

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR
FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y
TELECOMUNICACIONES



**“DISEÑO DE UNA RED PRIVADA VIRTUAL ORIENTADA AL
TELETRABAJO DE ORGANIZACIONES CON ESCASOS
RECURSOS ECONÓMICOS POR LA COYUNTURA DEL COVID-19”**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de
INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

CASANOVA ROBLES, ABRAHAM

Villa el Salvador

2020

DEDICATORIA

A mi madre por haber forjado el profesional que soy en la actualidad, gracias a ella con cada palabra de aliento que me dio en los momentos que más lo necesite, es que logre culminar mi profesión.

A mis Hermanos y mi Padre, ejemplos de superación académica y personal, por su apoyo incondicional, siempre presentes con su amor incondicional.

A mi novia que, con su apoyo emocional, paciencia y comprensión supo siempre estar presente en los peores y mejores momentos.

AGRADECIMIENTO

En primer lugar, siempre a Dios por haberme dado una Madre que supo guiarme por el camino correcto y que no se amíñalo frente a las adversidades de la vida.

A mi asesor, Carlos Mugruza, por su profesionalismo como guía de apoyo, a lo largo de todo mi trabajo de sustentación profesional, gracias a sus recomendaciones y observaciones, siendo claves en todo el proceso.

A mis profesores de la universidad, cada uno de ellos supo aportar una pieza fundamental en mi desarrollo profesional a lo largo de mi carrera universitaria.

ÍNDICE

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
LISTADO DE FIGURAS.....	viii
LISTADO DE TABLAS.....	xii
RESUMEN.....	1
INTRODUCCIÓN.....	2
OBJETIVOS.....	4
a. General.....	4
b. Específicos.....	4
CAPÍTULO I: MARCO TEÓRICO.....	5
1.1 BASES TEÓRICAS.....	5
1.1.1 ANTECEDENTES DE LA INVESTIGACIÓN.....	5
a. Antecedente Nacional.....	5
b. Antecedente Internacional.....	6
1.1.2 CONCEPTOS ESPECÍFICOS.....	8
1.1.2.1 Red Privada Virtual (VPN).....	8
1.1.2.2 Tipos de Redes Privadas Virtuales.....	9
a. Red Privada Virtual de acceso remoto:.....	9
b. Red Privada Virtual de sitio a sitio:.....	10
1.1.2.3 COMPONENTES PARA ESTABLECER UNA VPN.....	11
a. Autenticación:.....	11
b. Tunnelización (Tunneling):.....	12
c. Cifrado:.....	12
1.1.2.4 Protocolo de Túnel punto a punto (PPTP):.....	12
1.1.2.5 Protocolo de túnel de capa 2 (L2TP):.....	13

1.1.2.6 Protocolo de Seguridad de Internet (IPsec):.....	13
1.1.2.7 Protocolo de Intercambio de claves en internet (Protocolo IKE):	13
1.1.2.8 Calidad de servicio (QoS):.....	14
1.1.2.9 Modelo de Red:	14
1.1.2.10 Mikrotikls SIA:.....	15
1.1.2.11 Routerboard:	15
1.1.2.12 RouterOS:	15
1.1.2.13 Configuración RouterOS:	16
1.2 DEFINICIÓN DE TÉRMINOS BÁSICOS	17
CAPÍTULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO	
PROFESIONAL.....	22
2.1 DELIMITACIÓN DEL PROYECTO.....	22
2.1.1 Delimitación Teórica	22
2.1.2 Delimitación Espacial	22
2.1.3 Delimitación Temporal.....	22
2.2 DETERMINACIÓN Y ANÁLISIS DEL PROBLEMA	23
2.2.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA	23
2.2.2 JUSTIFICACIÓN DEL PROBLEMA	26
2.2.3 FORMULACIÓN DEL PROBLEMA	27
2.2.3.1 Problema General	27
2.2.3.2 Problemas Específicos	27
2.3 MODELO DE SOLUCIÓN PROPUESTO.....	27
2.3.1 Fase de Análisis	29
a. Análisis Logístico.....	29
b. Análisis de Infraestructura Tecnológica.....	30
2.3.2 Fase de Planteamiento.....	31
a. Puntos que determinaron usar el tipo de Red Privada Virtual de acceso remoto:	31

b. Puntos que determinaron usar el tipo de Red Privada Virtual de sitio a sitio: ..	31
c. Puntos que determinaron el uso de la tecnología Mikrotik Routerboard:.....	32
d. Puntos que determinarán si se usará la IP Pública del proveedor de Internet que se tiene contratado en la Organización o un dominio Cloud VPN, en la configuración.....	32
2.3.3 Fase de configuración Mikrotik.....	33
2.3.3.1 Configuración de acceso a internet en RB Mikrotik.....	33
2.3.3.2 Configuración de Red privada Virtual Mikrotik por tipo de VPN	42
a. Configuración – Tipo VPN de Acceso Remoto:.....	42
i. Escenario: Ip Pública Estática - Protocolo PPTP.....	42
ii. Escenario: Ip pública Estática – Protocolo L2TP/IPsec	47
b. Configuración – Tipo VPN de Sitio a Sitio:	51
i. Escenario: Ip Pública Estática - Protocolo PPTP.....	51
ii. Escenario: Ip Pública Estática - Protocolo L2TP/IPsec.....	60
2.4 RESULTADOS	65
2.4.1 RESULTADO DE ANÁLISIS Y DIAGNÓSTICO	65
2.4.1.1 Resultados de Análisis y Diagnóstico para la Organización Q. H. S. E....	65
2.4.1.2 Resultados de Análisis y Diagnóstico para la Organización KT PERÚ	67
2.4.2 RESULTADOS DE MODELAMIENTO	72
2.4.2.1 Resultados de Modelamiento para la organización Q. H. S. E.....	72
2.4.2.2 Resultados de Modelamiento para la organización KT PERÚ	74
2.4.3 RESULTADOS DE INVERSIÓN	78
2.4.3.1 Resultados de Inversión para la organización Q. H. S. E.....	78
2.4.3.2 Resultados de Inversión para la organización KT PERÚ	80
CONCLUSIONES.....	82
RECOMENDACIONES	83
REFERENCIAS BIBLIOGRÁFICAS	84
ANEXOS	87

