de configuración para el estándar IPSec. IKE permite autenticar los homólogos IPSec, negocia claves IPSec y asociaciones de seguridad IPSec.
- IOS.- Internetworking Operating System. Sistema Operativo que utilizan todos los dispositivos de red de la marca Cisco.
- ISAKMP.- Internet Security Association Key Management Protocol. Conjunto de especificaciones definidas en el RFC 2408 que son usadas junto con IPsec. Definen

el procedimiento para autenticación, creación y administración de asociaciones de seguridad, generación de claves y uso de certificados digitales, cuando se establecen conexiones VPN.

- ISP.- Internet Service Provider. Compañía dedicada a proveer servicios de Internet.
- L2L.- Lan-to-Lan. Es un tipo de conexión VPN conocida también como Site-to-Site o Punto a Punto, el cual es usado para establecer una conexión entre dos entidades o ubicaciones distantes.
- MD5.- Message Digest 5. Función de hash unidireccional que produce un hash de 128 bits. MD5 verifica la integridad y autentica el origen de una comunicación.
- MPLS.- Multi-Protocol Label Switching. Es un estándar que se basa en la conmutación de etiquetas para identificar diferentes grupos de usuarios y tipos de información sobre la red, para lo cual se apoya en la creación de VPNs.
- NAT.- Network Address Translation. Técnica mediante la cual a determinado host o segmento de red se le realiza una conversión de direcciones IP.
- Oakley.- Protocolo basado en Diffie-Hellman y diseñado para ser un componente compatible de ISAKMP, que permite establecer claves secretas para que las utilicen las partes autenticadas.
- P2P.- Peer-to-Peer. Comunicación bilateral exclusiva entre dos host a través de Internet para el intercambio de información en general y en particular de archivos multimedia (Por ejemplo: BitTorrent, eMule, Kazaa).
- PBX.- Private Automatic Branch Exchanges. Centralita privada automática, con conexión a la red pública.
- PDA.- Personal Digital Assistant. Computadora de mano usada generalmente para inventarios móvil en bodegas, tomador de pedidos, etc.
- PKI.- Public-Key Infrastructure. Infraestructura de clave pública. Sistema de autoridades certificadoras (CA) y autoridades de registro (RA) que proporciona compatibilidad para utilizar una criptografía de claves asimétricas en la comunicación de datos mediante funciones, como la gestión de certificados, archivos, claves y tokens.
- PSTN.- Public Switched Telephone Network. Red Pública de Telefonía que es compartida entre muchos usuarios, donde cualquiera de ellos pude establecer comunicación con cualquier otro.
- QoS.- Quality of Service. Calidad de Servicio, son técnicas mediante las cuales se da prioridades de tráfico a ciertos servicios que circulan por una red.
- RDSI.- Red Digital de Servicios Integrados. Tipo de conexiones de red, utilizado para la transmisión digital de cualquier tipo de información (datos, voz, e imágenes).

