UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

CONEXIÓN DE SERVIDORES DEL SACMEX CON LAS CONCESIONARIAS MEDIANTE UNA VPN CON CERTIFICADOS DE SEGURIDAD EN OPENVPN

DESARROLLO DE CASO PRÁCTICO

QUE PRESENTA

MIGUEL ANGEL ALARCÓN LÓPEZ

PARA OBTENER EL TÍTULO DE

“INGENIERO EN COMPUTACIÓN”

ASESOR ING. GERARDO TORRES RODRÍGUEZ

MÉXICO 2016

AGRADECIMIENTOS

Quiero agradecer principalmente a mis padres Miguel Angel Alarcón López y Maria del Consuelo López González quienes me han inculcado a no darme por vencido, y dar lo mejor mí, acompañádome a lo largo de mi formación como hombre de bien y como profesionista, brindándome apoyo moral y económico.

Agradezco a mi hermana Angeles y a mi novia Aidali por ser compañeras de desvelos y de estudio los cuales serán recompensados para cada uno, y por la motivación que me han proporcionando.

Debo agradecer a Lic. José Antonio García Monroy por haberme dado la oportunidad de trabajar con él, ya que bajo su supervisión fue posible realizar este proyecto, en donde obtuve diversos conocimientos prácticos y pude desenvolverme en un ambiente laboral aplicando mi conocimiento en la materia, así como permitirme colaborar con su equipo de trabajo el Ing. Alberto, Marco, Octaviano, Ernesto y Rolando los cuales les doy un sincero agradecimiento.

Un agradecimiento en particular a mi asesor el Ing. Gerardo Torres Rodríguez por la orientación y sugerencias en el presente trabajo y los consejos para crecer como profesionista.

ÍNDICE

1. INTRODUCCIÓN

Hoy en día las redes de computadoras juegan un papel muy importante en el área de comunicaciones, debido a esto las empresas han adoptado esta tendencia, ya que, constantemente tienen que mantenerse en comunicación entre los distintos departamentos, o quizá con sucursales; es aquí en donde entran las redes computacionales o redes de datos las cuales nos servirán para lograr establecer comunicación de los diversos equipos que se encuentran en cualquier parte del mundo, recordando el concepto de globalización dentro del cual esta inmersa la tecnologia de comunicaciones.

En el presente documento se plantea y describe la problemática sobre establecer una alternativa eficaz de comunicación punto multipunto como conexión alterna en caso de emergencia, dentro de la red de datos del Sistema de Aguas de la Ciudad de México; la cual está conformada por diferentes centros de acceso por todo el Distrito Federal, a dicho Organismo en lo sucesivo lo denominaremos SACMEX con domicilio en Nezahualcóyotl No. 89, esquina Isabel la Católica, Colonia Centro, Delegación Cuauhtémoc, en México, Distrito Federal.

La red de comunicaciones esta conformada por el edificios que se encuentra ubicado en Izazaga no. 89, Colonia Centro, pisos 4°, 8°, 14° y 16°, los 10 pisos del Edificio de Nezahualcóyotl no. 109, Colonia Centro, así como las instalaciones ubicadas en el SITE Díaz Mirón con dirección prolongación Díaz Mirón no. 411 colonia Santo Tomas, y las redes privadas de 4 concesionarias, estas últimas son empresas “Particulares contratadas por el G.D.F. a través del SACMEX encargadas de tomar lectura de los medidores de agua potable, emisión y distribución de las boletas de los derechos correspondientes, así como la atención a los usuarios y la cobranza de los Derechos y su gestión asociada sostienen actividades con los servicios comerciales, así como la operación y mantenimiento

de la infraestructura hidráulica que forma parte del servicio público antes mencionado.“ Para mayor referencia consultar la siguiente URL: (www.sacmex.df.gob.mx/sacmex/index.php/acerca-de/empresas-concesionarias). Cada empresa concesionaria brinda el servicio a las delegaciones del D.F. Que le fueron asignadas por el G.D.F. las concesionarias tienen sucursales conocidas como OAP (Oficinas de Atención al Publico) las cuales están distribuidas en distintos puntos las delegaciones del D.F.

Cabe mencionar que el 95% de la infraestructura de equipo activo sobre el cual esta implementada la red de datos es de la marca CISCO, las conexiones que hacen posible establecer la comunicación entre el SACMEX y las empresas concesionarias (consesionaria1, consesionaria2, consesionaria3 y consesionaria4) es por medio de diferentes tipos de tecnologias como lo son MPLS (Multiprotocolo Label Switching) y enlaces dedicados, los cuales se encuentran contratados con diferentes CARRIES o ISP (Proveedor de Servicios de internet).

Las concesionarias y por consiguiente las OAP necesitan entrar a un sistema de Información Comercial Centralizado denominado SICOMCE el cual almacena el padrón de usuarios y tomas de agua del Distrito Federal, los cuales son aproximadamente 2, 000,100.

Entre las diferentes tareas que se realizan en dicho sistema se encuentras las siguientes:

- Alta a nuevos usuarios al padron de agua
- Baja a usuarios,
- Cambios en el padron
- Cambios en el uso de tomas (domesticas, no domesticas, mixtas)
- Cambio de diámetro de toma,

- Aclaración de pagos, deudas, consultas históricos,
- Lecturas y facturaciones del cobro de agua.

Las OAP como ya se mencionó anteriormente acceden desde sus instalaciones al SICOMCE, el cual se encuentra hospedado en las instalaciones centrales del SACMEX, dichas OAP se conectan por medio de una red privada establecida con enlaces MPLS de anchos de banda que oscilan entre 512k bps y 2Mbps, por tal motivo se ha detectado que ocasionalmente los enlaces principales sufren algún daño físico o lógico que repercuten en fallas y lo cual se refleja en pérdidas de servicio a la ciudadanía.

A lo largo del trabajo se hará mención de concesionarias y direccionamientos IP, por motivos de seguridad y privacidad de la institución no se mencionara los nombres de las concesionarias, en su lugar serán sustituidos por concesionaria1, concesionaria2, etc. y no se mostraran las direcciones IP originales es por ello que serán utilizadas direcciones IP ficticias.

2. PLANTEAMIENTO DEL PROBLEMA

Las oficinas de atención al público (OAP) realizan su trabajo en el Sistema Comercial SICOMCE, si una o varias OAP de las concesionarias pierde la comunicación con dicho sistema estas dejaran de brindar servicio, debido a que no cuentan con otro medio de comunicación con el SICOMCE, lo cual traerá como consecuencia: molestia a los usuarios por retraso en la facturación y emisión de boletas del cobro de agua y retardos en el pago de agua,entre otros lo que conlleva a pérdidas monetarias para el SACMEX.

El diagnóstico realizado expresa que el problema radica en que no se tiene una alternativa de comunicación u otro medio fisico para restablecer la comunicación por lo cual se han planteado los siguientes cuestionamemientos: ¿Por qué medio establecer la comunicación entre ambos puntos?, ¿Qué medio es seguro?, ¿Bajo

qué tecnología trabajar?, ¿Qué tipo de solución se debe utilizar software o hardware?, si es por software ¿Qué Sistema Operativo utilizar?, o si es por hardware ¿Qué dispositivo dedicado utilizar? .

La sugerencia para esta problemática debe de ser un plan alterno o en otras palabras elaborar un “plan de contingencia”, este solo se utilizara en caso de fallo de comunicación.

Es importante considerar que los recursos economicos en el gobierno local son limitados por lo cual deberán ser optimizados y de preferencia construir alternativas de solucion utilizando software de uso libre, partiendo de la anterior premisa, se han realizado visitas a las OAP con el fin de ver que dispositivos podrían ser de utilidad, en donde se ha detectado, que cuentan con un servicio de tecnología ADSL bajo la responsabilidad de Telmex.

Por otra parte los router de las concesionarias que enlazan al SACMEX por la nube MPLS de Axtel utilizan el protocolo de ruteo BGP (Border Gateway Protocol) para el envío de tráfico según su destino (Izazaga o Díaz Mirón). Tomando en consideración lo anterior es de suma importancia que la solución sugerida deberá tener la capacidad de direccionar el tráfico según su destino ¿Cómo direccionar el tráfico?

Es importante mencionar que el la propuesta a la resolución del problema deberá permitir poder trabajar con todo el entorno del SICOMCE, inclusive implementar el esquema de balanceo de cargas e impresión.

3. ANÁLISIS

En el desarrollo del presente proyecto se realizaron diferentes tareas de investigación, recopilación y prototipos en el mundo del networking una de las ramas de la ingeniería, donde el ingeniero en computación también se desenvuelve, para ser específicos el trabajo se desarrolla en el área de redes de computadoras.

Teniendo en cuenta que las telecomunicaciones es una rama de la ingeniería y que el trabajo se desarrollara en el área de redes de computadora por consiguiente serán definidas:

La ingeniería es el conjunto de conocimientos, habilidades y técnicas aplicadas a la creación, desarrollo, perfeccionamiento e implementación de estructuras o sistemas que proporcionen segurida, eficiencia y calidad con el fin de resolver problemas y satisfacer necesidades de la sociedad.

Según la Facultad de Estudios Superiores Aragón (2013.) “El Ingeniero en Computación, es un profesional especializado en la aplicación de Tecnologías de la Información, capaz de generar y transformar sistemas relacionados con las telecomunicaciones y la computación, proporcionando a su entorno soluciones innovadoras en beneficio de las personas e instituciones que lo requieran”.[1]
Como ya se ha mencionado el ingeniero en computación, puede desempeñarse en el área telecomunicaciones por consiguiente hablaremos de telecomunicaciones para comprender como está ligado a las redes de computadoras.

“Al hablar de telecomunicaciones nos estamos refiriendo a toda la infraestructura, protocolos y dispositivos que permiten la comunicación a distancia con el fin de

[1] http://www.dgae.unam.mx/planes/aragon/Ing-comp_aragon.pdf

trasmitir un mensaje e intercambiar información entre personas desde un punto a otro. Es la forma de comunicarse con las grandes masas de personas ya sea por televisión, radio, internet, etc."[2]

"Un sistema de telecomunicaciones consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones (voz, datos, video etc.)"[3]

Se le conoce como red de telecomunicaciones a la "infraestructura encargada del transporte de la información."[4]

En telecomunicaciones existen tipos redes como:

- Redes de computadoras
- Red telefónica fija, móvil.
- Red global Telex
- Red aeronáutica ACARS

El objetivo principal del trabajo se encuentra dentro de las redes de computadoras ya que es en este tipo de red donde se desarrolla la problemática.
Debido a lo anterior se define las redes de computadoras como la interconexión de dispositivos activos para establecer una comunicación entre sí.

Se propone para resolver la problemática descrita en el presente documento implementar una red privada virtual (VPN), ya que está se encuentra construida dentro de una infraestructura de la red pública como internet, por lo que los puntos a conectar (SACMEX y OAP) cuentan con un medio que les proporciona

[2] https://sites.google.com/site/cursotelecomunicaciones/defincion_telecomunicaciones
[3] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm
[4] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

salida a internet. Las VPN son utilizadas por las empresas para establecer una conexión de la oficina a usuarios remotos por medio de internet. De manera más clara los usuarios remotos para este caso las OAP podrán trabajar en el sistema (SICOMCE) como si estuvieran en la red de área local debido a que se establece una conexión virtual punto a punto o punto multipunto por medio de un enlace a internet a lo que se le conoce como tunneling protocol o tráfico encriptado lo que las hace seguras y los datos viajan de manera correcta a su destino a través de internet.

3.1 Protocolos VPN

Existen diferentes protocolos de túnel, como:

PPTP (Protocolo de túnel punto a punto), L2F, L2TP (Protocolo de túnel de capa dos), IPSec y OpenVPN.

A continuación se mostrara en la tabla 1 las características de los protocolos antes mencionados.

Protocolo	Características
PPTP	• Desarrollado por Microsoft. • Capa 2 • Encriptación básica (128 bits). • OS (Sistema operativo) que lo soporta: Windows, Mac OS X, Linux, iOS, Android, DD-WRT. • Autenticación MS-CHAPv2.
L2F	• Desarrollado por CISCO • Capa 2 • Encriptación básica (128 bits).

	• Puede trabajar con Frame Relay o ATM. • Autenticación por: PPP (Point-to-Point Protocol), TACACS+ (Terminal Access Controller Access Control System) y RADIUS (Remote Authentication Dial-In User Service).
L2TP	• Diseñado por la IETF. • Capa 2 • Fusión de PPTP y L2F. • OS (Sistema operativo) que lo soporta: Windows, Mac OS X, Linux, iOS y Android. • Autenticación: PPP, PAP, CHAP y RADIUS.
IPSEC	• Diseñado por la IETF. • Encriptación fuerte (256 bits) • Capa 3 • OS (Sistema operativo) que lo soporta: Windows, Mac OS X, Linux, iOS y Android. • Autenticación HEADER (AH). • Autenticidad de origen, integridad y protección por medio de protocolo ESP (Encapsulating Security Payload).
OpenVPN	• OpenVPN project / OpenVPN Technologies, Inc. • Encriptación fuerte (160 bits y 256 bits) • Capa 2 y 3 • OS (Sistema operativo) que lo soporta: Windows, Mac OS X, Linux, iOS y Android. • Certificados de seguridad. • Encriptación simétrica o asimétrica.

Tabla 1. Características principales de los protocolos de redes privadas virtuales "VPN".

De la tabla anterior se escogieron dos posibles soluciones, el protocolo IPSec y el protocolo OpenVPN, de los cuales IPSec puede sugerir una solución por software o por hardware y OpenVPN solo por software. Estos protocolos fueron seleccionados debido a la seguridad con la que se cuenta y el tipo de VPN que se puede configurar en este caso sitio a sitio (LAN to LAN).

3.2 Solución IPSec hardware

Para esta solución es necesario contar con un dispositivo de uso específico "VPN IPSec" en cada punto a conectar. Los dispositivos deberán contar con direcciones IP públicas fijas o ip publicas dinamicas, para la configuración de la VPN. Es por ello que es necesario contratar un servicio de comunicaciones denominado enlace dedicado o un enlace ADSL.

En las instalaciones del SACMEX se cuenta con un router cisco small business modelo RV042 en el que se puede configurar una VPN utilizando el protocolo IPSec, a su vez hay un Firewall palo alto y balanceadores de carga que permiten este protocolo.

El SACMEX cuenta en su infraestructura con 2 enlaces dedicados los cuales fureron utilizados para probar esta posible solución. Para ello se armaron los siguientes laboratorios.

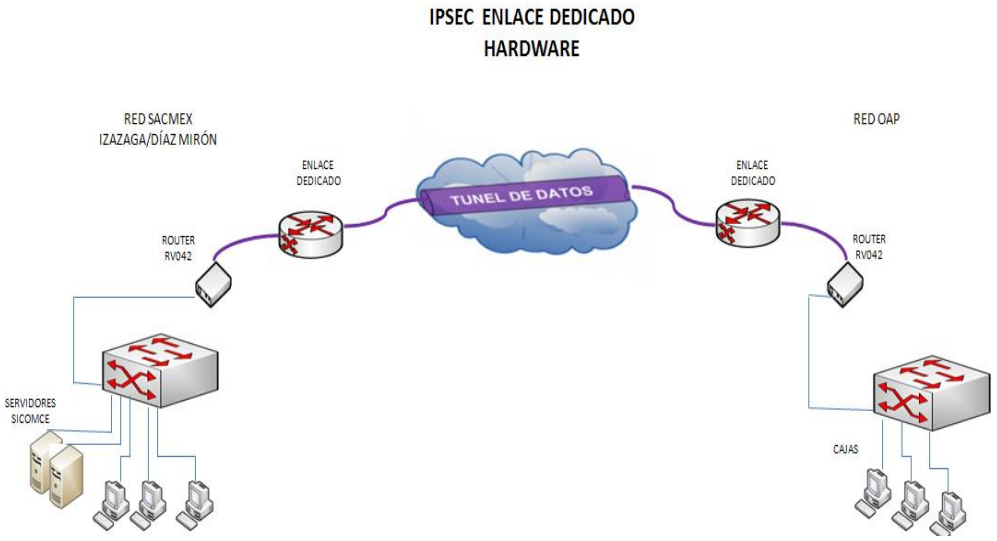


Figura 1. Diagrama conexión izazaga/Díaz Míron a OAP por enlace deicado.

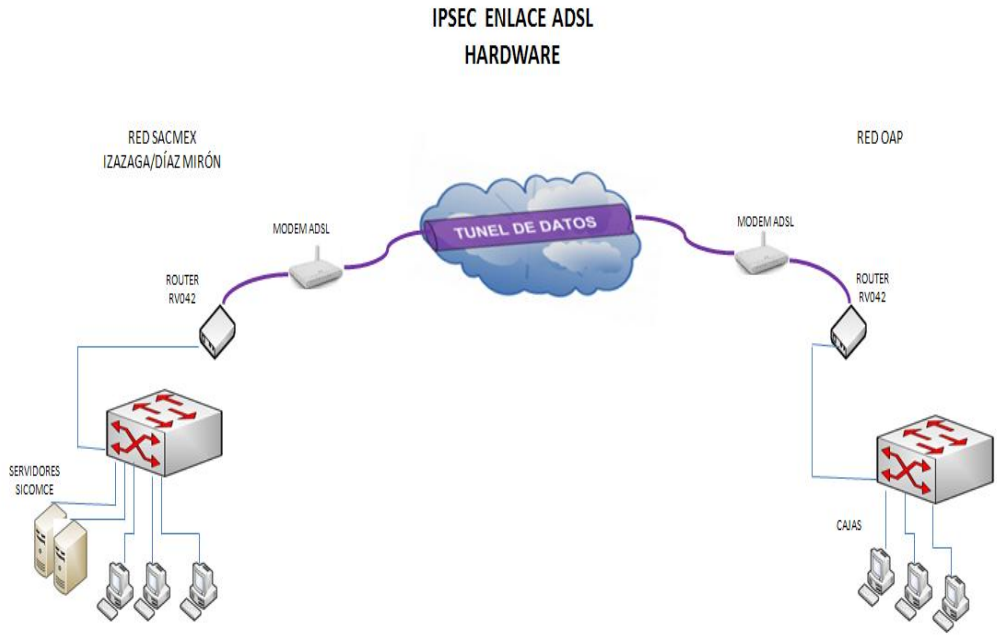


Figura 2. Diagrama conexión izazaga/Díaz Míron a OAP por enlace ADSL.

En la tabla 2 se muestran los costos que conyeva realizar un proyecto por dispositivos de uso especifico.

Tabla 2. Costos de dispositivos y servicios de la solución IPSec hardware.