ANEXO A: Configuración Dominio Nube VPN	87
ANEXO B: Pruebas realizadas en el RB Mikrotik – Q. H. S. E.....	91
ANEXO C: Especificaciones MIKROTIK RB750R2.....	95
ANEXO D: Especificaciones MIKROTIK RB450GX4	97

LISTADO DE FIGURAS

Figura 1: Esquema de Red Privada Virtual de la empresa Hardsoft S.A.	7
Figura 2: Red Privada Virtual de acceso remoto.	9
Figura 3: Red Privada Virtual de sitio a sitio.	11
Figura 4: EDT del Diseño de una VPN para Organizaciones con Bajos Recursos.	28
Figura 5: Topología de implementación VPN Básica en una Sede.	33
Figura 6: Icono de Herramienta WINBOX	34
Figura 7: Ventana principal de Inicio WINBOX.....	34
Figura 8: Ventana de configuración de nombre de interfaces - WINBOX	35
Figura 9: Ventana de configuración de nombre de interfaces - WINBOX	36
Figura 10: Ventana de configuración de nombre de interfaces - WINBOX	36
Figura 11: Ventana de configuración de nombre de interfaces - WINBOX	37
Figura 12: Lista de interfaces - WINBOX.....	37
Figura 13: Configuración IP LAN - WINBOX.....	38
Figura 14: Configuración IP WAN - WINBOX.....	38
Figura 15: Lista de direcciones IPs - WINBOX.....	39
Figura 16: Configuración de enmascaramiento para WAN- WINBOX	39
Figura 17: Enmascarado WAN- WINBOX	40
Figura 18: Configuración GATEWAY con la dirección IP de enrutador Proveedor – WINBOX	40
Figura 19: Lista de rutas - WINBOX	41
Figura 20: Configuración DNS - WINBOX.....	41
Figura 21: Configuración PPP - WINBOX	42
Figura 22: Configuración PPP - WINBOX	43
Figura 23: Configuración IP Pool VPN - WINBOX.....	43
Figura 24: Configuración IP Pool VPN - WINBOX.....	44
Figura 25: Lista de direcciones IP LAN / WAN - WINBOX	44
Figura 26: Perfil PPP - WINBOX.....	45
Figura 27: Perfil PPP – Pestaña Protocolos - WINBOX	45
Figura 28: Perfil PPP - Pestaña “Secrets” - WINBOX	46
Figura 29: Perfil PPP - Pestaña “Secrets” - WINBOX	46

Figura 30: Pestaña “L2TP Server” - WINBOX	47
Figura 31: Pestaña “New PPP Secret” - WINBOX	48
Figura 32: Pestaña “New PPP Secret” - WINBOX	48
Figura 33: Pestaña “New Firewall Rule “- Protocolo UDP - WINBOX	49
Figura 34: Pestaña “New Firewall Rule - Protocol IPsec” - WINBOX	50
Figura 35: Aplicando protocolos - WINBOX	50
Figura 36: Reglas en Pestaña Cortafuego (<i>Firewall</i>) - WINBOX.....	51
Figura 37: Lista de dirección que incluye Ip Pública de sede secundaria - WINBOX.....	51
Figura 38: Lista de rutas que incluye Ip Pública de sede secundaria - WINBOX	52
Figura 39: Pestaña PPP donde se habilita el “PPTP Server” - WINBOX	52
Figura 40: Pestaña PPP donde se habilita el “PPTP Server Binding” - WINBOX	53
Figura 41: Pestaña PPP donde se coloca el nombre del servicio habilitado – WINBOX	53
Figura 42: Pestaña “Profiles” donde se configuran IP Estática de punto a punto – WINBOX	54
Figura 43: Configuración de perfil - Ip Estática de punto a punto – WINBOX	54
Figura 44: Configuración usuario de acceso en el túnel PPTP - WINBOX.....	55
Figura 45: <i>Firewall</i> , puerto de conexión del servicio PPTP - Protocolo TCP – WINBOX	55
Figura 46: “ <i>Firewall</i> ”, puerto de conexión del servicio PPTP - Protocolo GRE – WINBOX	56
Figura 47: Lista de rutas – agregando ruta de Sede Secundaria - WINBOX	57
Figura 48: Lista de direcciones de la Sede Secundaria – WINBOX.....	57
Figura 49: Lista de rutas de la Sede Secundaria - WINBOX.....	58
Figura 50: Pestaña PPP – <i>Interface</i> – PPTP <i>Client</i> - WINBOX.....	58
Figura 51: Pestaña “ <i>Dial Out</i> “– Sede Secundaria - WINBOX.....	59
Figura 52: Pestaña “General “– Sede Secundaria - WINBOX.....	59
Figura 53: Configuración PPTP en la pestaña PPP de la Sede Secundaria - WINBOX.....	60
Figura 54: Pestaña “PPP – L2TP Server “– Sede Principal - WINBOX.....	61
Figura 55: Pestaña “IP – IPsec - Peer “– Sede Principal - WINBOX	61
Figura 56: Pestaña “PPP – Secrets “– Sede Principal - WINBOX.....	62