- RIP.- Routing Information Protocol. Protocolo de enrutamiento dinámico, para lo cual usa algoritmos de vector distancia.
- RFC.- Request for Comments. Petición de comentarios, constituido por un conjunto de archivos donde se describen los estándares TCP/IP, así como el resto de protocolos que se usan en Internet. Se escriben bajo texto ASCII y con una estructura definida.
- Router.- Dispositivo de red cuya función es segmentar redes y enrutar paquetes de datos de acuerdo a una tabla de enrutamiento interna.
- SA.- Security Association. Conjunto de parámetros de seguridad sobre el que se ponen de acuerdo dos homólogos para proteger una sesión específica de un túnel en particular. Tanto IKE como IPSec utilizan SA, aunque las SA son independientes entre sí.
- SAP.- Sistemas, Aplicaciones y Productos para Procesamiento de Datos. Sistema que comprende varios módulos completamente integrados, que abarca todos los aspectos de la administración empresarial en conjunto.
- SHA.- Secure Hash Algorithm. Algoritmo de hash seguro que usan algunos sistemas para generar firmas digitales, como alternativa al MD5.
- SSL.- Secure Socket Layer. Tecnología de cifrado para la Web utilizada con el fin de proporcionar transacciones seguras, como por ejemplo, la transmisión del número de la tarjeta de crédito para el comercio electrónico
- UPS.- Uninterrumpible Power Supply. Fuente de Alimentación Ininterrumpible usada para proveer de alimentación eléctrica a dispositivos conectados a él, cuando éstos dejan de recibir energía de la red eléctrica convencional.
- VPN.- Virtual Private Network. Red privada virtual que proporciona la misma conectividad de red para usuarios en una infraestructura pública que la que se hubiera obtenido en una red privada. Las VPN permiten que el tráfico IP se transfiera con seguridad a través de las redes TCP/IP públicas mediante el cifrado del tráfico de una red a otra. Las VPN utilizan una arquitectura de túneles para cifrar toda la información en el nivel IP.
- VoIP.- Voice over IP. Voz sobre IP es la tecnología que permite la transmisión de voz a través de redes IP en forma de paquetes de datos.

BIBLIOGRAFÍA

1. Gert De Laet, Gert Schauwers, "Network Security Fundamentals", Cisco Press, 08 de Setiembre de 2004.

2. James Henry Carmouche, "IPsec Virtual Private Network Fundamentals", Cisco Press, 19 de Julio de 2006.

3. Santiago Pérez Iglesias, "Publicaciones Telefónica Investigación y Desarrollo. Análisis de Protocolo IPsec: El Estándar de seguridad en IP", Noviembre de 2001.

4. S. Kent and K. Seo, "Security Architecture for the Internet Protocol. (RFC 4301)", IETF, Diciembre de 2005.

5. "IPsec VPN WAN Design Overview", Cisco System, Inc. 2007.

6. Richard Deal, "The Complete Cisco VPN Configuration Guide", Cisco Press, 15 de Diciembre 2005

7. Mark Lewis, "Comparing, Designing, and Deploying VPNs", Cisco Press, 12 de April 12 2006

8. Vijay Bollapragada, Mohamed Khalid, Scott Wainner, "IPSec VPN Design", Cisco Press, 07 de Abril de 2005

9. Victor Olifer, "Different Flavours of VPN: Technology and Applications", The JNT Association, 2007.

10. S. Kent, "IP Authentication Header. RFC 4302", IETF, Diciembre de 2005.

11. S. Kent, "IP Encapsulating Security Payload (ESP). RFC 4303", IETF, Diciembre de 2005.

12. C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH. RFC 2403" IETF, Noviembre de 1998.

13. C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH. RFC 2404" IETF, Noviembre de 1998

14. Mark Egan, "The Executive Guide to Information Security", Symantec Corporation, 2005.

15. Linda McCarthy, "IT Security: Riskinng the Corporation", Prentice Hall PTR, 2003.

16. Andrew G. Mason, "Cisco Secure Virtual Private Networks", Cisco Press - Cisco Systems, Inc., 2002.

17. Greg Bastien & Christian Abera Degu, "CCSP Cisco Secure PIX Firewall Advanced", Cisco Press - Cisco Systems, Inc., 2003.

18. Wesley J. Noonan, "Hardening Network Infrastructure", Mc Graw-Hill / Osborne, 2004.

19. Amrit Tiwana, "Web Security", Digital Press, 1999.

20. Rosalind Resnick & Dave Taylor, "The Internet Business Guide: Riding the Information Superhighway to Profit", Sams Publishing, 1994.

21. Cisco System, Inc.
http://www.cisco.com/

22. Virtual Private Network Consortium (VPNC)
http://www.vpnc.org

23. Internet Engineering Task Force (IETF)
http://www.ietf.org

24. SANS Institute
http://www.sans.org

25. InfoSecurity
http://www.infosecurityonline.org