DISPOSITIVO O SERVICIO	COSTO POR PIEZA	CANTIDAD	COSTO
Router RV042	$3,500.00 M.N	32	$112,000.00 M.N.
Enlace E1 (2)	$10,000.00	24	$240,000.00 M.N.
o			
ADSL (8)	$500.00	32	$16,000.00 M.N.
DynDNS	$500.00	8	$4000.00 M.N.
TOTAL			$372,000 M.N.

3.3 Solución IPSec software

En el caso de solución por software deberán instalar un servidor de VPN de preferencia en Linux (por su estabilidad, confiabilidad y software libre) en cada punto a conectar este deberá contar con dos tarjetas de red, de igual forma esta solución ocupa direcciones IP públicas, para la configuración de los servidores. Al igual que la solución por hardware, se podrá hacer la conexión por medio de enlaces dedicados o enlaces ADSL.

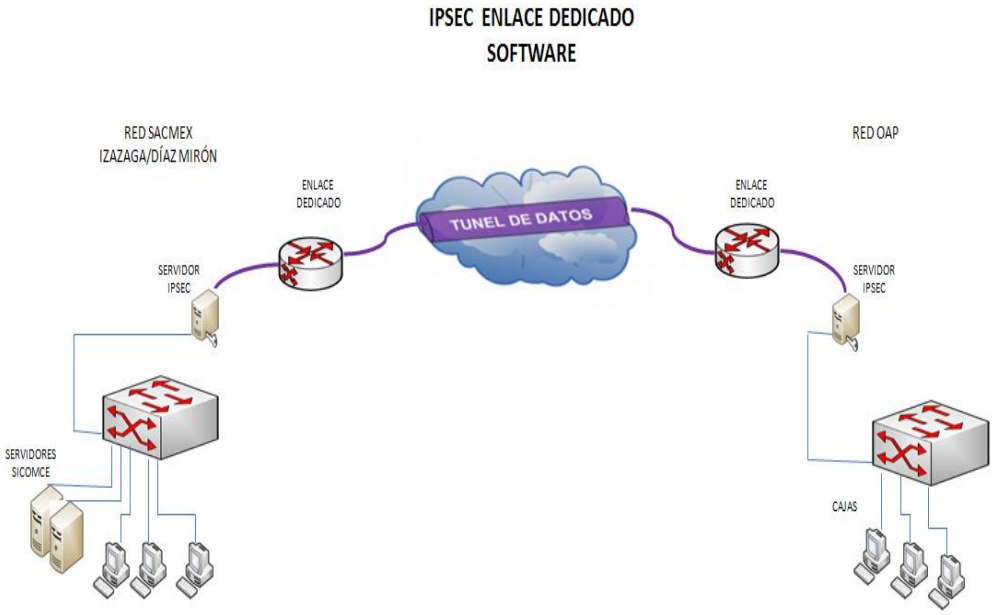


Figura 3. Diagrama conexión izazaga/Díaz Míron a OAP por enlace dedicado.

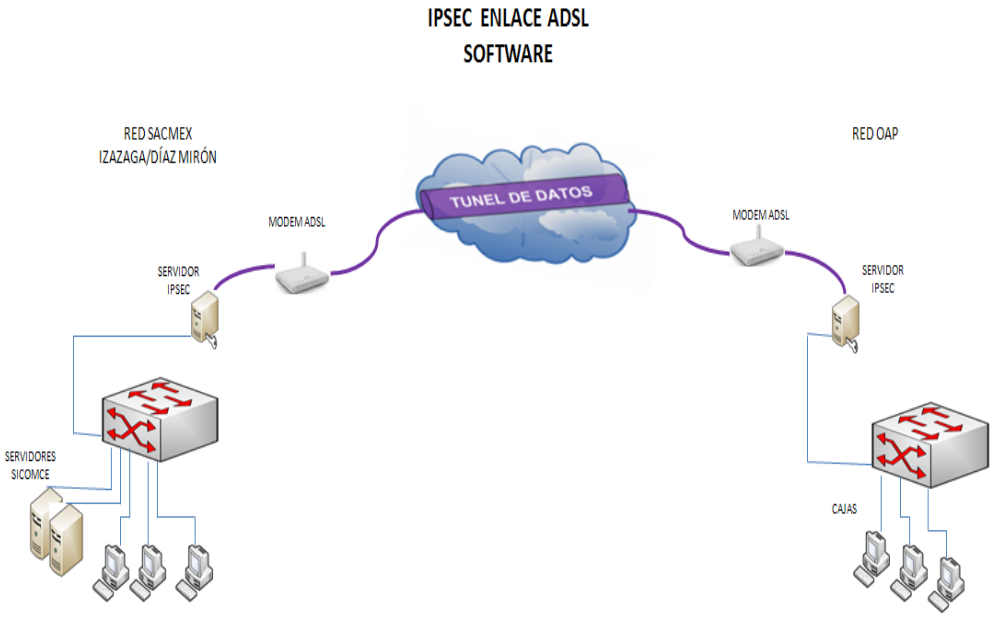


Figura 4. Diagrama conexión izazaga/Díaz Míron a OAP por enlace dedicado.

Tabla 3. Costos de servicios de la solución IPSec software.

DISPOSITIVO O SERVICIO	COSTO POR PIEZA	CANTIDAD	COSTO
Computadoras	$5000.00 M.N.	32	$160,000.00 M.N.
Tarjeta de red	$180.00 M.N.	32	$5760.00 M.N.
Enlace E1	$10,000.00	24	$240,000.00 M.N.
o			
ADSL	$500.00	32	$16,000.00 M.N.
DynDNS	$500.00	8	$4000.00 M.N.
TOTAL			$425,760.00 M.N.

3.4 Solución OpenVPN

La solución de OpenVPN es por medio de software, por consiguiente es necesario instalar y configurar un servido VPN en Linux (por su estabilidad, confiabilidad y software libre) utilizando el protocolo OpenVPN, los servidores de VPN deben contar con dos tarjetas de red, por otra parte se necesitaran configurar clientes los cuales se conectaran al servidor de OpenVPN, estos serán configurados en maquinas con sistema operativo Linux server, al igual que el servidor deberán contar con dos tarjetas de red cada equipo cliente.

Las computadoras que juegan el papel de cliente en este caso las OAP de cada concesionaria para establecer comunicación con el servidor de VPN podrán

hacerlo por medio de un dispositivo ADSL con salida a internet. Retomando lo antes mencionado las OAP cuentan con este servicio con el ISP Telmex denominado Internet Infinitum. Es importante mencionar que los clientes utilizaran el enlace ADSL para conectarse con el servidor no importando las soluciones mencionadas posteriormente.

Los servidores deberán estar ubicados físicamente en donde habita el sistema SICOMCE de manera que uno estará ubicado en el edificio de Izazaga y el otro en Díaz Mirón además en estos sitios se cuenta con enlaces dedicados los cuales pueden proporcionar direcciones IP públicas para la configuración de estos, pero es importante mencionar que esos enlaces fueron contratados para un fin por lo tanto las direcciones IP públicas son prestadas a lo que se sugiere contratar enlaces ADSL así se podrá tener un doble plan de contingencia asegurando de esta forma la conexión entre el SACMEX y las concesionarias.

Se recomienda que los enlaces dedicados sean de 2 Mbps o más debido a que el caudal de datos es estable, tanto de bajada como de subida es por ello que su costo es más elevado en consecuencia entre más Mbps más se eleva su costo y en los enlaces ADSL se sugiere 10 Mbps para obtener buenos tiempos de respuesta ya que en estos, su caudal de datos es variable en la subida y en la bajada es decir este al querer subir datos es menor la velosidad, en un enlace de 10 Mbps su velocidad de subida osila entre 3 Mbps y 2 Mbps,Este tipo de enlaces pueden reducir su servicio hasta un 60%; previendo este inconveniente se parte de 10 Mbps lo cual no afectara el performance de transmisión además de que este enlace es mas varato a comparación de un enlace dedicado, las computadoras deberán tener un procesador de dos nucleos o más, las tarjetas de red deberan trabajar a 100 Mbps y a 1000 Mbps por consiguiente el cable de red (pach cord) que se sugiere es un categoría 6.

Con fines informativos se presenta en la tabla 4 los costos que conlleva realizar la solución por esta alternativa.

Tabla 4. Costos de servicios de la solución OpenVPN.

DISPOSITIVO O SERVICIO	COSTO POR PIEZA	CANTIDAD	COSTO
Computadoras	$5000.00 M.N.	32	$160,000.00 M.N.
Tarjeta de red	$180.00 M.N.	32	$5760.00 M.N.
Enlace E1 (2)	$10,000.00 M.N	2	$20,000.00 M.N.
o			
ADSL (8)	$500.00 M.N	32	$16,000.00 M.N.
DynDNS	$500.00	4	$2000.00 M.N.
TOTAL			$203,760.00 M.N.

Como ya se menciono anteriormente el SACMEX cuenta en su infraestructura con enlaces dedicados y la mayoría de las empresas concesionarias reutilizaran computadoras, retomando el uso de recursos existentes en las OAP se tienen enlaces ADSL por lo tanto los gastos se reduciran.

Luego de hacer las observaciones al protocolo de IPSec (vía software y hardware) y al protocolo OpenVPN **se escogió este último por su bajo coste, seguridad, estabilidad, escalabilidad y por los tiempos de respuesta que fueron entregados**. Las soluciones a implementar con OpenVPN serán vía enlace dedicado y vía ADSL previniendo así un posible fallo en los enlaces dedicados,

por consiguiente tanto los servidores como los clientes de OpenVPN contaran con dos configuraciones, habilitando solamente una configuración, la designada por el administrador según sea el caso de contingencia.

3.4.1 Solución OpenVPN por enlace dedicado

Los equipos que fungirán como servidores deberán contar con una dirección IP pública para que puedan ser vistos de cualquier punto del mundo. Las direcciones IP pública serán proporcionadas por un enlace dedicado que tiene el SACMEX contratado con el ISP de Telmex.

3.4.2 Solución OpenVPN por enlace ADSL

Al igual que la solución por enlace dedicado los servidores OpenVPN deberán contar con una dirección IP pública para que puedan ser vistos de cualquier punto del mundo. La dirección IP pública será proporcionada por un enlace con tecnología ADSL, pero como esta tecnología proporciona una IP dinámica se le asignara un dominio al servidor, el cual será dado de alta en un servidor de dominios con IP dinámica para su publicación, en este caso se utilizara el servidor DynDNS.

3.4.3 Definición de elementos que comprende OpenVPN

Ahora veremos los elementos que comprende este protocolo de VPN.

“Cifrado

Es el proceso que transforma tu información de manera que no cualquier usuario pueda entenderla, se realiza con base a un elemento único conocido como llave, así nadie, excepto el poseedor de la llave puede leerla. El procedimiento inverso al cifrado es el descifrado.

Llave pública y llave privada

Son un par de “llaves” digitales asociadas a una persona o entidad y generadas mediante métodos criptográficos. La llave pública es usada para

cifrar la información, haciendo una analogía, es como la llave utilizada para cerrar una puerta y mantener fuera a cualquier persona mientras que la llave privada se usa para descifrar, es decir, la llave que abre la puerta y sólo la posee la persona autorizada, por lo tanto ésta debe mantenerse en secreto.

Firma digital

Del mismo modo que tu firma autógrafa, es un elemento que te identifica y distingue de las demás personas y que al firmar con ella adquieres derechos y obligaciones. La firma digital se genera con base a la llave privada de quien firma y por lo tanto es única.

Autoridad Certificadora (AC)

Una Autoridad Certificadora (AC, en inglés CA) es una entidad confiable que se encarga de garantizar que el poseedor de un certificado digital sea quien dice ser, bridando confianza a ambas partes de una comunicación segura SSL/TLS.

Certificado Digital SSL/TLS

Es un documento digital único que garantiza la vinculación entre una persona o entidad con su llave pública.

Contiene información de su propietario como nombre, dirección, correo electrónico, organización a la que pertenece y su llave pública, así como información propia del certificado por mencionar: periodo de validez, número de serie único, nombre de la AC que emitió, firma digital de la AC cifrada con su llave privada y otros datos más que indican cómo puede usarse ese certificado."[5]

"OpenVPN puede ser configurado por 2 tipos de interfaz de red virtuales:

[5] Ramírez D. 2011

TUN: Esta interfaz simula que es un dispositivo Ethernet que trabaja sobre la capa 3 del modelo OSI, esta interfaz es ocupada cuando hacemos un Ruteo dentro de la red de la VPN.
TAP: Esta interfaz simula que es un dispositivo Ethernet que trabaja sobre la capa 2 del modelo OSI, esta interfaz es ocupada cuando queremos utilizar redes en modo puente".[6]

Para la implementación, la interfaz en la que se configurará OpenVPN será TUN, por que este trabaja en capa 3 del modelo OSI, debido a que se trabajara con un direccionamiento ajeno al de la red local, de esta forma será posible encaminar el trafico hacia su destino.

OpenVpn puede trabajar con los protocolos de la capa de transporte TCP o UDP del modelo TCP/IP, describiremos cómo trabajan estos protocolos.

TCP (Protocolo de Control de Transmisión) es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión libre de errores, sin pérdidas y con seguridad, es un protocolo fiable en el flujo de bits entre aplicaciones.

UDP (Protocolo de datagrama de usuario) es un protocolo no orientado a conexión, este protocolo es muy simple ya que no proporciona detección de errores, solo añade la información necesaria para la comunicación extremo a extremo al paquete que envía al nivel inferior.
Con respecto a los protocolos de transporte estos se tendrán que vincular a un puerto lógico es por ello que a continuación se define puerto lógico:

[6]http://www.linuxparatodos.net/web/comunidad/base-de conocimiento//wiki/Base+de+Conocimiento/Servidor+Virtual+Private+Network+(VPN)

Puertos lógicos. “Zona, o localización, de la memoria de un ordenador que se asocia con un puerto físico o con un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.”[7]

El manejo de los puertos lógicos nos permite tener un cierto control sobre conexiones, así como abrirlas, cerrarlas, "escuchar" posibles accesos por cualquiera de ellas.

Por lo tanto los protocolos de transporte TCP y UDP se vinculan a un puerto lógico por el cual OpenVPN previamente instalado fungirá como servidor, este se comunicara con las máquinas cliente de la red a la que estará conectada.

Para este caso el protocolo de transporte que se utilizara en la configuración de OpenVPN será TCP y será vinculado al puerto 1194 ya que viene predefinido por OpenVPN.

Se elegirá TCP debido a que está hecho para poder enviar grandes cantidades de información y con la fiabilidad que llegara completo el mensaje.

Por consiguiente se define IP privada e IP publica ya que estas las utilizaremos para la configuración de OpenVPN. Pero antes hay definir que es una dirección IP.

“Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP, que corresponde al nivel de red del protocolo TCP/IP”. [8]

[7] https://sites.google.com/site/gestionderedesdedatossmt/puertos-y-servicios/puertos-fisicos/puertos-fisicos
[8] http://www.direccionip.com/

Dirección IP privada.

Esta es una dirección que se encuentra dentro de una red de área local, debido a lo anterior, esta dirección no puede ser vista por algún equipo que se encuentre fuera de este tipo de red.

Dirección IP pública.

Este tipo de dirección es aquella que puede ser vista desde cualquier computadora conectada a internet.

Para la configuración de OpenVPN se necesita contar con dos direcciones IP una del tipo privada está se comunicará con la red de área local, y la otra del tipo publica por la cual las maquinas cliente podrán firmarse en el servidor de OpenVPN y establecer el túnel.

Túneles.

El cliente deberá ser capaz de conectarse a los dos servidores de VPN (Izazaga y Díaz Mirón), dicho de otra manera el cliente deberá levantar dos túneles, para ello se tendrá que configurar un archivo en el cliente por cada servidor de VPN, así mismo el servicio de OpenVPN se iniciara en el cliente por servidor.

Direccionamiento

Como se ha dicho el enlace de Axtel de tipo MPLS direcciona el tráfico por medio del protocolo de ruteo BGP según su destino (Izazaga o Díaz Mirón) por lo que será necesario implementar rutas estáticas en los servidores de VPN, pero se tiene que ser cuidadoso al implementar este tipo ruteo debido a que las B.D. (Bases de datos) del sistema SICOMCE se encuentran dentro del mismo segmento de red, considerando lo anterior no se deberá implementar ruteo estático con máscara de 24 bits en los servidores de VPN debido a que el trafico

no llegaría a su destino si la ruta que sigue no es el camino correcto, así que se implementará ruteo estático con un destino especifico en otras palabras se utilizara mascara completa de 32 bits así de esta forma se asegura que el trafico se vaya por el camino previamente indicado.

4. DISEÑO

4.1 Red de producción

A continuación se presenta un mapa de la “red de producción” actual del SACMEX con las concesionarias y a su vez las OAP.

Como se puede apreciar la siguiente imagen muestra los enlaces que comunican el nodo Izazaga hacia las empresas concesionarias y OAP y de igual manera el nodo Díaz Mirón hacia las empresas concesionarias y OAP.

Cuando una OAP de cualquier empresa concesionaria trabaja en el sistema SICOMCE el router del enlace MPLS manda el tráfico hacia la nube de MPLS en donde un “ingress router” (router de ingreso) recibirá el trafico, lo etiquetara y enviara por medio del protocolo BGP según su destino, a un egress router (router de salida) en donde este a su vez manda el trafico al router del enlace MPLS para posteriormente reenviar el trafico al Core el cual lo encamina hacia los servidores del entorno SICOMCE ver figura 5.