Figura 57: Pestaña “ <i>PPP – Interface – L2TP Client</i> ” – Sede Secundaria – WINBOX.....	62
Figura 58: Pestaña “ <i>Interface – Dial Out</i> ” – Sede Secundaria – WINBOX	63
Figura 59: Visualización pestaña “ <i>PPP – Interface</i> ” Sede Secundaria – WINBOX	63
Figura 60: Visualización pestaña “ <i>Route List</i> ” Sede Secundaria – WINBOX	64
Figura 61: Topología Organización Q. H. S. E.	67
Figura 62: Topología Sede Principal KT PERÚ	70
Figura 63: Topología Sede Secundaria KT PERÚ	71
Figura 64: Modelamiento Organización Q. H. S. E.	72
Figura 65: Visualización de la lista de interfaces totales - Q. H. S. E. - WINBOX	73
Figura 66: Modelamiento de la interconexión entre las dos sedes de KT PERÚ, usando una VPN Tipo de Sitio a Sitio	75
Figura 67: Modelamiento de la Sede Principal KT PERÚ.	75
Figura 68: Modelamiento de la Sede Secundaria KT PERÚ.....	76
Figura 69: Visualización de la lista de interfaces totales - KT PERÚ - WINBOX	77
Figura 70: Pestaña “ <i>Certificates</i> ” – WINBOX	87
Figura 71: Visualización pestaña “ <i>Interfaces – OVPN Client</i> ” – WINBOX.....	88
Figura 72: Configuración pestaña “ <i>Interfaces – ovpn-out1</i> ” – WINBOX	89
Figura 73: Trafico sobre la “ <i>ovpn-out1</i> ” <i>configurada con el dominio</i> “core12.cloud2site.com” – WINBOX.....	90
Figura 74: “ <i>PPP- secrets</i> ” dentro del RB Mikrotik Q. H. S. E. - WINBOX	91
Figura 75: Dirección IP - WAN RB Mikrotik Q. H. S. E - WINBOX	92
Figura 76: Dirección IP - LAN Usuario remoto - WINDOWS 10	92
Figura 77: Agregar conexión VPN en equipo Usuario - WINDOWS 10	93
Figura 78: Agregar conexión VPN en equipo Usuario - WINDOWS 10	93
Figura 79: CMD - PING - WINDOWS 10	94
Figura 80: CMD - TRACERT - WINDOWS 10	94
Figura 81: Lista de direcciones - Conectividad de usuario TEST NOVA- WINBOX	95
Figura 82: - Detalles - MIKROTIK RB750R2	95
Figura 83: Potenciado de consumo - MIKROTIK RB750R2.....	96
Figura 84: Velocidad de puertos de interfaz - MIKROTIK RB750R2	96

Figura 85: MIKROTIK RB450GX4.....	97
Figura 86: MIKROTIK RB450GX4 Especificaciones	98

LISTADO DE TABLAS

Tabla 1: Empleo formal en Lima Metropolitana según sectores económicos, 2019 – Porcentaje de la población ocupada en cada sector.	24
Tabla 2: Cronograma de ejecución de actividades del Proyecto.	27
Tabla 3 Velocidad de transferencia máxima de datos por las capas de los medios de comunicación – Modelo OSI (Q. H. S. E.)	74
Tabla 4 Velocidad de transferencia máxima de datos por las capas de los medios de comunicación – Modelo OSI (KT PERÚ).....	77
Tabla 5 Comparación de precios mínimos y máximos de los equipos que se pueden utilizar en una implementación VPN, tomando en consideración principales marcas proveedoras.....	78
Tabla 6 Costo total de la implementación VPN - Q. H. S. E.....	80
Tabla 7 Costo total de la implementación VPN - KT PERÚ	81

RESUMEN

El presente Trabajo de Suficiencia Profesional Titulado “Diseño de una Red Privada Virtual orientada al Teletrabajo de Organizaciones con escasos Recursos Económicos, por la coyuntura del COVID-19”, trata acerca del diseño y modelamiento de implementación, orientado a la tecnología e infraestructura de Redes Privadas Virtuales (VPN), usando dispositivos Mikrotik y de cómo son tan imprescindibles en la pandemia que estamos viviendo.

La elaboración del trabajo comprende realizar tres fases para lograr un diseño óptimo de VPN, y de implementación accesible en toda organización que lo necesite. La primera Fase es de Análisis, donde se desarrolla un diagnóstico logístico y de infraestructura tecnológica en redes. La segunda Fase es de Planteamiento, donde se determinará qué tipo de VPN se implementará, tomando en cuenta las necesidades de la organización y evaluando también que tipo de dispositivo Mikrotik será conveniente en la misma. La tercera Fase es de Configuración, en la cual se procederá a configurar el tipo de equipo Mikrotik, así como el tipo de VPN que se eligió para el diseño, tomando en cuenta que en este trabajo se evaluaron posibles escenarios para que se logre la interconectividad VPN, es decir, así la organización no cuente con todos los recursos necesarios para dicha interconexión, igual se lograra dar solución a lo que se necesite, como por ejemplo la Ip Pública estática, que se puede reemplazar por un Dominio Nube VPN.

El Diseño se enfoca en ofrecer una propuesta viable en el aspecto tecnológico y financiero, para que toda organización y en específico las de bajos recursos, puedan contar con una VPN que les permita seguir efectuando operaciones laborales, así como frenar la propagación del COVID-19, gracias al distanciamiento social que nos brinda la nueva normalidad del teletrabajo, evitando así los contagios y dando una ciberseguridad de interconexión laboral.

Palabras claves: Implementación, diseño, tecnología e infraestructura de VPN, COVID-19.

INTRODUCCIÓN

En la coyuntura actual que vivimos por la pandemia del COVID-19, existen organizaciones con bajos recursos económicos, que presentan la problemática de seguir con normalidad sus operaciones laborales, así como de disponer del trabajo de todos sus colaboradores, los cuales viven en una disyuntiva diaria de movilizarse hasta sus centros de trabajo y ser infectados en el transcurso de dicha movilización, o de quedarse en sus hogares con el temor de bajas de sueldo y en un caso más crítico ser despedidos sin oportunidad de conseguir un nuevo trabajo en las circunstancias actuales.

La Constitución Política del Perú establece que el trabajo, en sus diversas formas y modalidades, es objeto de atención prioritaria del Estado, así como dispone que ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales, ni desconocer o rebajar la dignidad del trabajador (Artículo 23 de la Constitución Política del Perú, 1993). Por lo tanto, toda organización deberá velar por la seguridad de sus empleados, implementando medidas de trabajo contemporáneas, tales como el teletrabajo, que permite dar continuidad en las operaciones, así como de reducir el daño colateral de posible contagio que afectaría a sus colaboradores o su entorno, y por ende limitar la propagación del virus en la ciudadanía.

Una Red Privada Virtual (VPN) es una solución tecnológica de conexión cifrada que brinda la interconexión de las organizaciones entre sus sedes y con sus empleados, en modo teletrabajo. Pero como toda implementación tecnológica, implica una inversión acorde con los requerimientos y necesidades de cada organización, para lo cual dicha inversión según los estándares de costos empresariales, son en su mayoría de medios a elevados, entre \$/. 2237,2 a \$/. 3044,91 como se menciona en la tesis de Torres Rodríguez (2016, p. 50) y la cifra sigue en aumento dependiendo si la empresa requiere más funcionalidades incluidas en la Red Privada Virtual (VPN), así como hardware que soporte dichos requerimientos de manera óptima, tales como CISCO, JUNIPER, etc.

En el presente trabajo se diseñó una Red Privada Virtual (VPN), teniendo como prioridad contemplar una reducción significativa de la inversión, utilizando

tecnología de hardware MikroTik RouterBOARD (SIA Mikrotiks, 1996-2020), con el objetivo de dar continuidad laboral a las organizaciones empresariales o gubernamentales de bajos recursos, interconectando las redes locales (LAN) y las redes externas o ampliadas (WAN), empleando la arquitectura en hardware de redes que la organización ya tenga en uso. El desarrollo del trabajo se realizará mediante tres fases: análisis, planteamiento e implementación, las cuales integrarán la configuración de: túneles IP, seguridad encriptada, modo puente (*Bridge mode*) para enrutador (*router*) operador nativo, dominio nube IP (*Domain Cloud IP*) y demás particularidades.

OBJETIVOS

a. General

Realizar un diseño de Red Privada Virtual (VPN), usando tecnología Mikrotik RouterBOARD (SIA Mikrotīkls, 1996-2020), optimizando el rendimiento de la infraestructura de redes, en la parte física y lógica. Además, de lograr accesibilidad en costos de inversión, para asegurar la continuidad laboral mediante el teletrabajo en las organizaciones de bajos recursos.

b. Específicos

- Analizar y diagnosticar las posibles soluciones de reutilización, por sobre la infraestructura ya existente de hardware y software de redes locales (LAN).
- Realizar un modelamiento óptimo de una arquitectura de redes, para implementar una Red Privada Virtual (VPN), con equipos Mikrotik RouterBOARD (SIA Mikrotīkls, 1996-2020).
- Reducir el costo de inversión para la implementación de una VPN, sin afectar la calidad y el rendimiento tecnológico de su arquitectura.

CAPÍTULO I: MARCO TEÓRICO

1.1 BASES TEÓRICAS

1.1.1 ANTECEDENTES DE LA INVESTIGACIÓN

a. Antecedente Nacional

Hoy en día las tecnologías de la información y comunicación (TICS), nos permiten interconectarnos y comunicarnos a nivel mundial, a través de sus diversos códigos de información, tales como imágenes, textos, sonido, etc. Siendo algunos de los medios: celulares, tabletas, computadores y demás recursos digitales, los cuales permiten dicha interconexión e interacción entre la informática y las telecomunicaciones mediante el internet, y por ello es fundamental considerar las (TICS), dentro del diseño e implementación de toda Red Privada Virtual (VPN). En la Tesis de Martel (2019), diseñó e implementó una red de comunicación VPN sobre internet, que permitió la comunicación en tiempo real y agilización de los procesos de negocio en la organización, mediante un eficiente uso de los recursos TI basado en el RFC 2764. Esto debido a que identificó el problema de la falta de comunicación en tiempo real entre la sede principal y sus sucursales de la organización e implementó la solución bajo un marco para redes privadas virtuales basadas en IP (RFC 2764). Teniendo como resultado una VPN con una topología centralizada en la organización, e interconecto su sede principal y sucursales, además de lograr un nivel de disponibilidad óptimo.