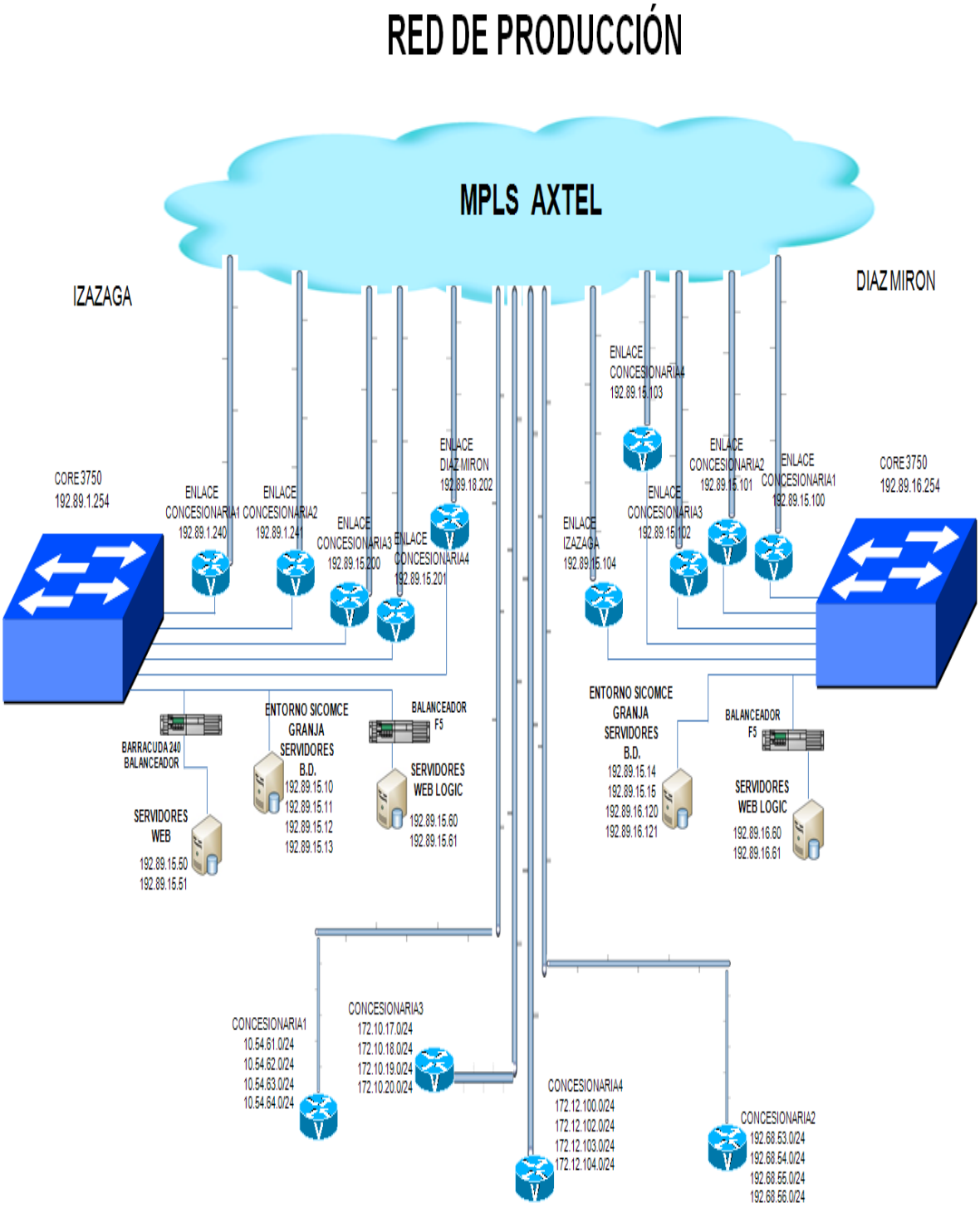


Figura 5. Red de producción del entorno SICOMCE del SACMEX.

Es necesario mencionar de la imagen anterior que cada direccionamiento de los router que representan las empresas concesionarias es una OAP.

Con la finalidad de ser más puntual en el enlace de comunicación de una OAP hacia el SACMEX enseguida se presenta una imagen del plano de trabajo de una OAP de la empresa concesionaria1 hacia el SACMEX (Izazaga y Díaz Mirón), ver figura 6.

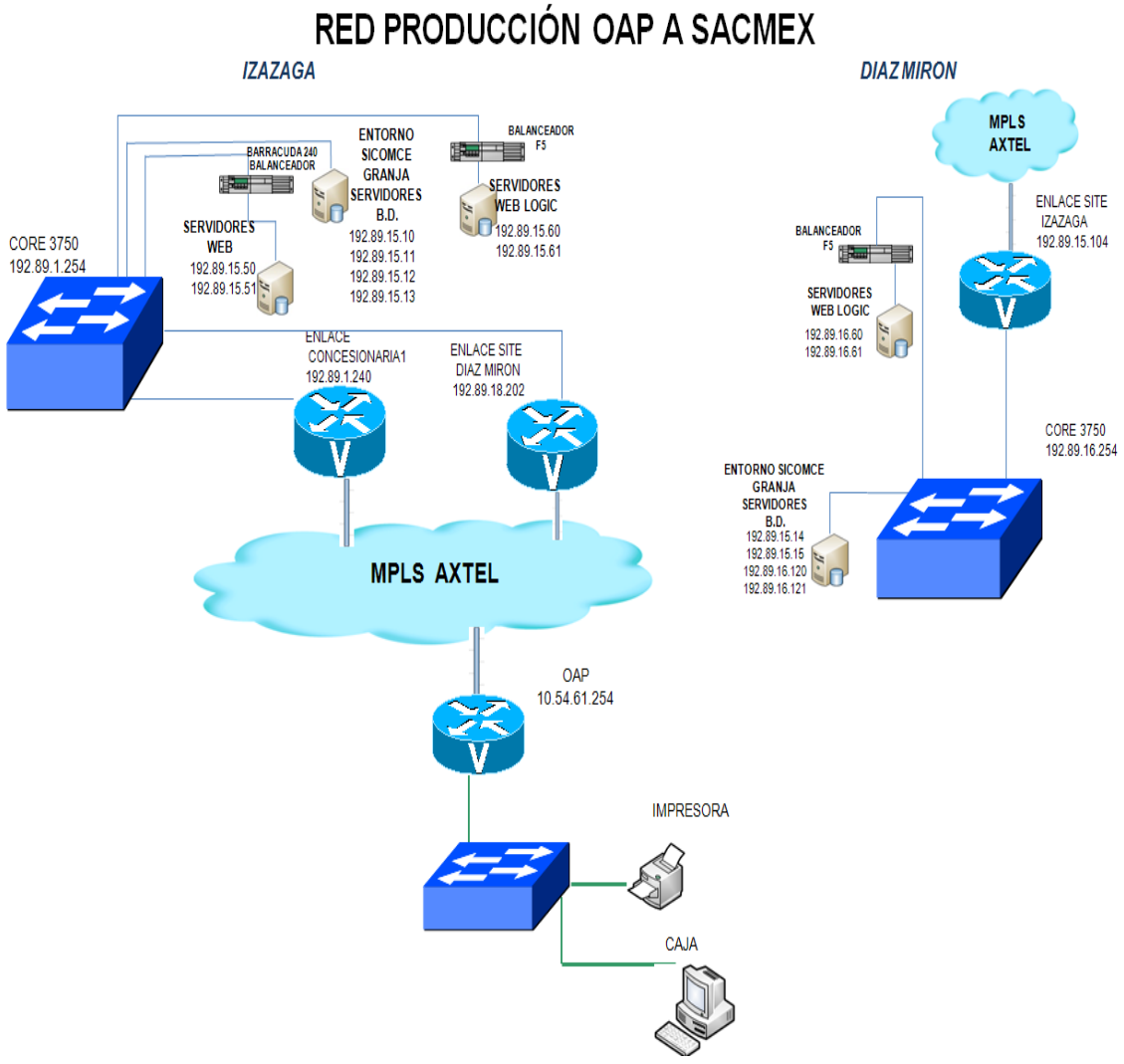


Figura 6. Red de producción del entorno SICOMCE de una OAP al SACMEX.

4.2 Características de equipos servidor y equipos cliente

Considerando el plan de trabajo actual será necesario montar dos servidores de VPN, uno estará ubicado en Izazaga y el otro en Díaz Mirón, cada servidor deberá contar con 2 tarjetas de red a las que se le proporcionara una dirección IP publica y una dirección IP privada, las direcciones IP publicas será proporcionadas por un enlace dedicado que se tiene contratado con el ISP de Telmex o por un enlace ADSL y las direcciónes IP privadas se tomaran de uno de los segmentos privados con los que se cuenta, también deberán de contar con SSH (Secure SHell) para la administración remota del equipo, es necesario instalar traceroute esta herramienta será útil para en caso de falla saber que camino está tomando y en donde se está quedando.

Por otro lado las concesionarias por cada OAP deberán contar con una PC cliente de la VPN, al igual que los servidores deberán contar con 2 tarjetas de red, estas a su vez fungirán el papel de router para las PC´s de producción (Cajas) de las OAP, es por ello que se denominarán como un cliente-servidor, los cliente-servidor les será asignada en una tarjeta de red una dirección IP privada, esta no debe de ser cualquiera, la dirección IP que le será proporcionada es la del router del enlace MPLS debido a que esta es la puerta de enlace que utilizan las cajas para trabajar en el SICOMCE y en la otra tarjeta de red se les configurara servicio por DHCP (Dynamic Host Configuration Protocol) el cual será proporcionada por el dispositivo ADSL de Telmex o Axtel, este nos proporcionará salida a internet y por lo consiguiente por el medio para llegar al servidor de VPN y establecer la conexión vía VPN. De igual manera al cliente-servidor se le instalará SSH y traceroute.

4.3 Red plan de contingencia OAP a SACMEX por medio de enlace dedicado

En seguida se presenta un escenario en donde deja de funcionar un enlace MPLS de una OAP hacia Izazaga y Díaz Mirón y se restablece la comunicación por medio de la VPN utilizando enlaces dedicados, ver figura 7.

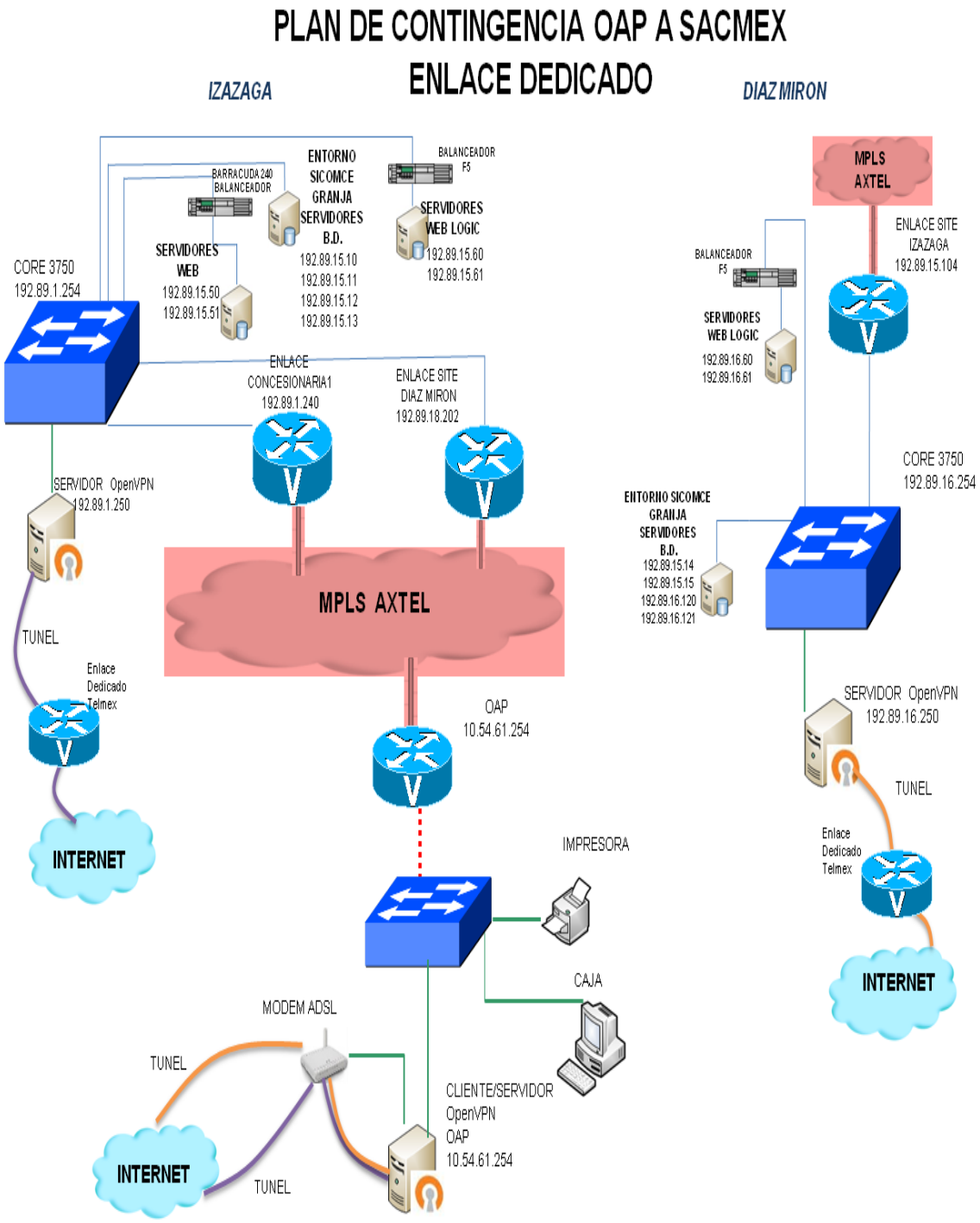


Figura 7.Plan de contingencia del entorno SICOMCE de una OAP al SACMEX por medio de un enlace dedicado.

En la imagen anterior lo que esta sombreado en rojo corresponde a el enlace MPLS, el cual se encuentra inactivo debido a problemas de comunicación, para restablecer la comunicación se observa que una de las tarjetas de red de los servidores OpenVPN se conecta a la red de área local y la otra tarjeta de red a un enlace dedicado con salida a internet. Suponiendo que deja de funcionar el enlace MPLS de la OAP hacia el SACMEX, deberá de ser desconectado de manera fisica de la red de la OAP el router del enlace MPLS y se procederá a conectarde manera fisica a la red local el cliente-servidor el cual utilizara la dirección IP del router del enlace MPLS, es por ello que solo en caso de que el enlace falle el cliente-servidor podrá ser conectado a la red de no ser así deberá permanecer desconectado de la red, la otra tarjeta de red del equipo cliente-servidor será conectada a un modem ADSL, el cual proporcionara salida hacia internet y por consiguiente permitirá establecer comunicación con el servidor VPN y a su vez iniciar el servicio del túnel lo que permitirá a las cajas de la OAP seguir trabajando de forma segura en el SICOMCE. Es de real importancia mencionar que para los usuarios es transparente este cambio, debido a que no hay que modificar ninguna configuración en la red local de la OAP que posteriormente pueda afectar al ser regresada a su conexión original.

De esta forma la OAP podrá seguir operando de forma normal, es recomendable trabajar con 3 cajas para que no baje el performance.

4.4 Red plan de contingencia OAP a SACMEX por medio de enlace ADSL

En el siguiente escenario deja de funcionar un enlace MPLS (este se observa sombreado de rojo), de una OAP hacia Izazaga y Díaz Mirón y se restablece la comunicación por medio de la VPN utilizando enlaces ADSL.

Las conexiones serán similares a las mencionadas en el plan de contingencia por enlace dedicado lo único que cambiaria es poner un modem ADSL, ver figura 8.

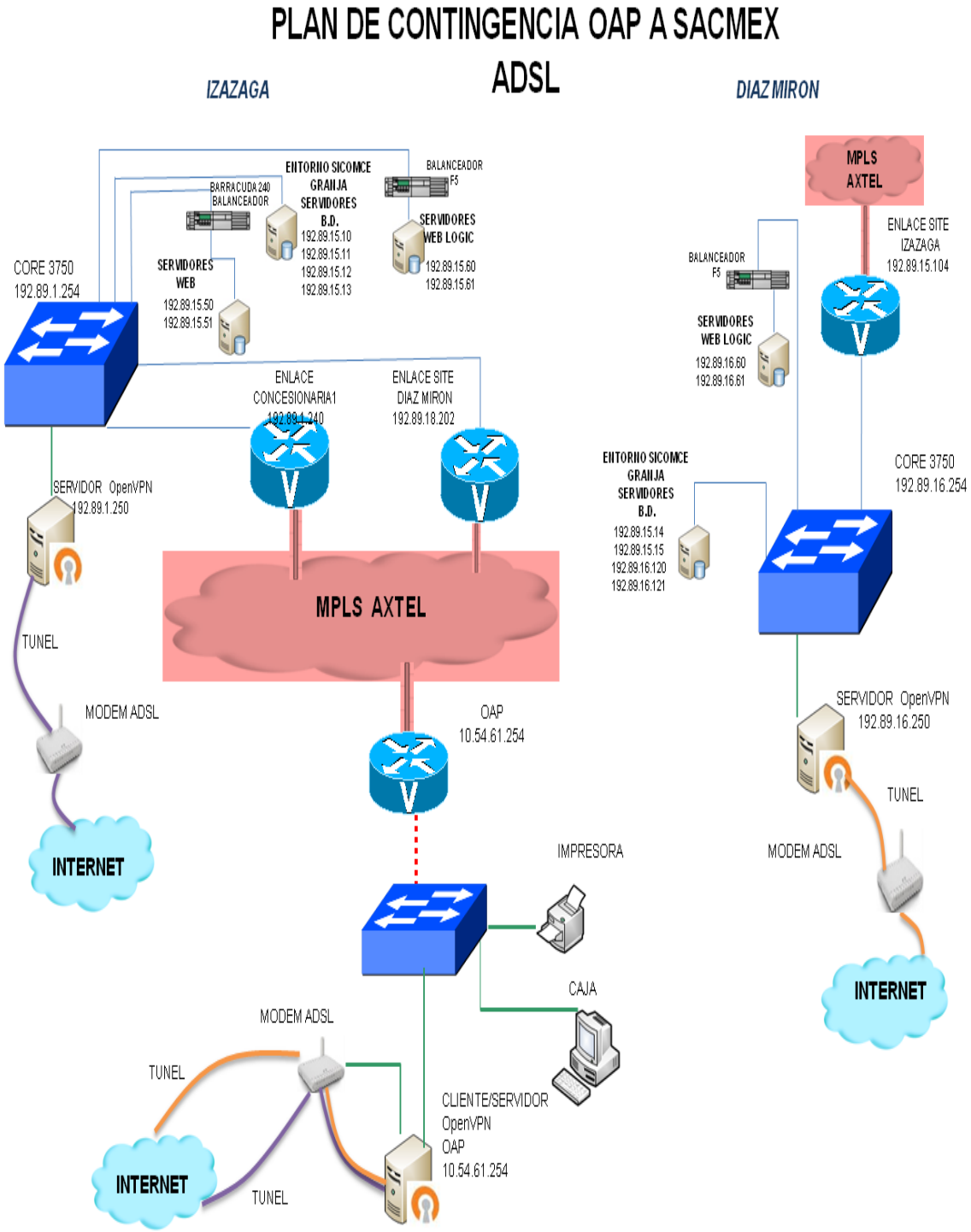


Figura 8.Plan de contingencia del entorno SICOMCE de una OAP al SACMEX por medio de un enlace ADSL.