En la Tesis de Atencio, Mamani (2017), se realizó el Diseño e implementación de una Red Privada Virtual en capa 3 del modelo de Interconexión de Sistemas Abiertos (OSI), con la finalidad de prevenir ataques cibernéticos y riesgos de pérdida de información en la transacción de envíos entre las diferentes oficinas de la Universidad Nacional del Altiplano. Para ello utilizaron tecnología CISCO, realizando pruebas de transmisión de datos de punto a punto, encriptándolos y encapsulándolos, en conjunto de la utilización de protocolos Ipsec para capa 3 o capa de red. Teniendo como resultado un rendimiento mínimo de 89.29% de cada 56 datos transmitidos, a partir de pruebas realizadas antes de la implementación,

la cual se realizó entre la Oficina de Tecnología e Informática y las coordinaciones académicas de las 19 facultades de la Universidad Nacional del Altiplano. Además, se contempló el diseño de esta Red Privada Virtual bajo la utilización del túnel IPsec punto a punto que trabaja bajo la política ISAKMP de IKE brindando confidencialidad, integridad y autenticación a la red, estableciendo así un tráfico de datos seguros en las oficinas de la institución que operan bajo la Red Privada Virtual implementada.

b. Antecedente Internacional

A medida que el mundo es más vulnerable debido a la pandemia del COVID-19, las Redes Privadas Virtuales (VPN), se han tomado de suma importancia y se han incrementado como solución necesaria en toda organización académica y laboral. La utilización de cualquier red de comunicaciones pública, naturalmente, plantea nuevos problemas de seguridad, que no se presentan al utilizar entornos más controlados como líneas arrendadas punto a punto en una red local (LAN), es por ello que se pone énfasis en la seguridad encriptada que nos ofrece una Red Privada Virtual. En el artículo de Favale et al. (2020) analizaron el impacto de la pandemia COVID-19 que conllevó la adopción de medidas que se tomaron para dar continuidad académica en la Universidad de Turin en Italia, tomando como punto de referencia el campus Politécnico de Torino, en el cual se implementó dos servicios principales a manera de contingencia en esta pandemia, para acceder a los recursos internos del Campus mientras se trabaja desde casa, los cuales fueron el servicio de Red Privada Virtual (VPN) y Protocolo de Escritorio Remoto (RDP), mostrando cómo ha cambiado con el tiempo la cantidad de usuarios que dependen de las VPN y las soluciones de escritorio remoto (RDP). Las VPN se utilizan para acceder a los servicios y servidores del campus, mientras que RDP permite acceder de forma remota a los archivos o ejecutar aplicaciones en las computadoras de su oficina. El campus Politécnico de Torino ofrece servicios VPN tanto sobre IPsec como SSL. Curiosamente, el uso de VPN basada en SSL aumenta significativamente más que la solución basada en IPsec. Esto indicó un crecimiento de los usuarios no expertos a recurrir a una VPN, y han optado por una VPN basada en SSL, que es más fácil de configurar.

En el trabajo de Grado de Prieto (2011) se implementó un diseño de Red Privada Virtual (VPN), para la empresa HardSoft S.A. el cual consistió en la utilización de un canal de internet, para la comunicación privada entre sus oficinas remotas, usuarios, proveedores, clientes y empleados, aplicando encapsulamiento de un protocolo de red sobre otro creando un túnel de red, el establecimiento de este túnel se implementó incluyendo una Unidad de Protocolo de Datos (PDU) determinada, dentro de otra Unidad de Protocolo de Datos (PDU) con el objetivo de transmitir desde un extremo al lado del túnel sin ser necesaria una interpretación intermedia de la PDU encapsulada, ello asegura una eficiencia óptima de ciberseguridad, utilizando transmisión de datos encriptados.