4.5 Red plan de contingencia concesionarias a SACMEX por medio de enlaces dedicados

En seguida se presenta un escenario en donde deja de funcionar todo el enlace MPLS por consiguiente deja de haber comunicación en todas las OAP de las concesionarias hacia el SACMEX (Izazaga y Díaz Mirón), se restablece la comunicación por medio de la VPN utilizando como medio un enlace dedicado, ver figura 9.

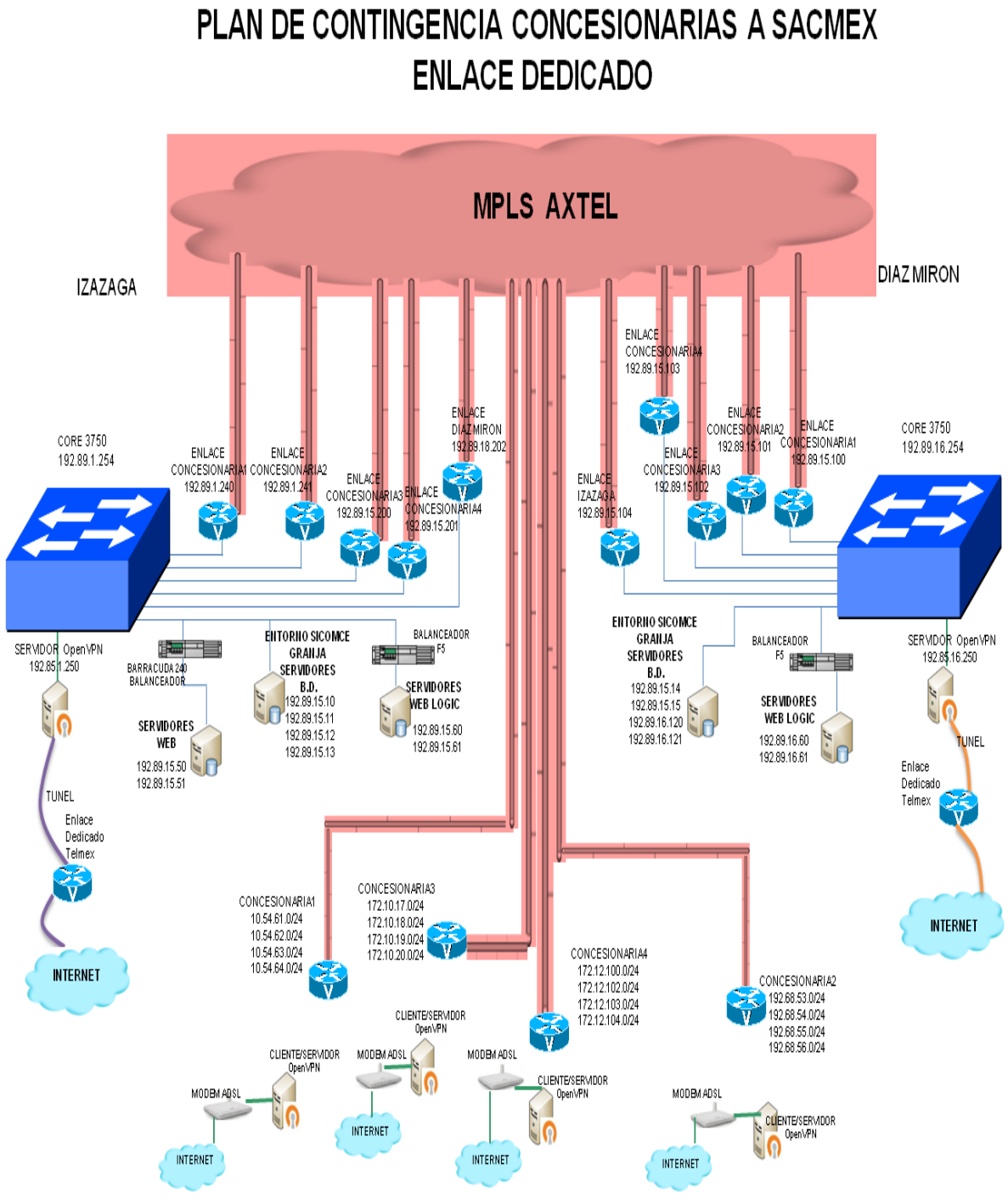


Figura 9.Plan de contingencia del entorno SICOMCE de concesionarias al SACMEX por medio de enlaces dedicados.

Como se puede apreciar en la imagen anterior los enlaces MPLS dejan de transmitir por algún problema (En la imagen se puede apreciar el corte de comunicación de los enlaces MPLS los cuales están sombreados de rojo), para este problema se sugiere conectar todos los clientes-servidores de todas las OAP de las concesionarias y levantar el servicio de OpenVPN para que puedan establecer comunicación con el SACMEX, antes de conectar los clientes-servidores a la red, se deberá desconectar los router del enlace MPLS de las OAP para no causar conflictos en la red “overlap”.

4.6 Red plan de contingencia concesionarias a SACMEX por medio de enlaces ADSL

A continuación se muestra un escenario en donde dejo de funcionar los enlaces MPLS (sombreados de rojo) y se restablece la comunicación de las concesionarias hacia el SACMEX por medio de OpenVPN utilizando un enlace ADSL, ver figura 10.

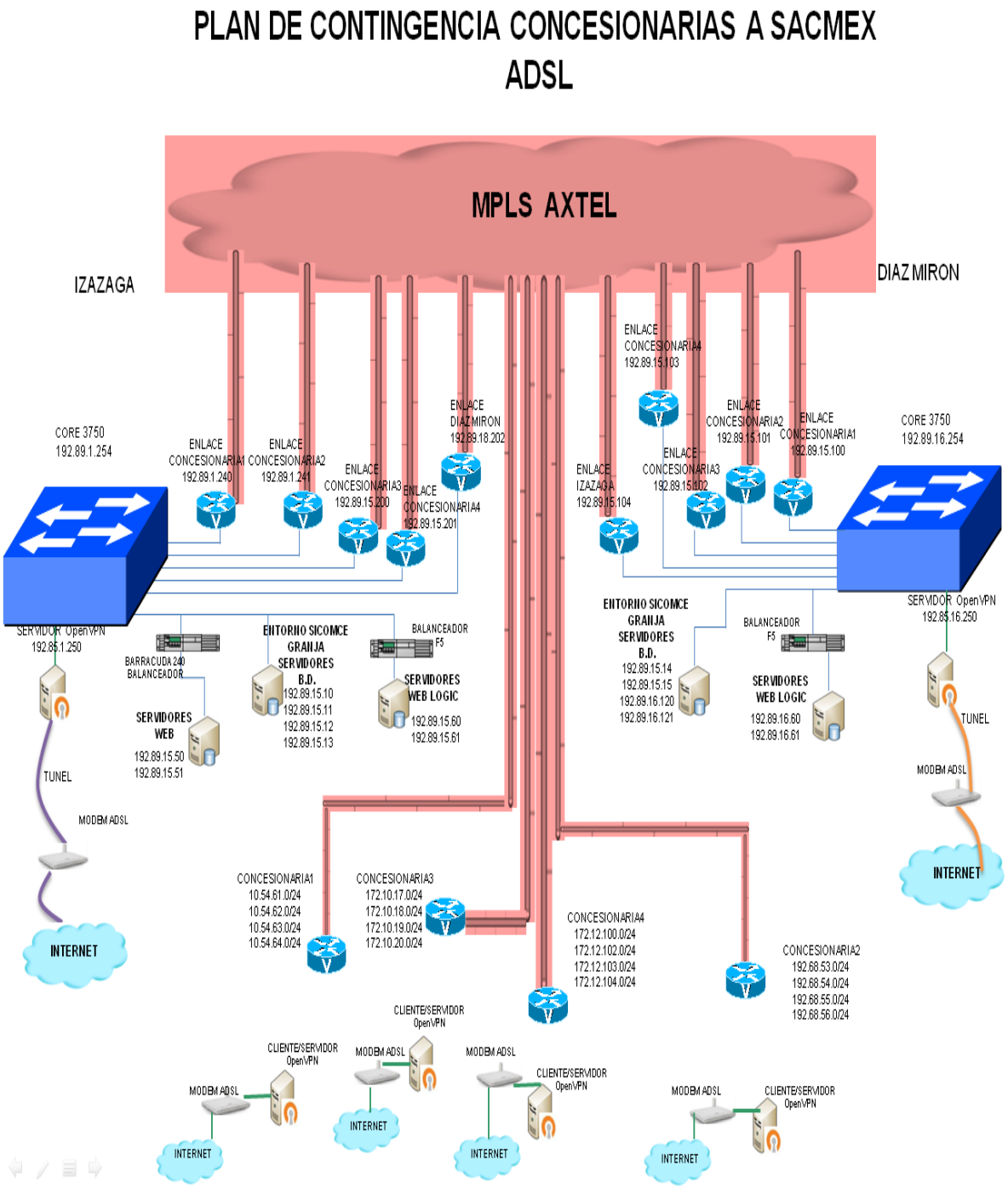


Figura 10.Plan de contingencia del entorno SICOMCE de concesionarias al SACMEX por medio de enlaces ADSL.

5. CONSTRUCCIÓN

5.1 Adecuación física de las PC

Con respecto a las características con las que deben de contar los equipos que fungirán como servidores y como clientes-servidores, se deberá verificar si cuentan con dos tarjetas de red, de no ser así se deberá añadir la tarjeta de red faltante.

Es recomendable poner un identificador a las tarjetas de red, para que no existan posibles errores de conexión, en este caso las tarjetas adicionales tomaron el valor de la intarfaz eth0 y la tarjeta de red que tiene por default la computadora tomo el valor eth1.

Figura 11.CPU con dos tarjetas de red

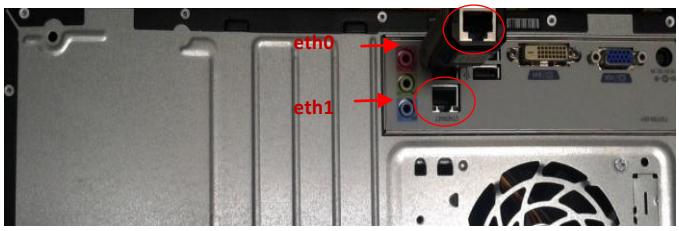


Figura 12.CPU con una tarjeta de red y adaptador USB a cable de red RJ45.

5.2 Instalación y configuración OS y software de monitoreo

A continuacion se instalara el sistema operativo a los equipos, en este caso será instalada la version Ubuntu server 14.04.01, Una vez instalado el sistema operativo en las computadoras designadas, se procederá a la configuración de las tarjetas de red, de los DNS, configuración de iptables y habilitar forwarding, cabe

mencionar que el usuario con que se trabajara para la configuración de los equipos será root, debido a los privilegios con los que cuenta.

Se sujiere que la versión del sistema operativo a instalar sea estable y que con esta misma, se desarrolle todo el proyecto debido a que si la prueba se hace en varias versiones llega a cambiar algunos paso lo que implica perdida de tiempo en la investigación de cómo configurar para otra versión. La versión que se escogio para realizar este proyecto tenia un bug en el servicio networking el cual no podía ser reiniciado o detenido, para que este tomará las configuraciones era necesario rebootear la computadora; se soluciono sustituyendo los ficheros de arranque de networking por los de la versión 13.10 para mayor referencia consultar la siguiente URL: https://github.com/metral/restore_networking

5.2.1 Habilitar root

Para trabajar con root, en un sistema Ubuntu se habilita mediante la asignación de su password con el siguiente comando:

sudo passwd root

En donde preguntará la contraseña del usuario con el que se esta trabajando para poder asignar el password a root una vez ya introducida la contraseña del usuario proceder ha asignar el password de root.

5.2.2 Configuración de tarjetas de red en el servidor para enlace dedicado

Para la configuración de las tarjetas de red se tendrá que editar el fichero de interfaces el cual se encuentra en el directorio de network, para acceder al directorio ejecutar la siguiente ruta

cd /etc/network

Se procede a editar el fichero interfaces, para ello se utiliza el editor vi.

vi interfaces

En seguida se muestra una configuración de tarjetas de red de un servidor de VPN de una de las concesionarias.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 186.212.168.245
        netmask 255.255.255.247
        network 186.212.168.240
        broadcast 186.212.168.255
        gateway 186.212.168.241


auto eth1
iface eth1 inet static
        address 192.89.1.250
        netmask 255.255.255.0
        network 192.89.1.0
        broadcast 192.89.1.255

up route add -net 192.89.1.0 netmask 255.255.255.0 gw 192.89.1.254
up route add -net 192.89.15.10 netmask 255.255.255.255 gw 192.89.1.254
up route add -net 192.89.15.11 netmask 255.255.255.255 gw 192.89.1.254
up route add -net 192.89.15.12 netmask 255.255.255.255 gw 192.89.1.254
up route add -net 192.89.15.13 netmask 255.255.255.255 gw 192.89.1.254
```

En la configuración anterior se observan las tarjetas de red, en donde la tarjeta eth0 tiene asignada una dirección pública (WAN) y la eth1 tiene asignada una dirección privada (LAN), las tarjetas de red de los equipos que fungirán como servidores OpenVPN de las otras concesionarias deberán presentar ese orden con el fin de tener un control administrativo.

Dentro de la configuración de las tarjetas, serán agregados bajo la interface eth1 direccionamientos necesarios para que el servidor pueda alcanzar los equipos deseados.

La configuración anterior se realizara en el servidor OpenVPN, que se encontrará ubicado en Izazaga, para el servidor de OpenVPN que se encontrara ubicado en Díaz Mirón las rutas que serán agregadas serán las siguientes:

up route add -net 192.89.16.0 netmask 255.255.255.0 gw 192.89.16.254
up route add -net 192.89.1.0 netmask 255.255.255.0 gw 192.89.16.254
up route add -net 192.89.15.14 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.15.15 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.16.120 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.16.121 netmask 255.255.255.255 gw 192.89.16.254

5.2.2.1 Configuración de tarjetas de red en el servidor para enlace ADSL

En seguida se muestra la configuración de tarjetas de red de un servidor de VPN utilizando un enlace ADSL, el cual proporcionara una dirección IP privada haciendo uso del protocolo DHCP y por lo tanto se tendrá una dirección IP pública dinámica.

 # This file describes the network interfaces available on your system
 # and how to activate them. For more information, see interfaces(5).

 # The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 192.89.1.250
netmask 255.255.255.0
network 192.89.1.0
broadcast 192.89.1.255

up route add -net 192.89.1.0 netmask 255.255.255.0 gw 192.89.1.254
up route add -net 192.89.15.10 netmask 255.255.255.255 gw 192.89.1.254
up route add -net 192.89.15.11 netmask 255.255.255.255 gw 192.89.1.254
up route add -net 192.89.15.12 netmask 255.255.255.255 gw 192.89.1.254

up route add -net 192.89.15.13 netmask 255.255.255.255 gw 192.89.1.254

Para el servidor de OpenVPN que se encontrará ubicado en Díaz Mirón las rutas que serán agregadas serán las siguientes:

up route add -net 192.89.16.0 netmask 255.255.255.0 gw 192.89.16.254
up route add -net 192.89.1.0 netmask 255.255.255.0 gw 192.89.16.254
up route add -net 192.89.15.14 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.15.15 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.16.120 netmask 255.255.255.255 gw 192.89.16.254
up route add -net 192.89.16.121 netmask 255.255.255.255 gw 192.89.16.254

5.2.3 Configuración de tarjetas de red en el cliente-servidor

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 10.54.61.254
        netmask 255.255.255.0
        network 10.54.61.0
        broadcast 10.54.61.255
auto eth1
iface eth1 inet dhcp
```

Como se puede observar en la configuración anterior de la tarjetas de red, la parte LAN (red de área local) se encuentra configurada en la tarjeta 0 (eth0) y la parte WAN (red de área amplia) en este caso la salida a internet, que será proporcionada por un modem ADSL estará configurada en la tarjeta 1 (eth1) por

DHCP y por lo tanto no será necesario la configuración de DNS ya que en el DHCP vienen implícitos.

Es importante respetar el orden y asignación de las tarjetas, debido a que las máquinas que funjan como cliente servidor deben de estar configuradas de manera uniforme, para que se lleve un mejor control de administración.

Para que las configuraciones, tomen efecto se debe reiniciar el servicio de network, esto se realiza tecleando el siguiente comando.

service networking restart

5.2.4 Configuración de DNS enlace dedicado

Se configura los DNS (Sistema de Nombres de Dominio) que la maquina utilizara para resolver los nombres de dominio, ya que con esta configuración se podrá descargar el software que será utilizado y actualizar el sistema operativo.

Se editara el fichero base ejecutando el siguiente comando.

vi /etc/resolvconf/resolv.conf.d/base

Una vez dentro del fichero base añadir las siguientes líneas.

nameserver 200.33.146.193
nameserver 200.33.146.201

Para actualizar, ejecutar el siguiente comando.

resolvconf -u

5.2.5 Habilitar forward

Se habilitara forward para el reenvió de paquetes. Esto se configurará en el servidor y en el cliente-servidor.
Para habilitar forward se tendrá que editar el archivo sysctl.conf el cual se encuentra en el directorio /etc, para acceder a este entramos al directorio con el siguiente comando.

cd /etc

Para editar el fichero

vi sysctl.conf

En este archivo solo se borra el signo # de la línea de forward.
En el archivo siguiente se muestra con negritas la habilitación del forward.

```
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
##############################################################3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

```
# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#
```

5.2.6 Configuración de IPTABLES

Esta configuración solo se realiza en los servidores.
Ahora se editara el documento rc.local localizado en el directorio /etc en este archivo se añadirá una regla iptables, la cual se encargará de encaminar el trafico proveniente del direccionamiento proveniente de la VPN y en mascarlo como si fuera enviado por la tarjeta eth1 (LAN), para que los usuarios de la VPN puedan acceder a los segmentos de red 192.89.X.X que son parte del Sistema de Aguas

de la Ciudad de México.
Uno de los direccionamientos de la VPN a configurar en las empresas concesionarias es (192.168.69.0/24).

El iptables es configurado estratégicamente en este archivo para que al momento de encender el equipo, estos se inicien en automático con el sistema.

Para acceder a rc.local, hay que entrar en el directorio /etc

cd /etc

Se procede a editar el archivo.

vi rc.local

En el siguiente archivo se muestran en letras negritas las iptables que se agregaron.

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
```

iptables -t nat -A POSTROUTING -s 192.168.69.0/24 -o eth1 -j MASQUERADE

exit 0

En caso de ocupar el enlace ADSL será necesario agregar otra iptables ejecutándose esta directamente en el shell para que encamine el trafico proveniente del direccionamiento 192.168.69.0/24 proveniente de la VPN hacia la tarjeta eth0, dicha tarjeta brindara salida a internet para poder encontrar los dominios que hayan sido configurados en los servidores de VPN.

/sbin/iptables -t nat -A POSTROUTING -s 192.168.69.0/24 -o eth0 -j MASQUERADE

5.2.7 Actualización del Sistema Operativo

Actualización del OS (Sistema Operativo) para que se lleve a cabo esta tarea ejecutar.

aptitude update && aptitude upgrade

Posteriormente se procede a la instalación de software de monitoreo el cual será empleado para el control, administración y soporte.

5.2.8 Instalación Traceroute

Traceroute se instalará con el fin de saber que camino está tomando el tráfico y en caso de que no llegue a su destino la información saber en qué punto se está quedando.

La instalación de traceroute se realiza mediante el siguiente comando.

apt-get install traceroute

5.2.9 Instalación y configuración SSH

SSH se instalará para tener el acceso remoto a los equipos en caso de que algo llegase a fallar, poder dar solución al problema.

La instalación de SSH (SERCURE SHELL) se realiza mediante el siguiente comando.

apt-get install openssh-client openssh-server

Se configurará SSH para dar mayor seguridad a los equipos y no sean atacados por este medio, para ello se deshabilitara el login con root habilitando el login con un usuario especifico común, se reducirá el tiempo de login y solo permitirá abrir una sesión para la configuración, se editara el fichero sshd_config, a continuación se muestra que líneas deberán de ser modificadas y que líneas deberán de ser agregadas.

Los cambios y modificaciones que serán configurados en el fichero sshd_config aparecerán en negritas en el ejemplo siguiente.

Edición del archivo sshd_config

vi /etc/ssh/sshd_config

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

Logging
SyslogFacility AUTH
LogLevel INFO

Authentication:
LoginGraceTime 20
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
similar for protocol version 2
HostbasedAuthentication no
Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
ChallengeResponseAuthentication no

Change to no to disable tunnelled clear text passwords

```
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

Allowusers 1nf0rm4t1c4
MaxAuthTries 1
```

MaxStartups 1

Se creará un usuario, el cual será utilizado para logearse por SSH.

Crear usuario

adduser 1nf0rm4t1c4

5.3 Instalación y configuración de OpenVPN en el servidor

OpenVPN es el protocolo, por el cual se configura la VPN, en este caso se configurará en los servidores, para que se establezca comunicación entre el SACMEX y las OAP de las concesionarias.

Para instalar el software de OpenVPN hay que ejecutar el siguiente comando.

apt-get -y install openvpn easy-rsa

5.3.1 Configuración del servidor OpenVPN para enlace dedicado

A continuación se creará el fichero de configuración del servidor. Para ello dirigirse al directorio openvpn en donde se configurara el archivo llamado server.conf, esto se realiza ejecutando:

vi /etc/openvpn/server.conf

El fichero server.conf deberá contener las siguientes lineas:

local 186.212.168.245
management 127.0.0.1 1195
dev tun
proto tcp
port 1194
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/SERVER_VPN_CONCESIONARIA1.crt

```
key /etc/openvpn/keys/ SERVER_VPN_CONCESIONARIA1.key
dh /etc/openvpn/keys/dh2048.pem
tls-auth /etc/openvpn/keys/ta.key 0
user nobody
group nogroup
server 192.168.69.0 255.255.255.0
route 10.54.61.0 255.255.255.0 192.168.69.8
ifconfig-pool-persist /etc/openvpn/clients.txt
client-to-client
client-config-dir ccd
topology subnet
status /etc/openvpn/status.txt
persist-key
persist-tun
push "redirect-gateway def1"
keepalive 10 120
verb 4
comp-lzo
max-clients 85
```

Descripción de las opciones del fichero de configuración server.conf:

local: Dirección IP asignada al servicio de OpenVPN.

managment: consola de administración de OpenVPN.

dev: Tipo de interfaz tun/tap de conexión virtual que se utilizará el servidor OpenVPN.

proto: tipo de protocolo TCP/UDP que se empleará en la conexión a través de VPN.

port: Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor por default tiene 1194.

Parámetros SSL/TLS

- ca: Especifica la ubicación de [ca.crt] de Autoridad Certificadora .
- cert: Especifica la ubicación [.crt] creado para el servidor OpenVPN.
- key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

Parámetros Diffie Hellman generados con openssl
dh: Ruta de [.pem] .

ta: Ruta de la llave secreta, seguridad extra de SSL/TLS creada en HMAC firewall, bloquea ataques DoS. Para el servidor se pone parámetro 0 y para el cliente parámetro 1.

Parámetros utilizados para los sistemas que no son Windows

- user nobody
- group nogroup

server: Se asigna el direccionamiento IP virtual que se utilizará en la red del túnel VPN.

route: Se anuncia el direccionamiento que tiene el cliente en su LAN .

Ifconfig-pool-persist: Archivo en donde quedarán registrado las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.

client-to-client: Permite la comunicación entre clientes

client-config-dir ccd :configuración de direccion ip del cliente y ruteo

topology subnet: Esta opción permite que el direccionamiento con mascara de 24 bits trabaje de forma adecuada .

status: archivo donde se almacenará los eventos y datos sobre la conexión del servidor [.log]

La opción persistente permitirá reconectar a los clientes después de un reinicio sin necesidad de volver a reiniciar sesión

- persist-key

- persist-tun

push "redirect-gateway def1": Permite redireccionar el tráfico proveniente del tunel.

Keepalive 10 120: Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.

verb: Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si se desea un buen resumen de qué está sucediendo.

comp-lzo: Específica que los datos que recorren el túnel VPN serán compactados durante la trasferencia.

max-clients : Establece el numero de clientes conectados simultaneamente.

Para que a los clientes (OAP) de la VPN se les asigne una dirección IP fija se tiene que crear un directorio en OpenVPN, este directorio se llamara **ccd**, en donde se crearán los ficheros de los clientes, que contendrán una dirección IP de la VPN que se les va asignar de manera fija y el ruteo que debe contener.
Crear directorio ccd, como se menciono anteriormente, esta se localizara dentro del directorio openvpn.

cd /etc/openvpn

Una vez estando en el prompt, crear el directorio ccd.

mkdir ccd

Una vez creado el directorio ccd, se procederá a elaborar el fichero del cliente el cual estará dentro del directorio ccd, el fichero contendrá la dirección IP fija de la VPN que le será asignada al cliente y el ruteo que deberá de conocer.
En este caso se trabajara con la OAP “oap1”.

touch oap1

Posteriormente se edita el fichero oap1 el cual contendrá:

vi oap1

```
ifconfig-push 192.168.69.8 255.255.255.0
push "route 192.89.1.0 255.255.255.0 192.168.69.1"
push "route 192.89.15.10 255.255.255.255 192.168.69.1"
push "route 192.89.15.11 255.255.255.255 192.168.69.1"
push "route 192.89.15.12 255.255.255.255 192.168.69.1"
push "route 192.89.15.13 255.255.255.255 192.168.69.1"
iroute 10.54.61.0 255.255.255.0
```

5.3.1.1 Configuración del servidor OpenVPN para enlace ADSL

El fichero server.conf deberá contener las siguientes lineas:

```
management 127.0.0.1 1195
dev tun
proto tcp
port 1194
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/SERVER_VPN_CONCESIONARIA1.crt
key /etc/openvpn/keys/ SERVER_VPN_CONCESIONARIA1.key
dh /etc/openvpn/keys/dh2048.pem
tls-auth /etc/openvpn/keys/ta.key 0
user nobody
group nogroup
server 192.168.69.0 255.255.255.0
route 10.54.61.0 255.255.255.0 192.168.69.8
ifconfig-pool-persist /etc/openvpn/clients.txt
client-to-client
client-config-dir ccd
topology subnet
status /etc/openvpn/status.txt
persist-key
persist-tun
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
verb 4
comp-lzo
```

max-clients 85

Como se puede observar la configuración anterior es parecida a la configuración del enlace dedicado, las líneas que se agregan, son los DNS de google, que seran proporcionados a los clientes (OAP) para que encuentren el dominio que se designo al servidor OpenVPN.

push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"

La linea que se elimino fue la opción “local”.

5.3.2 Habilitar modo TUN

Se procederá a, activar el modulo TUN, ejecutando los comandos:

modprobe tun

echo "tun" >> /etc/modules

5.3.3 Creación de certificados

A continuación se configurará el cifrado, la entidad emisora de los certificados, el certificado y llave del servidor y los certificados y llaves para los clientes.
Para ello copiar el directorio easy-rsa este se encuentra en el siguiente path:
“/usr/share/easy-rsa/” y serán copiadós en el directorio de openvpn. Ejecutar

cp –R /usr/share/easy-rsa /etc/openvpn

Ya que se copio el directorio easy-rsa en el directorio de OpenVPN, se accede a este y dentro del subdirectorio easy-rsa se creara un directorio llamado keys

cd /etc/openvpn/easy-rsa

mkdir keys

Posteriormente se editará el fichero vars, que se encuentra bajo el subdirectorio

easy-rsa, en este fichero se configurara el parámetro de cifrado DH, se especificara el lugar donde se encontraran los certificados al ser creados y se establecerá la entidad emisora de los certificados.

Se procede a editar el archivo vars ejecutando el comando:

vi /etc/openvpn/easy-rsa/vars

Dentro del archivo se sustituirán las siguientes líneas:

export KEY_DIR="$EASY_RSA/keys"

Por

export KEY_DIR="/etc/openvpn/easy-rsa/keys"

Las líneas de la entidad emisora.

export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"

Por

export KEY_COUNTRY="MX"
export KEY_PROVINCE="DF"
export KEY_CITY="IZAZAGA"
export KEY_ORG="SACMEX"
export KEY_EMAIL=miguel.alarcon@sacmex.df.gob.mx
export KEY_ou= “INFORMATICA”

En seguida se procede a crear los certificados de autenticación del servidor de OpenVPN y sus clientes. Lo anterior se realizara dentro del directorio easy-rsa que se encuentra en el path /etc/openvpn/easy-rsa

Ejecutar los siguientes comandos

source ./vars

Después de ejecutar el comando anterior, aparecerá un texto el cual indicará que si se ejecuta el comando "./clean-all" se borraran las llaves y certificados antes creadas, como se acaba de instalar el software no se cuenta con ningún certificado ni llave.

En seguida se generara el cifrado Diffie Hellman de 2048bits
./build-dh

A continuación se designará la entidad emisora de certificados.

./build-ca

Ahora se procederá a generar los certificados y las llaves.
Primero se creará el certificado y llave del servidor.
Al momento de crear el certificado y llave del servidor, se pondrá el nombre especificado en el fichero server.conf, en este caso, el nombre del servidor será: "SERVER_VPN_CONCESIONARIA1". Ejecutar el comando para crear el certificado y la llave del servidor.

./build-key-server SERVER_VPN_CONCESIONARIA1

Después de ejecutar el comando anterior, pedirá información para crear el certificado, en donde se pondrá:

Country Name: **MX**
State Or Providence Name: **DF**
Locality Name: **NZ**
Organizatinal Name: **SACMEX**
Organizational Unit Name: **INFORMATICA**
CommonName: **VPN_SACMEX**
Name: **VPN_SACMEX**
EmailAddress: **miguel.alarcon@sacmex.df.gob.mx**

Ya que se haya introducido la información requerida preguntará si se desea

agregar un password y un nombre a la compañía en estos puntos debemos teclear “enter” para continuar, en seguida preguntara si se firma el certificado, a lo que se responde con una “**Y**”, de lo contrario no creara el certificado ni la llave.

Los certificados y las llaves para los clientes, se crearán individuales ya que a cada certificado de los clientes se le asignara un nombre, para ello se recomienda nombrarlo de forma que el nombre nos indique la identidad de la institución.

Para este caso, se creará un certificado “oapx”.
Ejecutar el siguiente comando para crear certificado del cliente:

./build-key–pass oapx

Después de ejecutar el comando anterior, pedirá que se le asigne un password y enseguida pedirá información para crear el certificado, en donde se pondrá dependiendo la ubicación del cliente. Por ejemplo:

Country Name: **MX**
State Or Providence Name: **DF**
Locality Name: **MT**
Organizatinal Name: **CONCESIONARIA1**
Organizational Unit Name: **INFORMATICA**
CommonName: **OAPX**
Name: **OAPX**
EmailAddress: **miguel.alarcon@sacmex.df.gob.mx**

Para seguir creando más clientes solo se ejecutara el comando antes mencionado, recordando cambiar el nombre del cliente en este caso se llamara “oapy” lo cual se ejecuta de la siguiente manera

./build-key-pass oapy

Ya que hayan sido creados los certificados, se copia el directorio de keys en el path “/etc/openvpn” ya que en el archivo server.conf se indico esta ruta en donde se encontrarán los certificados.
Esto se efectuará con siguiente comando:

cp -r /etc/openvpn/easy-rsa/keys /etc/openvpn/

Una vez copiado el directorio keys, se procede a verificar si se encuentran los certificados, para ello ejecutar

cd /etc/openvpn/keys

ls

Se procede a generar un certificado de seguridad llamado ta.key dentro del directorio keys, que se encontrará en el path /etc/openvpn/keys ejecutando.

openvpn --genkey --secret ta.key

5.3.4 Iniciar servicio OpenVPN

Para iniciar el servicio, de la VPN ejecutar

/etc/init.d/openvpn start

Para comprobar que se hayan levantado correctamente el servicio de OpenVPN mandar ping al servidor de OpenVPN, que por default le es asignada la dirección IP 192.168.69.1 o ver las interfaces ejecutando “ifconfig”.

5.3.4.1 Automatización para levantar servicios de OpenVPN “enlace dedicado o ADSL”

Con la finalidad de agilizar el proceso del enlace por el cual se desea restablecer la comunicación ya sea por enlace dedicado o por enlace ADSL se decidió que en los servidores se crearan ficheros los cuales contuvieran las configuraciones pertinentes a los dos tipos de enlace, para que en una contingencia se escogiera una u otra.

Para la automatización de que configuración elegir se realizó un script.

```
opcion=x
echo $opcion
while [ $opcion != z ]
do
```

```
clear
echo "\n\n"
echo "\033[1m SERVIDOR DE OpenVPN \033[0m"
echo "\n"
echo "\033[31m OPCIONES CON LAS QUE PODRAS ELEGIR QUE CONFIGURACION ESTABLECER"
echo " PARA CONECTAR LA OAP CON LOS SITE'S DE DIAZ MIRON E IZAZAGA \033[0m"
echo "\n"
echo "\033[1m\033[35m a) \033[0m Enlace OpenVPN a traves de IP FIJA"
echo "\033[1m\033[35m b) \033[0m Enlace OpenVPN a traves de DynDNS DHCP (TELMEX)"
echo "\033[1m\033[35m z) \033[0m Salir"
echo "\n\n"
echo "\033[1m Elige la OPCION correspondiente \033[0m"
read opcion
case "$opcion" in
a) clear
    echo "\n"
    echo "\033[1m\033[34m Elegiste la OPCION de Enlace OpenVPN a traves de IP FIJA \033[0m"
    echo "\n"
    echo "\033[0m\033[32m Copiando archivo /etc/network/interfaces_uno a /etc/network/interfaces \033[0m"
    cp /etc/network/interfaces_uno  /etc/network/interfaces
    echo "\n\n"
    sleep 3
    echo "\033[0m\033[32m REINICIANDO SERVICIO INTERFACES \033[0m"
    service networking stop
    sleep 2
    service networking start
    echo "\n\n"
    sleep 2
    echo "\033[1m Copiando archivo /etc/openvpn/server_uno a /etc/openvpn/server.conf  \033[0m"
    cp /etc/openvpn/server_uno  /etc/openvpn/server.conf
    echo "\n\n"
    echo "\033[0m\033[32m REINICIANDO SERVICIO OPENVPN \033[0m"
    echo "\n\n"
    /etc/init.d/openvpn restart
    echo "n\n"
    sleep 5;;
```

```
b) clear
     echo "\n"
     echo "\033[1m\033[34m Elegiste la OPCION de Enlace OpenVPN a traves de
DynDNS DHCP (TELMEX)\033[0m"
     echo "\n"
     echo "\033[0m\033[32m Copiando archivo /etc/network/interfaces_dos a
/etc/network/interfaces \033[0m"
     cp /etc/network/interfaces_dos  /etc/network/interfaces
     echo "\n\n"
     echo "\033[0m\033[32m REINICIANDO SERVICIO INTERFACES \033[0m"
     service networking stop
     sleep 2
     service networking start
     echo "\n\n"
     sleep 2
     echo "\033[1m Copiando archivo /etc/openvpn/server_dos a
/etc/openvpn/server.conf  \033[0m"
     cp /etc/openvpn/server_dos  /etc/openvpn/server.conf
     echo "\n\n"
     /etc/init.d/openvpn restart
     echo "n\n"
     sleep 2
     echo "\033[1m LEVANTANDO ENRUTAMIENTO HACIA LA NUVE  \033[0m"
     /sbin/iptables -t nat -A POSTROUTING -s 192.168.69.0/24 -o eth0 -j
MASQUERADE
     echo "\n\n"
     sleep 5;;
     sleep 5;;
z) clear
    echo "\n"
    echo "SALIR"
    exit;;
*) clear
    echo "opcion invalida"
    sleep 5;;
esac
done
```

5.4 Configuración de dominio enlace ADSL

A continuación se establecerán los dominios que tendrán los servidores de OpenVPN, es necesario contar con una cuenta con un servidor de dominios dinámicos para este caso se utiliza el servidor DynDNS en donde se creará el dominio y este se encargará de publicarlo.
En las siguientes figuras se podrá apreciar cómo dar de alta un dominio en el servidor DynDNS.

Figura 13. Inicio de sesión en la página del servidor DyDNS.

Dirigirse a al apartado mis servicios y entrar en la opción DynDNS Pro.

Figura 14. Opción DyDNS Pro para configurar dominio.

Seleccionar la opción añadir nombre del servidor.

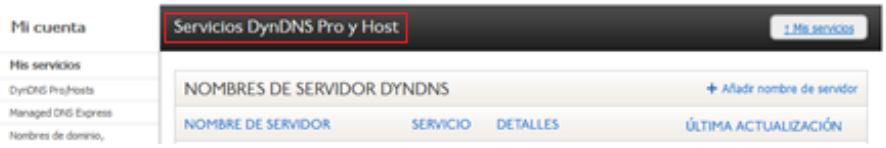


Figura 15. Añadir nombre de servidor.