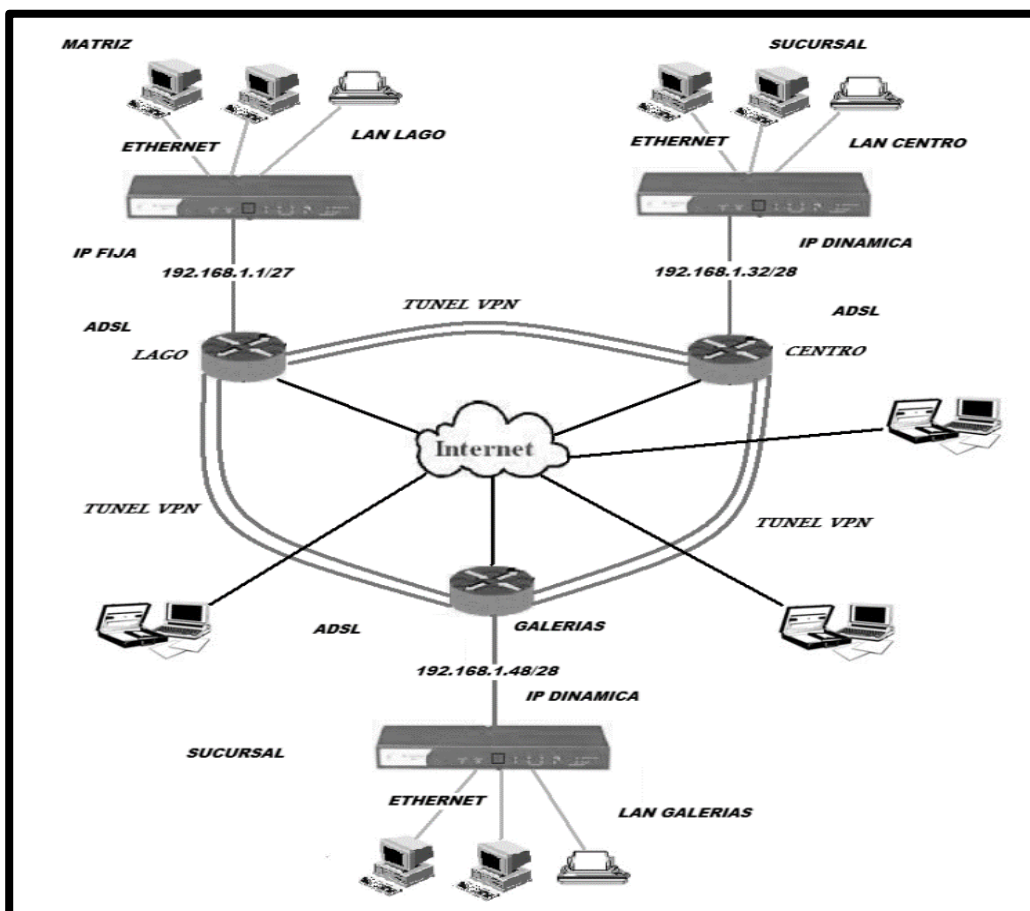


Figura 1: Esquema de Red Privada Virtual de la empresa Hardsoft S.A.

Fuente: Trabajo de Grado de Prieto (2011).

El diseño de Red Privada Virtual que se implementó en la empresa Hardsoft S.A. se realizó desde cero, tomando en consideración la arquitectura de redes e informática con la cual la empresa ya contaba antes de la implementación, esto con

el fin de evitar inconsistencias en el futuro para la empresa y en reducción de costos de inversión que implicaría adquirir recursos tecnológicos para una implementación tecnológica de este tipo.

1.1.2 CONCEPTOS ESPECÍFICOS

1.1.2.1 Red Privada Virtual (VPN)

Según Mar (2016). Una red privada virtual - VPN (*Virtual Private Network*), es una tecnología de red que permite extender la red local sobre una red pública, con el fin de evitar un costoso sistema de arrendamiento o compra de líneas, que será utilizada por una sola organización.

El objetivo de una VPN es ofrecer a la organización las mismas capacidades de seguridad, pero a un menor costo, esta tecnología también:

- Nos da la posibilidad de interconectar dos o más sucursales de la empresa utilizando como medio el Internet.
- Permite a los trabajadores de una determinada empresa, la conexión desde sus casas al centro de cómputo.
- Hace posible que los usuarios puedan tener acceso a su equipo del hogar desde algún lugar remoto.

1.1.2.2 Tipos de Redes Privadas Virtuales

El Diseño de implementación se basa en dos tipos de Red Privada Virtual:

a. Red Privada Virtual de acceso remoto:

Según Castro (2019). Este tipo de Red Privada Virtual proporciona acceso remoto a una intranet o extranet corporativa, permitiendo a los usuarios acceder a los recursos de la compañía siempre que lo requieran, con el cliente VPN instalado o configurado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre. Las VPN de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión con un ISP local.

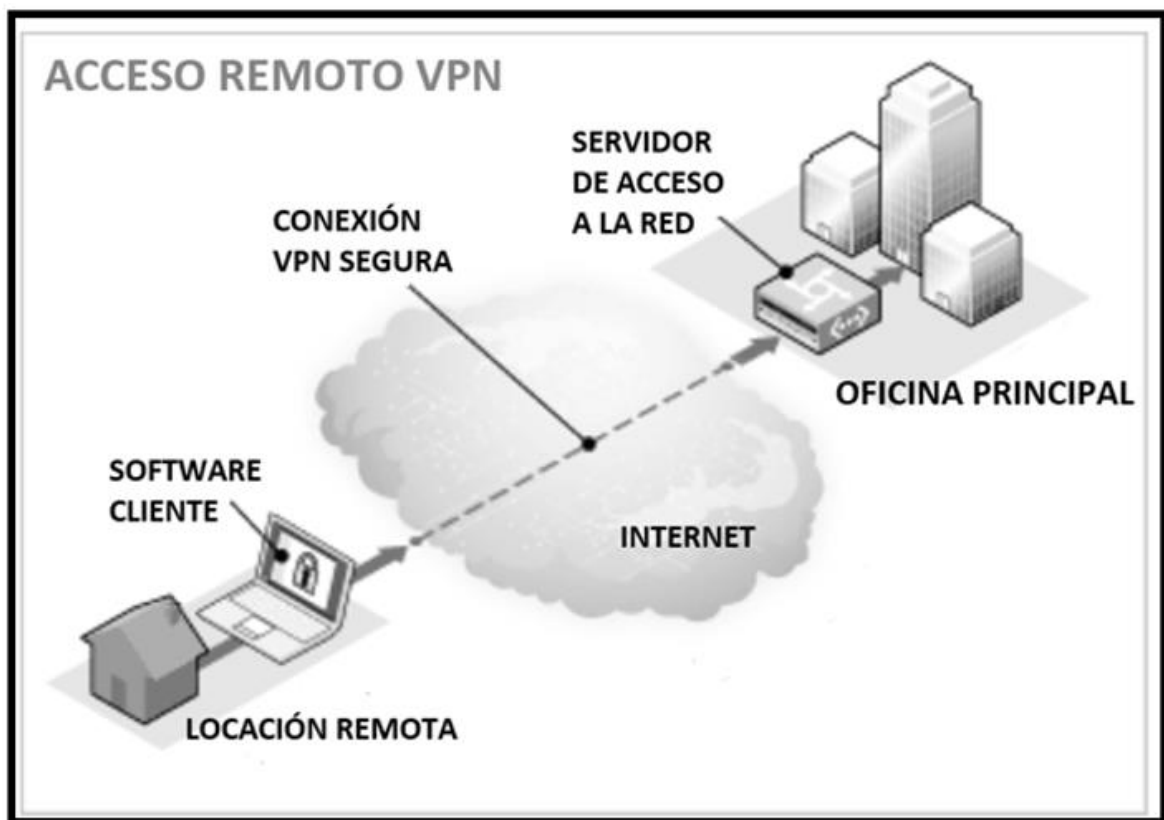


Figura 2: Red Privada Virtual de acceso remoto.