Se crea el dominio para el servidor OpenVPN y se elige en una lista el subdominio, para este caso se utulizo homelinux.com, posterirmente pide que se proporcione una dirección IP publica, si se esta conectado al modem en el que se habilitará el servicio de DynDNS existe una opción la cual detecta la ip pública de este, si no, se podrá proporcionar la dirección IP.

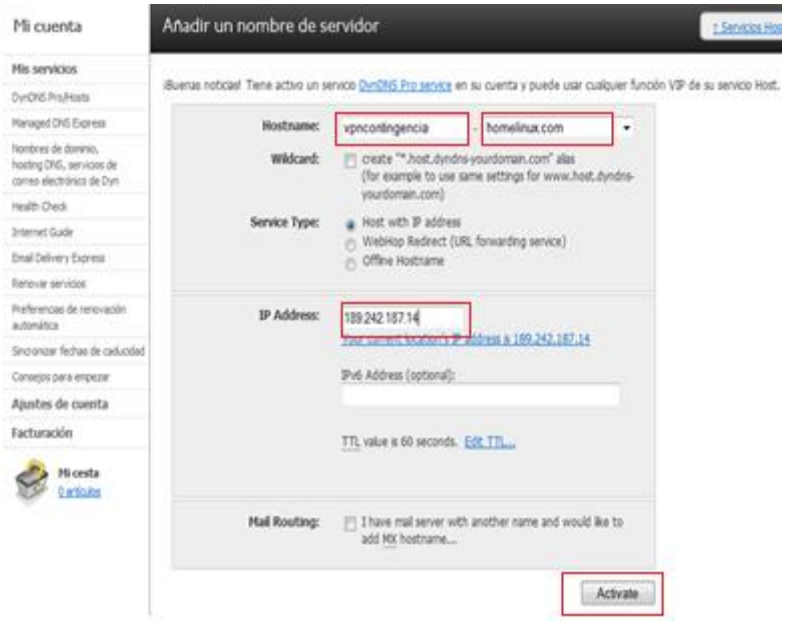


Figura 16. Establecimiento del dominio y vinculación a dirección IP.

En la siguiente ilustración se pude ver que el dominio ya ha sido vinculado con la dirección IP.

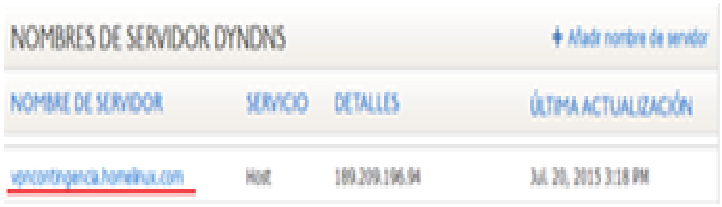


Figura 17. Dominio publicado.

Después de haber creado el dominio se configura el modem (en este caso fue utilizado un Technicolor modelo TG582n), habilitándo el DNS dinámico en donde se proporciona el cliente, el usuario, el host. Para ello dirigirse a la pestaña herramientas elegir la opción DNS dinámico.

El servidor de OpenVPN deberá estar conectado al modem.

En las siguientes ilustraciones se mostrará como se habilita el DNS dinámico, dirijirse a la opción herramientas donde se despliega un menú, escoger la opción DNS dinámico y en el lado superior derecho entrar en configuración.

Figura 18. Servicio DNS dinámico.

Posteriormente se selecciona la opción habilitado, se proporciona el usuario de la cuenta de DynDNS y su contraseña, se proporciona el nombre del servidor que se encargará de publicar el dominio en este caso DynDNS y por ultimo el hostname o dirección ip del equipo que contendrá el dominio.

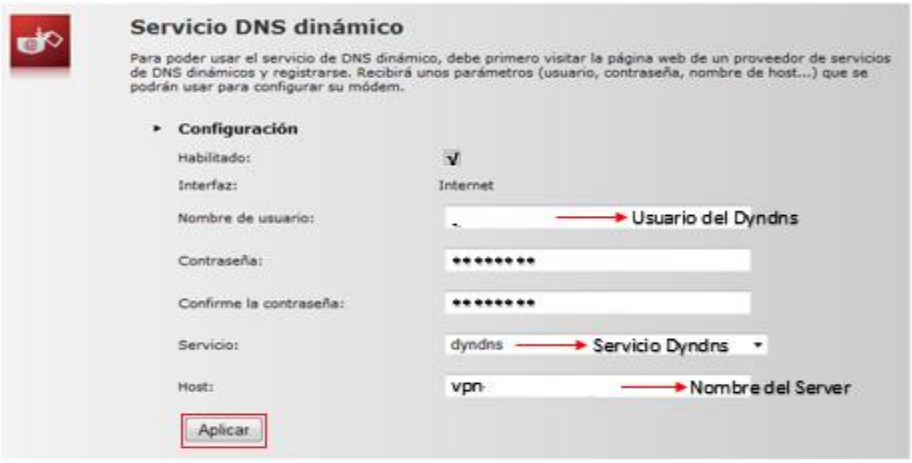


Figura 19. Configuración de servicio DNS dinámico.

A continuación se define la aplicación o servicio que será utilizado, dirijirse a la opcion crear un nuevo juego o aplicación.

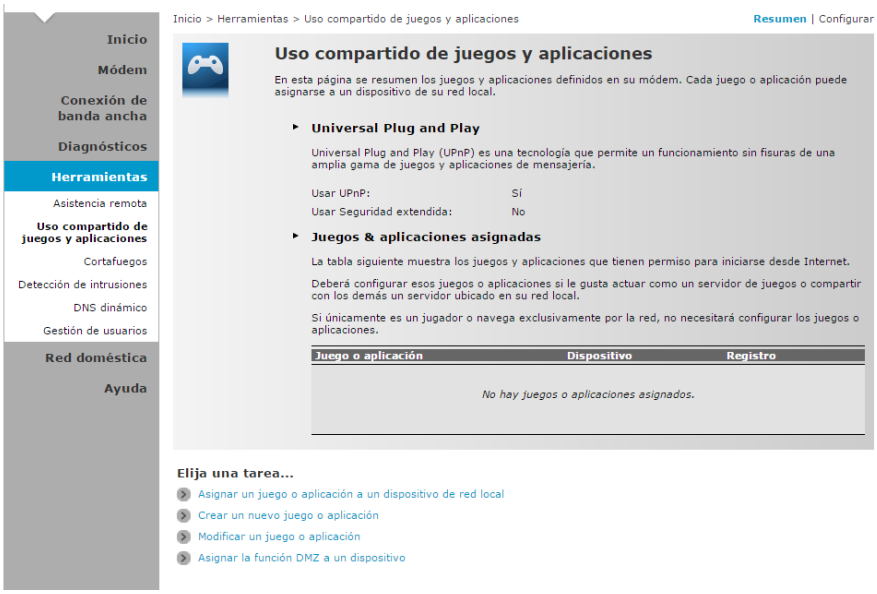


Figura 20. Crear un nuevo juego aplicación.

Introducir el nombre de la aplicación y seleccionar entrada manual de mapa de puertos.

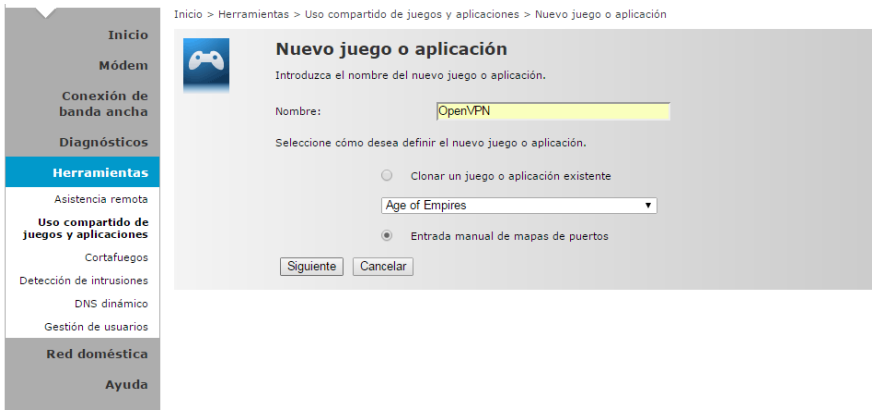


Figura 21. Asignar nombre al servicio.

Se proporciona el protocolo de trasporte y el puerto de comunicación que utilizara en este caso OpenVPN esta configurado para trabajar con el protocolo TCP y por default trabaja con el puerto 1194.

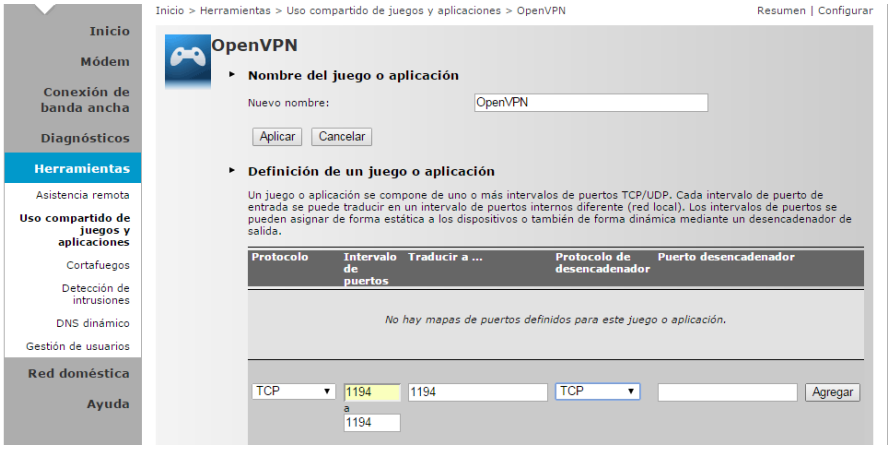


Figura 22. Definicion del servicio OpenVPN.

Figura 23. Servicio definido OpenVPN.

Dirijirse a uso compartido de juegos y aplicaciones y en el lado superior de entrar en configurar en el apartado de juegos y aplicaciones asignadas abra una pestaña al desplegarla apareseran varias aplicaciones y servicios, escoger OpenVPN y en la otra pestaña muestra el hostname, o dirección mac de las máquinas conectadas al módem ahí se selecciona la máquina a la que le será asignado el servicio de OpenVPN.

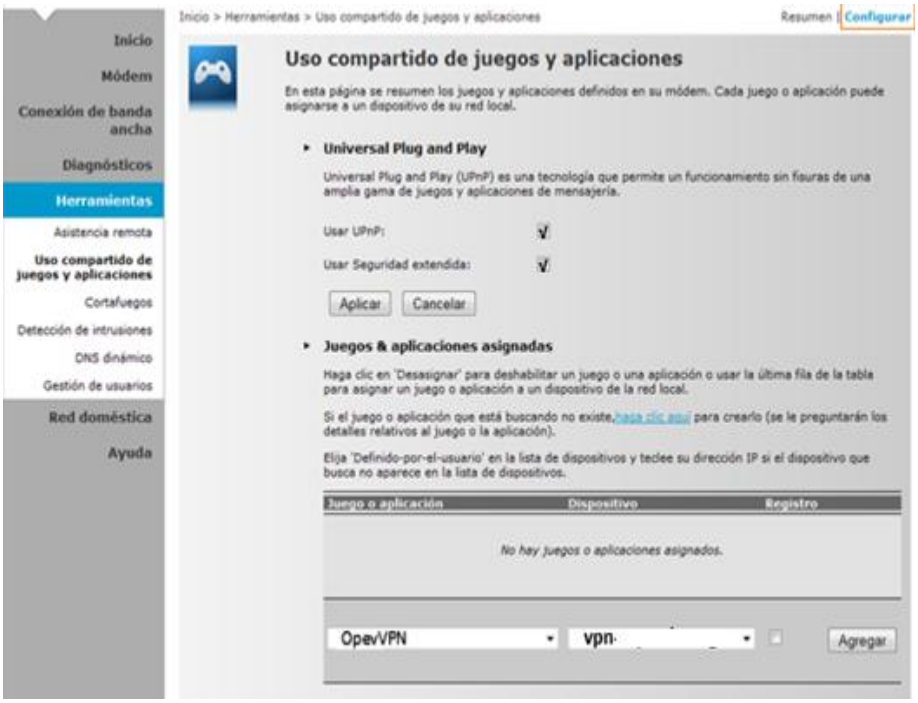


Figura 24. Asignacion de servicio OpenVPN al host.

También se realizaron pruebas en un rouer de Axtel Zhone modelo znid-gpon-2426 en donde la configuración del DNS dinamico es similar al del modem Technicolor de Telmex.

Para habilitar DNS dinámico dirigirse a sistemas, seleccionar DNS Dynamic y la opción agregar. Pedira que sea proporcionado el nombre del servidor DNS dinamico (DynDNS), el hostname y la interface del router donde fue conectado, por ultimo pedirá el ususario y crontraseña de la cuenta de DynDNS.

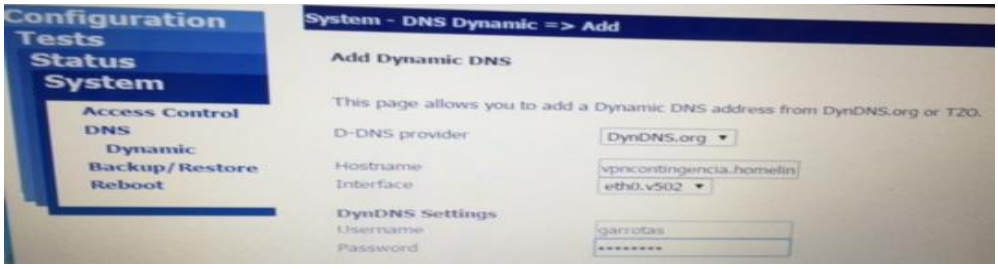


Figura 25. Configuración de servicio DNS dinámico.

En la figura 26 se muestra que el DNS dinámico ya ha sido habilitado.

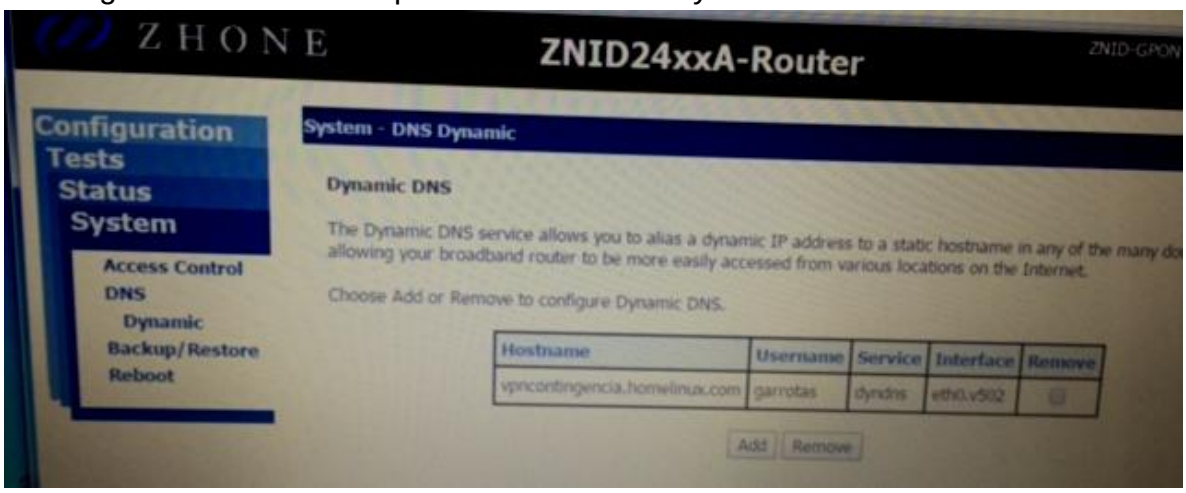


Figura 26. DNS dinámico habilitado.

A continuación se define el servicio OpenVPN, puertos y protocolos por los que este trabajara y su dirección IP privada. Esto se realizará en configuración en la opción firewall port forwarding.

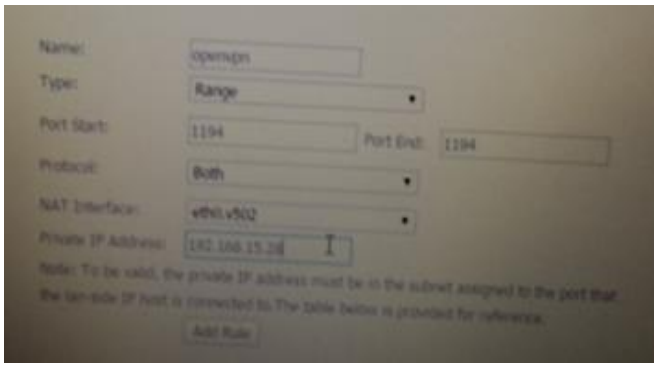


Figura 27. Definición del servicio OpenVPN.

En la siguiente ilustración se muestra que el servicio ya ha sido definido.

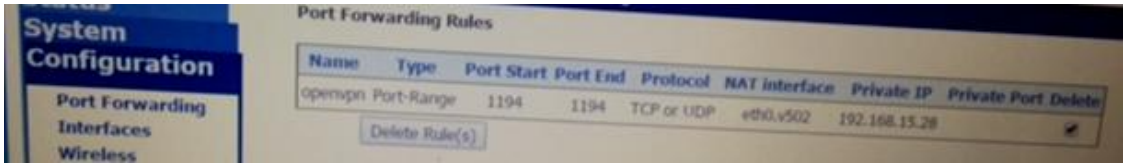


Figura 28. Servicio OpenVPN Definido.

En el caso del módem Zhone proporcionado por Axtel no fue necesario la instalación de ddclient, debido a que este tipo de módem cuenta ya con un cliente pre instalado que se encargara de avisar al servidor cada que exista un cambio en su dirección IP. Para el modem Technicolor de Telmex si fue necesario instalar ddclient.

Posteriormente se procede a instalar el ddclient en el servidor de OpenVPN, esté se encargará de avisar al servidor de DynDNS cuando el módem haga cambio de dirección IP por lo tanto el servidor DynDNS se encontrará actualizado y se podrá acceder al servicio de OpenVPN por medio del dominio.

Instalación de ddclient

aptitude install ddclient

Configuración de ddclien en el siguiente fichero

/etc/ddclient.conf

protocol=dyndns2
use=web, web=checkip.dyndns.com
server=members.dyndns.org
login=AGUA
password='1nf0rm'
vpncontingencia.homelinux.com

Ejecutar la siguiente línea para informar al servidor DynDNS la dirección IP actual del modem.