Fuente: Bhattarai y Nepal (2016).

b. Red Privada Virtual de sitio a sitio:

Según Grados, Vásquez (2012) sirve para conectar oficinas remotas con la sede de la organización. El servidor VPN (en la sede principal) acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su ISP. Es decir permite eliminar los costosos vínculos punto a punto tradicionales como los canales de datos sobrevalorados, sobre todo en las comunicaciones internacionales, además según Bhattarai & Nepal (2016) tenemos que se subdivide en dos tipos.

i. Basada en Intranet: Si una empresa tiene una o más ubicaciones remotas que deseen unirse en una.

ii. Basada en Extranet: Cuando una empresa tiene una estrecha relación con otra compañía (por ejemplo, un socio, proveedor o cliente), se puede construir una VPN Extranet que conecta redes de área local de esas empresas. Esta extranet VPN permite a las empresas trabajar juntos en un entorno de red seguro compartido, al mismo tiempo que se evita el acceso a sus redes internas separadas.

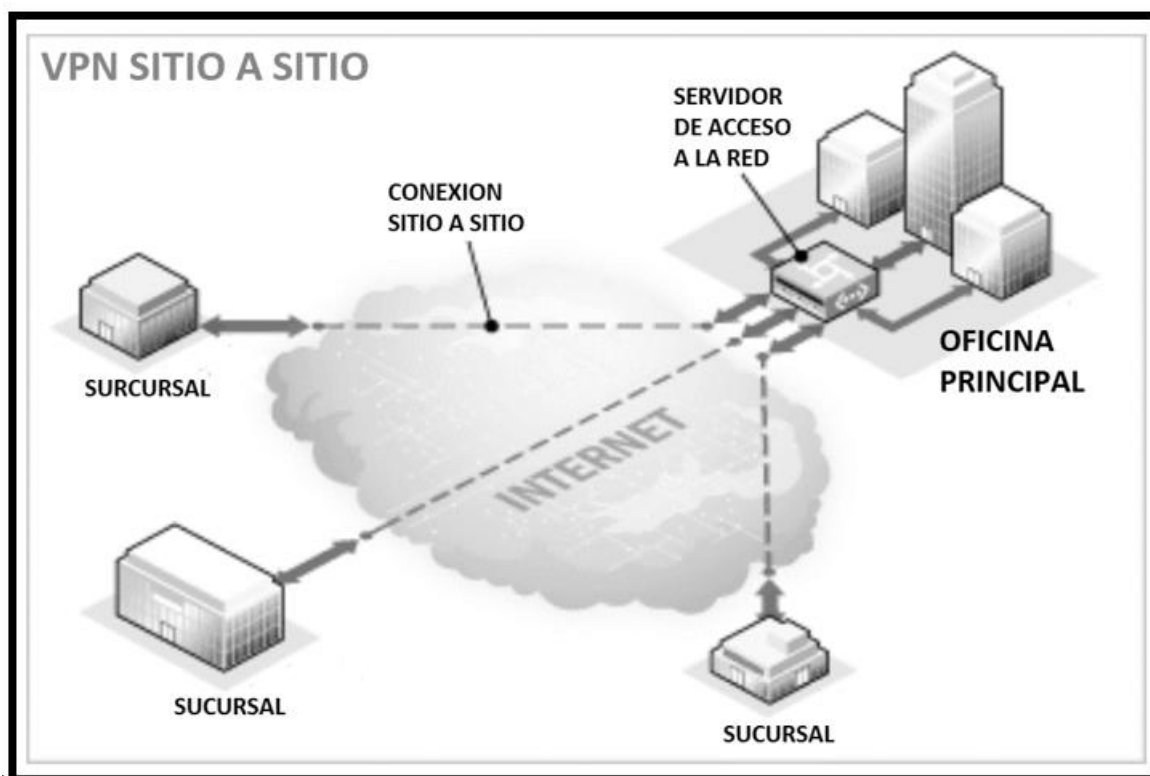


Figura 3: Red Privada Virtual de sitio a sitio.

Fuente: Bhattarai & Nepal (2016)

1.1.2.3 COMPONENTES PARA ESTABLECER UNA VPN

Toda Red Privada Virtual (VPN) está compuesta por 3 elementos:

a. Autenticación:

Según Bhattarai & Nepal (2016). Es necesario que los puntos finales del túnel deban ser autenticados para poder establecer túneles VPN seguros. La autenticación se puede realizar mediante contraseñas, biometría, autenticación de dos factores u otros métodos criptográficos, en estos túneles de red a red suelen utilizarse contraseñas o certificados digitales, los cuales se pueden almacenar de forma permanente como puntos clave para permitir que el túnel VPN se establezca automáticamente, sin intervención del usuario a no ser que fuera requerido.

b. Tunnelización (Tunneling):

Según la Tesis de Atencio, Mamani (2017). El *tunneling* es un método utilizado para encapsular paquetes (datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Esto ofrece grandes ventajas, ya que permite el transporte de protocolos con diferente esquema de direccionamiento. El *tunneling* es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

c. Cifrado:

Según Bhattarai & Nepal (2016). El cifrado de datos, proporciona confidencialidad de datos que se envían entre el cliente VPN y el servidor VPN a través de una red compartida o pública, donde siempre hay un riesgo de interceptación no autorizada. También se puede configurar el servidor VPN para forzar cifrado comunicaciones. Los usuarios que se conectaran al servidor que debe cifrar sus datos o no se permitirá la conexión. Para las conexiones VPN, la familia Windows Server utiliza el Protocolo Punto a Punto (PPTP) y el protocolo de seguridad de Internet (IPSec) de encriptación con la capa de protocolo de túnel (L2TP).