/usr/sbin/ddclient -file /etc/ddclient.conf -cache /home/usuario/.ddclient.cache

Para automatizar este proceso y no se tenga que correr de nuevo esta línea se hace un cron (programa que permite a usuarios Linux/Unix ejecutar automáticamente comandos o script a una hora o fecha específica).

crontab -e

0 */2 * * * /usr/sbin/ddclient –file /etc/ddclient.conf -cache /home/usuario/.ddclient.cache – quite

Este avisará cada dos horas al servidor DynDNS si el módem ha cambiado su IP.

Algunos módems ya traen por default un cliente instalado que se encarga de avisar al servidor DynDNS si su dirección IP ha cambiado, y para estos casos no será necesario instalar ddclien a los servidores.

5.5 Instalación y configuración de OpenVPN en el cliente-servidor

OpenVPN es el protocolo, por el cual se configura la VPN, en este caso se configurarán los cliente-servidor, para establecer comunicación en cuanto se

levante el túnel, una vez que los clientes-servidores se hayan firmado en el servidor de VPN.

apt-get install openvpn easy-rsa

Ya que se ha instalado OpenVPN, se procederá a crear uno o dos subdirectorios según sea el caso, bajo el directorio de openvpn.

5.5.1 Creación de subdirectorios de OpenVPN
En esto subdirectorios se guardarán los certificados y el archivo de configuración cliente de OpenVPN, para mejor administración, a los directorios se les nombrará dependiendo el servidor de OpenVPN al que establezca la conexión.

mkdir izazaga

mkdir diazmiron

5.5.2 Configuración OpenVPN para enlace dedicado
Dirigirse al directorio izazaga o diazmiron según sea el caso

cd /etc/openvpn/izazaga

o

cd /etc/openvpn/diazmiron

Dentro del directorio de OPENVPN se creará un archivo llamado izazaga.conf o diazmiron.conf según sea el caso, para ello insertamos el siguiente comando:

vi izazaga.conf

o

vi diazmiron.conf

A continuación se muestra cómo debe quedar la configuración, para este caso se muestra el fichero izazaga.conf:

client
dev tun
topology subnet
proto tcp
remote 186.212.168.245 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/izazaga/oap1.crt
key /etc/openvpn/ izazaga/oap1.key
tls-auth /etc/openvpn/ izazaga/ta.key 1
comp-lzo
verb 3

Descripcion de opciones para cliente:

client: Especifica que el fichero.conf es configurado para un cliente de OpenVpn
remote: Indica la dirección IP que tiene el servidor de OpenVPN.
float: Acepta paquetes autenticados de cualquier dirección.
resolv-retry infinite: Intenta resolver indefinidamente la conexion al servidor OpenVPN en caso de llegará a interumpirse.
nobind: No agrega bind a la dirección local y al puerto.

Las opciones que faltaron por describirce podrán consultarce en configuración del servidor OpenVPN para enlace dedicado.

5.5.2.1 Configuración OpenVPN para enlace ADSL
Para este caso solo cambia la opción remote en la que se sustituye la dirección IP por el dominio del servidor de OpenVPN.

fichero izazaga.conf:

client
dev tun

topology subnet
proto tcp
remote vpncontinge.cia.homelinux.com 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/izazaga/oap1.crt
key /etc/openvpn/ izazaga/oap1.key
tls-auth /etc/openvpn/ izazaga/ta.key 1
comp-lzo
verb 3

5.5.2.2 Automatización ficheros de configuración para enlace dedicado y ADSL
Para agilizar por cuál de los dos enlaces se deberá restablecer la comunicación se crearon ficheros para ambos casos los cuales contienen sus respectivas configuraciones, para esto se creó un script el cual pregunta que enlace se utilizará y en automático el pondrá en ejecución el fichero de configuración necesario.

```
opcion=x
echo $opcion
while [ $opcion != z ]
do
clear
echo "\n\n"
echo "\033[1m CLIENTE DE OpenVPN \033[0m"
echo "\n"
echo "\033[31m OPCIONES CON LAS QUE PODRAS ELEGIR QUE
CONFIGURACION ESTABLECER"
echo " PARA CONECTAR LA OAP CON LOS SITE'S DE DIAZ MIRON E
IZAZAGA \033[0m"
echo "\n"
echo "\033[1m\033[35m a) \033[0m Enlace OpenVPN a traves de IP FIJA"
```

```
echo "\033[1m\033[35m b) \033[0m Enlace OpenVPN a traves de DynDNS "
echo "\033[1m\033[35m z) \033[0m Salir"
echo "\n\n"
echo "\033[1m Elige la OPCION correspondiente \033[0m"
read opcion
case "$opcion" in
a) clear
     echo "\n"
     echo "\033[1m\033[34m Elegiste la OPCION de Enlace OpenVPN a traves de
IP FIJA \033[0m"
     echo "\n"
     echo "\033[0m\033[32m Copiando archivo /etc/openvpn/izazaga_uno a
/etc/openvpn/izazaga.conf \033[0m"
     cp /etc/openvpn/izazaga/izazaga_uno  /etc/openvpn/izazaga/izazaga.conf
     echo "\n\n"
     echo "\033[0m\033[32m Copiando archivo /etc/openvpn/diazmiron_uno a
/etc/openvpn/diazmiron.conf \033[0m"
     cp /etc/openvpn/diazmiron/diazmiron_uno
/etc/openvpn/diazmiron/diazmiron.conf
     echo "\n\n"
     sleep 5;;
b) clear
     echo "\n"
     echo "\033[1m\033[34m Elegiste la OPCION de Enlace OpenVPN a traves de
DynDNS \033[0m"
     echo "\n"
     echo "\033[0m\033[32m Copiando archivo /etc/openvpn/izazaga_dos a
/etc/openvpn/izazaga.conf \033[0m"
     cp /etc/openvpn/izazaga/izazaga_dos  /etc/openvpn/izazaga/izazaga.conf
     echo "\n\n"
     echo "\033[0m\033[32m Copiando archivo /etc/openvpn/diazmiron_dos a
/etc/openvpn/diazmiron.conf \033[0m"
     cp /etc/openvpn/diazmiron/diazmiron_dos
/etc/openvpn/diazmiron/diazmiron.conf
     echo "\n\n"
     sleep 5;;
```

```
z) clear
   echo "\n"
   echo "SALIR"
   exit;;
*) clear
   echo "opcion invalida"
   sleep 5;;
esac
done
```

5.5.3 Copia de certificados

Copiar los certificados de los clientes, previamente hechos por el administrador del servidor openvpn, en este caso el administrador proporcionará los certificados en un dispositivo opendrive (memoria USB) para poder ser copiados en los clientes-servidores.

En los subdirectorios izazaga y diazmiron se copiarán los certificados correspondientes ya sea el servidor OpenVPN Izazaga o el servidor OpenVPN Diaz Miron.

En seguida se muestra en la figura 29 y figura 30 un ejemplo del contenido que deberá de tener cada subdirectorio (izazaga y diazmiron).

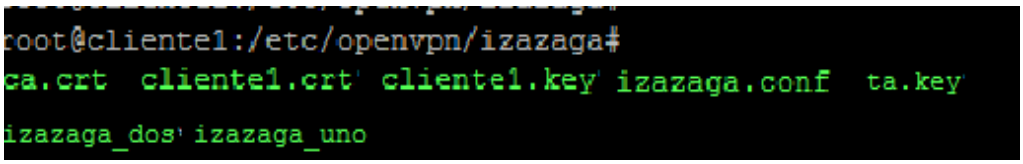


Figura 29.Visualizacion de certificados y ficheros de configuración en el directorio Izazaga.

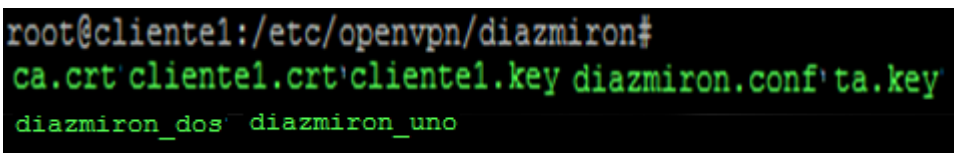


Figura 30.Visualizacion de certificados y ficheros de configuración en el directorio Díaz Mirón.

5.5.4 Script de inicio OpenVPN

Se copia el script de inicio de OpenVPN con la finalidad de modificar la ruta, en donde toma el archivo de configuración para que inicie el servicio.

Esto se realizará dos veces para cada servidor.

Se procederá a la copia de inicio del servicio de OpenVPN para modificar la ruta de inicio de la configuración de izazaga y posteriormente se realizara para Diaz Miron.

cp /etc/init.d/openvpn /etc/init.d/openvpn.izazaga

Editar openvpn.izazaga

vi /etc/init.d/openvpn.izazaga

Modificar la siguiente línea

CONFIG_DIR=/etc/openvpn

Por

CONFIG_DIR=/etc/openvpn.izazaga

Para Díaz Mirón se realiza de la siguiente forma.

cp /etc/init.d/openvpn /etc/init.d/openvpn.diazmiron

Editar openvpn.diazmiron

vi /etc/init.d/openvpn.diazmiron

Modificar la siguiente línea

CONFIG_DIR=/etc/openvpn

Por

CONFIG_DIR=/etc/openvpn.diazmiron

Por lo consecuente para iniciar el servicio de OpenVPN se tendrá que ejecutar las siguientes líneas.

/etc/init.d/openvpn.izazaga start

Y

/etc/init.d/openvpn.diazmiron start

En donde al levantar cualquiera de las dos conexiones pedirá que se proporcione el password, dicho password fue proporcionado por el administrador del servidor de OpenVPN.

5.5.5 Crear script para iniciar y finalizar servicio de OpenVPN

Por comodidad se creará un script en donde se inicie lo servicios de conexión para cada punto y otro script para que finalice la conexión de ambos puntos.

Script de inicio

El script de inicio se creara en el path /etc/openvpn.

chmod 777 tunel_inicio

Este archivo contendrá

/etc/init.d/openvpn.izazaga start
/etc/init.d/openvpn.diazmiron start
ifconfig

Script finalizar servicio.

El script para finalizar el servicio de OpenVPN se creara en el path /etc/openvpn.

vi tunel_final

Este archivo contendrá

/etc/init.d/openvpn.izazaga stop
/etc/init.d/openvpn.diazmiron stop
ifconfig

5.5.6 Iniciar y finalizar servicio de OpenVPN

Para iniciar o parar el servicio de OpenVPN se debe de estar en el path "/etc/openvpn" y ejecutar lo siguiente:

Inicio:

./tunel_inicio

Fin:

./tunel_final

Posteriormente pedirá que se proporcionen los password, dichos password fueron establecidos en la elaboración de los certificados del los clientes.

Después de haber iniciado el servicio de OpenVPN el cliente-servidor, podrá establecer comunicación con los equipos del SICOMCE.

5.6 Pruebas

A continuación se describirá el esquema de pruebas realizadas una vez configurados los servidores y los clientes-servidores. Para estas pruebas fueron montados laboratorios los cuales consistieron en conectar los servidores a la red del SACMEX, tanto a enlaces dedicados (Izazaga y Díaz Mirón), como a enlaces

ADSL, dichos servidores de OpenVPN se examinaron en dichas tecnologias y el cliente-servidor (simulación de la OAP) fue conectado a un enlace ADSL y a un switch en el que se conectaron equipos simulando las redes privadas lan de las OAP.

Las pruebas consistieron en que una vez establecida la sesión de tunel de la VPN en ambos servidores, las máquinas que representaban las cajas (red privada de la OAP) podían alcanzar los direccionamientos previamente establecidos para cada sitio (Izazaga y Díaz Mirón) y a su vez las maquinas del SACMEX, también ver a las cajas de cobro.

En la figura 31 y figura 32 se podrán apreciar los laboratorios de pruebas para enlace dedicado y para enlace ADSL.

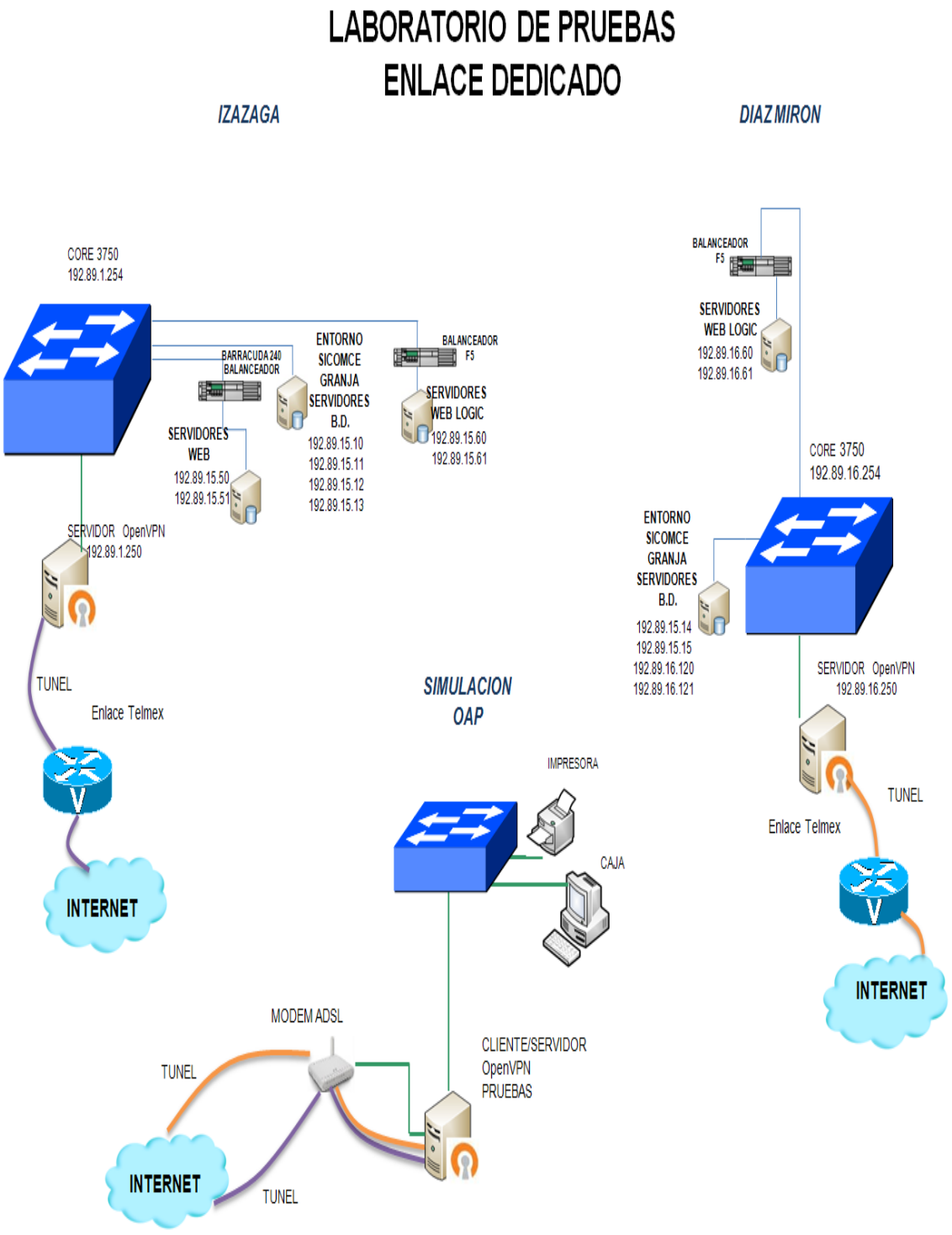


Figura 31.Laboratorio de pruebas de la VPN enlace dedicado.

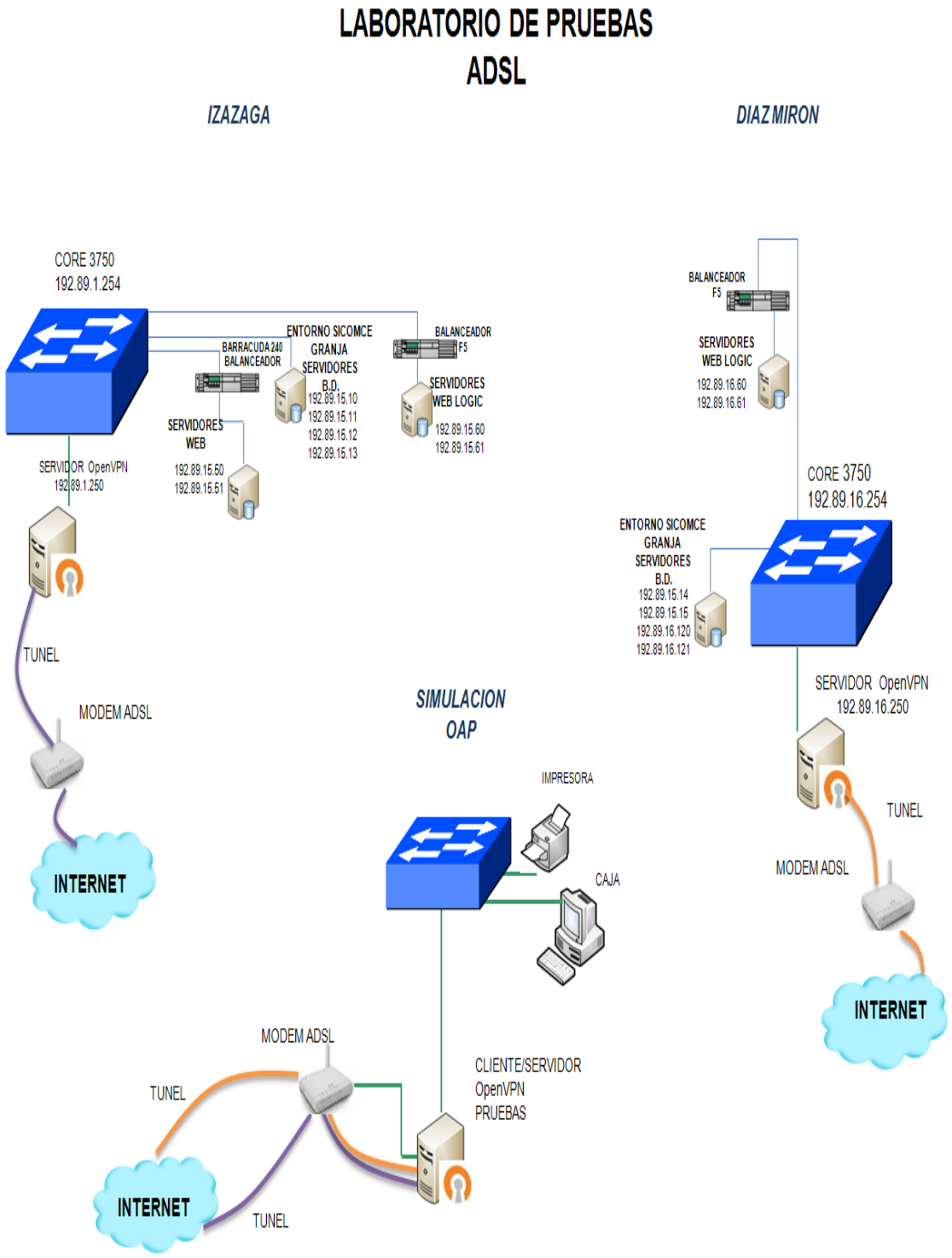


Figura 32.Laboratorio de pruebas de la VPN enlace ADSL.

6. RESULTADOS

Considerando que las pruebas realizadas en los laboratorios fueron exitosas, se decidió probar en la red privada de una OAP de las empresas concesionarias, en donde se plantearon los escenarios de la figuras 31 y 32, se procedio a realizar una prueba en ambiente controlado desconectando el router del enlace MPLS de la red de la OAP, en su lugar se pone el cliente-servidor el cual es conectado a un enlace ADSL y al switch de la red privada de la OAP, enseguida se indicó porque enlace restablecer la comunicación, posteriormente se inició el servicio de OpenVPN donde efectivamente se levantaron los túneles, por lo tanto se establece la comunicación con los equipos del SICOMCE del SACMEX.

Se le pidió al personal de “atención a público” de la OAP que procediera a accesar al SICOMCE y que iniciarán sesión, para realizar pruebas de impresión, consulta y facturación siendo favorables los resultados.

Las pruebas anteriores se realizaron en más OAP de las empresas concesionarias arrojando resultados exitosos.

7. CONCLUSIÓN

El protocolo OpenVPN como mencione anteriromente es seguro, estable y sus tiempos de respuesta son buenos, es por ello que fue una buena decisión el haber optado por esta solución, en el laboratorio de pruebas se obtuvieron buenos resultados y al hacer la prueba en la red local de una OAP, el comportamiento fue faborable. Además de que al servidor se le puede crear otro cliente el cual podrá ser instalado y configurado en sistemas Android, Windows, IOSX y mac OS, se menciona lo anterior debido a que existe personal del sistema comercial del SACMEX que realiza visitas de supervisión a las empresas concesionarias, este personal trabaja en uno de los servidores web del SACMEX por lo que tienen que establecer conexión con este servidor local, lo cual lo podrán hacer desde sus

dispositivos previamente configurados. Este protocolo podrá ser utilizado como LAN to LAN y como road warrior es por ello que le da un plus más a esta solución.

Es importante mencionar que esta solución es buena en caso de una contingencia, ya que si se quiere trabajar todo el tiempo con ella, podría presentar problemas de conectividad debido a que los enlaces ADSL no son constantes por que en ocasiones se interrumpe la comunicación con el ISP.

Durante la implementación y configuración del plan de contingencia se me permitió emplear, comprender y ampliar mis conocimientos en redes de datos, así como el manejo del sistema operativo Linux, uso de software libre donde se pueden implementar diversas soluciones (herramientas de monitoreo de red, correo, servidores DNS, Proxy, etc.) además que es una de las grandes bondades con las que se cuenta en OS Linux y Unix, de igual forma el manejo de nuevas tecnologías.

Otra enseñanza a lo largo de este proyecto fue líderear, en donde comprendí que un buen líder no solo da ordenes, además participa en la capacitacion, asesoramiento y comunicación con el equipo de trabajo, enseñar como se hacen las cosas de tal manera que se comprenda por que se hizo así, de tal forma que el equipo deberá ser capaz de ponerlo en función, Estos conocimientos son de suma importancia para mi formación como Ingeniero en computación.

A lo largo de este proyecto comprendí la importancia de los conocimientos teóricos debido a que son la base para atacar los problemas, complementándose con los conocimientos prácticos en los que intervienen conocimientos técnicos ya que en ocasiones las cosas no resultan como uno espera por no saber hacer las conexiones adecuadas o no saber interactuar con los dispositivos, al unir este conjunto de conocimientos es más fácil la implementación, configuración, detección y solución de problemas.

8. GLOSARIO

8.1 BGP

“Border Gateway Protocol (BGP) es el protocolo de enrutamiento utilizado en internet por los ISP para interconectar distintos sistemas autónomos y sus redes. Su objetivo es proveer un enrutamiento entre sistemas autónomos libre de bucles. Soporta VLSM y CIDR, lo cual ayuda en gran medida a reducir el tamaño de grandes tablas de enrutamiento. BGP no requiere una arquitectura jerárquica y posee la capacidad de soportar múltiples conexiones, acompañándolas con excelentes políticas de control de rutas. BGP se le conoce como un protocolo vector distancia mejorado, o también como protocolo Vector Path, siendo su métrica Path Vectors (Atributos). BGP busca el camino más estable hacia el destino, a diferencia de los otros protocolos de enrutamiento. Además este camino se basa en políticas de enrutamiento, lo cual permite controlar el flujo de tráfico entre los sistemas autónomos.”[9]

Características de BGP

“La conexión se mantiene por keepalive periódicos.

Cualquier cambio en la red resulta una actualización por disparo.

Las métricas utilizadas por BGP, llamadas atributos, permiten gran granularidad en la selección del camino.

Tiene su propia tabla de routing, sin embargo es capaz de compartir y peguntar sobre las tablas de routing interior.

Es posible manipular el flujo de tráfico utilizando atributos. Esto significa que una ruta no puede enviar tráfico si el siguiente salto no quiere.

[9] ZAMBRANO J. 2014http://www.teleccna.cl/bgp.html

BGP no le interesa comunicar a un conocimiento de cada subred de la organización, solo le interesa utilizar suficiente información para encontrar un sistema autónomo.

Las actualizaciones de routing de BGP lleva la sumarización al extremo comunicando únicamente los números de los sistemas autónomos, prefijos de direcciones agregadas e información de routing basada en políticas.”[10]

8.2 DHCP

“DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después.”[11]

Parámetros comunes que asigna un servidor DHCP

- Dirección IP
- Mascara de red
- Gateway (puerta de enlace)
- Dirección del servidor de DNS
- Nombre del servidor WINS

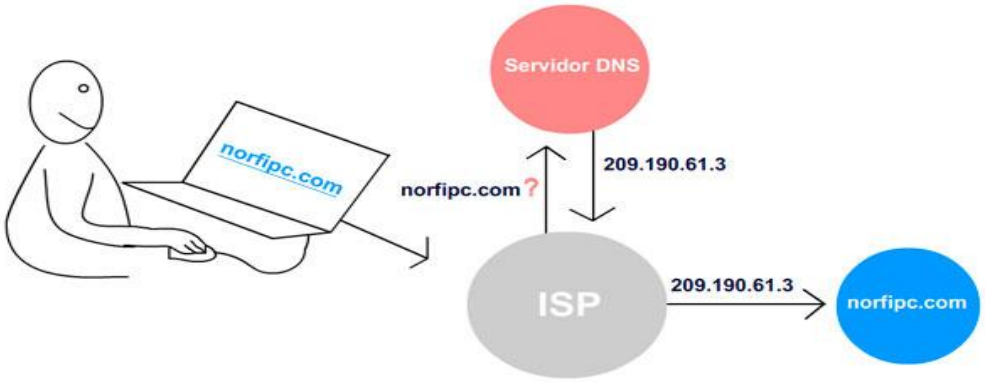
[10] http://trajano.us.es/~rafa/REDES/apuntes/T5-Introduccion_BGP.pdf

[11] https://camber1redes.wordpress.com/dhcp/

8.3 DNS

"Es una abreviatura para Sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios."[12]

Generalmente los usuarios de la red no trabajan con direcciones IP sino con nombres de dominio del estilo de http://www.red.net o correo.soporte.com y como el protocolo IP requiere direcciones IP al enviar sus datagramas. Para esto interviene un proceso que se conoce como resolución de nombres en el que la conversión o resolución de nombres de dominio a direcciones IP, se lleva a cabo por un servidor DNS el cual cuenta con una base de datos en donde tiene vinculadas las direcciones IP con los dominios correspondientes.



Funcionamiento de los servidores DNS

http://norfipc.com/internet/servidores-dns.html

[12] http://www.cuencanet.com.ar/how-to/dns/Definicion_de_DNS.pdf

8.4 DynDNS

Dynamic Network Services, es una empresa de (E.U.) de servicios en la nube especializada en el rendimiento en Internet, dedicada a soluciones de DNS en direcciones IP dinámicas.

8.5 Enlace ADSL

"El ADSL (Asimetric Digital Subscriber Line o Línea de Suscriptor Digital Asimétrica) es una tecnología de banda ancha que permite una velocidad buena (no garantizada "la velocidad constante") en la transmisión de datos e imágenes (Internet), todo ello a través de la línea de teléfono.

Cada usuario se conecta a través de su línea telefónica con un modem a una central telefónica (un cable de cobre) en concreto son dos pares de cobre. Los usuarios que se encuentren en la misma zona se conectan a la misma central y obtienen la interconexión."[13]

8.6 Enlace dedicado

"El servicio "conexión o enlace dedicado" es una conexión que permite estar conectado permanentemente en INTERNET, las 24 horas del día, los 365 días del año, sin requerir el uso de una línea telefónica, es una conexión que no se apaga al dejarla de utilizar y no se enciende al quererla utilizar, es una conexión permanente de alta calidad, confiable y segura.

Este tipo de conexión facilita el acceso a INTERNET a los usuarios y especialistas de redes locales, brindándoles la oportunidad de instalar servidores Web, de correo electrónico y mucho más aplicaciones en la red LAN de la Institución o empresa. No es necesario el uso de líneas telefónicas y garantiza un ancho de banda asegurado con alto nivel de confiabilidad, estabilidad y seguridad." [14]

[13] http://www.grupointerclan.com/internet/enlaces_dedicados.pdf
[14] http://www.grupointerclan.com/internet/enlaces_dedicados.pdf

8.7 Forward

"El mecanismo de "IP forwarding" se encarga de la retransmisión de los paquetes que se reciben por una interfaz física y de retransmitirlos por otra interfaz hacia otro nodo.

Cuando un paquete IP se recibe por una interfaz física, el modulo IP de entrada (IP_{input}) procesa el paquete. Si la dirección IP destino del paquete se corresponde con la del dispositivo se procesa el paquete y se pasa al modulo $TCPi_{nput}$.

En caso de que la dirección IP destino no se corresponda con la del dispositivo y el módulo IP forwarding está desactivado, el paquete IP se descarta.

En el caso de que la dirección IP destino no se corresponda con la del dispositivo y el módulo IP forwarding esté activado, se pasa el paquete al módulo IP de salida (IP_{output}), se consulta la tabla de encaminamiento y el paquete se retransmite por la interfaz correspondiente."[15]

8.8 Iptables

IPtables es un sistema de firewall vinculado al kernel de Linux, se basa en la aplicación reglas que definen políticas de filtrado del tráfico que circula por la red, realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

8.9 ISP

"Los proveedores de servicios de Internet (ISP), son las empresas y organizaciones que proporcionan a los usuarios el acceso a Internet y servicios relacionados. Estos proveedores conectan a sus clientes con los clientes de otros proveedores de servicio por medio de redes. A menudo, los Proveedores de servicios de Internet (también llamados Proveedores de acceso a Internet) son empresas que proporcionan servicios de telecomunicaciones, incluyendo el

[15] http://studies.ac.upc.edu/FIB/STD/lab/IP_forwarding.pdf

acceso a las comunicaciones de datos y la conexión telefónica. La mayoría de las empresas telefónicas también funcionan como Proveedores de acceso a Internet. Los ISP pueden ser comerciales, sin fines de lucro, de propiedad privada o propiedad de la comunidad."[16]

8.10 MPLS

"MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (Forward Equivalence Class), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio.

Los nodos MPLS al igual que los "router" IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar,

[16] http://es.xfinity.com/resources/internet-service-providers.html

tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. "[17]

Elementos de la red MPLS

Label Switch Router "LSR"

Nodo dentro de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada paquete.

Edge Label Switching Router, "Edge LSR"

Nodo MPLS de borde que maneja trafico que ingresa o sale de una red MPLS.

El de entrada adiciona etiqueta a cada paquete y designa el LSP.

El de salida extrae etiqueta del paquete IP y enruta según capa 3.

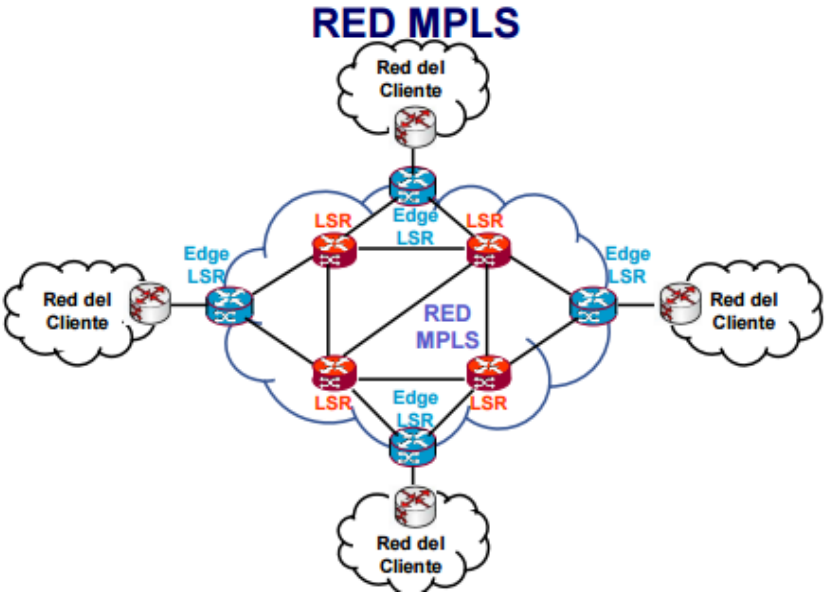
Label Switch Path "LSP"

Camino completo a través de la red (MPLS) que el FEC debe seguir tomando en cuenta su destino y su QoS (calidad de servicio) demandada.

Forwarding Equivalence Class "FEC"

Grupo de paquetes IP, ó flujos enviados por el mismo trayecto y con el mismo tratamiento (Dirección IP de origen o destino, valor de campo protocolo (protocol ID), valor de DSCP (nivel de prioridad del paquete IP)).

[17] http://www.ramonmillan.com/tutoriales/mpls.php#sthash.1xzm0GDq.dpuf



http://www-2.dc.uba.ar/materias/tc/downloads/diapositivas/MPLS-parte1-1C2011.pdf

8.11 SSH

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor, que permite a los usuarios conectarse a un host remotamente para manejar por completo la computadora mediante un intérprete de comandos. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

8.12 Traceroute

Es una herramienta de diagnóstico de redes. Esta herramienta permite determinar la ruta efectuada por un paquete. El comando Traceroute se puede usar para diagramar un mapa de los routers que se encontraron entre la máquina fuente y la máquina destino. El similar a traceroute en el sistema operativo Windows es tracert.

BIBLIOGRAFIA

- MARTINEZ E. 2007 http://www.eveliux.com/mx/redes-lan-can-man-y-wan.php
- PASTOR R. 2009) http://www.anexom.es/tecnologia/mi-conexion/vpn-%C2%BFque-es-y-para-que-sirve/
- http://www.cisco.com/web/LA/soluciones/la/vpn/index.html
- Ramírez D.2011 http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
- http://www.15dejuniomnr.com.ar/blog/apunteca/Definiciones%20de%20Ingenieria.pdf
- http://www.dgae.unam.mx/planes/aragon/Ing-comp_aragon.pdf
- https://sites.google.com/site/cursotelecomunicaciones/defincion_telecomunicaciones
- http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm
- http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm
- http://www.naguissa.com/universidad/wiki-td/SSL_TLS.html
- http://geeks.ms/blogs/enterprise/archive/2015/05/24/conectando-redes-con-nat-e-ip-din-225-micas-mediante-vpn-site-to-site-a-azure.aspx
- http://openvpn.net/index.php/open-source/documentation/howto.html
- http://www.linuxparatodos.net/web/comunidad/base-de conocimiento//wiki/Base+de+Conocimiento/Servidor+Virtual+Private+Network+(VPN)
- http://www.direccionip.com/
- https://sites.google.com/site/gestionderedesdedatossmt/puertos-y-servicios/puertos-fisicos/puertos-fisicos
- http://www.metropolitano.edu.mx/libros/semestre%206/FB6S_MetInvest.pdf

- http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html
- MILLÁN R. http://www.ramonmillan.com/tutoriales/mpls.php
- http://www.goldenfrog.com/ES/vyprvpn/features/vpn-protocols
- prezi.com/bdag5b4_m18k/redes-privadas-virtuales/
- es.slideshare.net/GabyElith/mtodos-de-encriptacin-en-las-redes-privadas-virtuales
- http://es.xfinity.com/resources/internet-service-providers.html
- http://www-2.dc.uba.ar/materias/tc/downloads/diapositivas/MPLS-parte1-1C2011.pdf
- ZAMBRANO J. 2014http://www.teleccna.cl/bgp.html
- http://www.cisco.com/cisco/web/support/LA/7/76/76167_bgp-toc.html
- http://trajano.us.es/~rafa/REDES/apuntes/T5-Introduccion_BGP.pdf
- https://camber1redes.wordpress.com/dhcp/
- http://www.cuencanet.com.ar/how-to/dns/Definicion_de_DNS.pdf
- http://norfipc.com/internet/servidores-dns.html
- https://camber1redes.wordpress.com/dns/
- http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/ch-ssh.html
- http://es.ccm.net/contents/357-traceroute
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-firewall-ipt-fwd.html
- http://www.pello.info/filez/firewall/iptables.html
- http://www.redeszone.net/redes/openvpn/
- http://trixmontero.blogspot.mx/2008/10/servidor-web-con-dyndns-e-ip-dinamica.html
- https://itiramos.wordpress.com/2014/11/13/configurar-red-estatica-en-ubuntu-server-14-04-lts/
- https://github.com/metral/restore_networking
- http://es.dyn.com/apps/update-client-faqs/
- http://studies.ac.upc.edu/FIB/STD/lab/IP_forwarding.pdf
- http://www.ual.es/~vruiz/Docencia/Apuntes/Networking/Protocols/Level-3/02-encaminamiento/index.html
- http://iptables.webnode.es/definicion-de-iptables/
- https://community.openvpn.net/openvpn/wiki/Topology