1.1.2.4 Protocolo de Túnel punto a punto (PPTP):

Según la Tesis de Mendoza (2010), PPTP es un protocolo de red que permite la transferencia desde clientes remotos a servidores localizados en redes privadas (LAN). Para ello emplea tanto líneas telefónicas conmutadas como Internet. PPTP es una extensión de PPP que soporta control de flujos y túneles usando multiprotocolo sobre el protocolo de internet.

1.1.2.5 Protocolo de túnel de capa 2 (L2TP):

Según la Tesis de Martel (2019), fue diseñado por el Grupo de Trabajo de Ingeniería de Internet (IETF) conformado por las mismas compañías creadoras de los protocolos: Protocolo de túnel punto a punto (PPTP) y Protocolo de reenvío de capa 2 (L2F), con el fin de corregir las deficiencias de estos protocolos, es así que L2TP heredó de PPTP y del L2F las mejores funciones y características. L2TP es un protocolo que crea un túnel entre un cliente y servidor (ambos L2TP) donde encapsula las tramas PPP para su envío a través de redes como IP. Una vez establecido el túnel se configura un mecanismo de autenticación de usuario con el fin de establecer su identidad. A través de las redes internas IP, L2TP utiliza el Protocolo de Datagrama de Usuario (UDP) y una serie de mensajes L2TP con el fin de crear, mantener y optimizar los túneles por donde se transmiten los datos.

1.1.2.6 Protocolo de Seguridad de Internet (IPsec):

Según el artículo de investigación de Hauser et al. (2020) el Protocolo de Seguridad de Internet (IPsec) es un conjunto de protocolos de red privada virtual muy extendido. El cual aplica autenticación y cifrado en la IP en escenarios de comunicación de host a host, puerta de enlace a puerta de enlace y de host a puerta de enlace.

1.1.2.7 Protocolo de Intercambio de claves en internet (Protocolo IKE):

Según el artículo de investigación de Hauser et al. (2020) se utiliza en la configuración del túnel IPsec, el cual requiere la configuración del usuario más material de codificación que intercambia los pares IPsec a través de dicho Protocolo de intercambio de claves (IKE). En resumen, este protocolo intercambia las claves en internet, utilizándose además para generar y gestionar las claves necesarias para establecer las conexiones de cabecera de autenticación (AH) y la carga de seguridad encapsulada (ESP).

1.1.2.8 Calidad de servicio (QoS):

Según el artículo de investigación de Caicedo-Muñoz et al. (2018), la Calidad de Servicio (QoS) en las redes, se preocupa por gestionar cualquier congestión en la misma, que afecta directamente a su rendimiento en relación con los parámetros de fluctuación, ancho de banda y algunos parámetros cuantitativos en la gestión de la red. Es decir, la Calidad de Servicio (QoS) se aplica a manera de mecanismo que asegura la priorización óptima del tráfico en el enlace.

1.1.2.9 Modelo de Red:

Según Santos (2014) define: “los modelos en capas, como el modelo TCP/IP, se utilizan para visualizar la interacción entre los protocolos”. Tenemos dos tipos de modelos de redes:

a. Modelo de protocolo: La arquitectura TCP/IP propone la existencia de cinco niveles: físico, enlace, red, transporte y aplicación. Como se observa, la diferencia más obvia es que en este modelo no aparecen los niveles de sesión y presentación. Lo que ocurre es que cualquier función por encima del nivel de transporte en TCP/IP se implementa en el nivel de aplicación. Los niveles con más similitudes entre el modelo OSI y el modelo TCP/IP son los de red y de transporte. (Santos, 2014, pág. 110).

b. Modelo de referencia: OSI es una arquitectura basada en niveles para el diseño de sistemas de red, que permite la interconexión de sistemas abiertos, es decir permite que dos sistemas diferentes se puedan comunicar independientemente se tenga indistinto tipo arquitectura (Santos, 2014, pág. 103).

1.1.2.10 Mikrotikls SIA:

Según SIA Mikrotikls (1996-2020). Mikrotikls SIA es una empresa dedicada a desarrollar enrutadores y sistemas de ISP inalámbricos. MikroTik ahora ofrece hardware y software para la conectividad a Internet en la mayoría de los países del mundo. Mikrotik es una empresa letona que fue fundada en 1996 para desarrollar dispositivos enrutadores y sistemas inalámbricos ISP. Mikrotik ahora proporciona hardware y software para la conexión a Internet en la mayoría de los países de todo el mundo. Su experiencia en el uso de la industria de hardware de PC estándar y sistemas de enrutamiento completos permitió en 1997 crear el sistema de software RouterOS que proporciona una amplia estabilidad, controles, y la flexibilidad para todo tipo de interfaces de datos y enrutamiento. En 2002, decidió hacer su propio hardware, y surge la marca RouterBOARD. Existen distribuidores y clientes en la mayoría de las partes del mundo.

1.1.2.11 Routerboard:

Según SIA Mikrotikls (1996-2020). Mikrotik Routerboard es la plataforma de hardware que engloba todos los productos de la empresa MikroTik. Se incluye en el hardware los diferentes tipos de placas electrónicas con las que se pueden ensamblar enrutadores (routers).

1.1.2.12 RouterOS:

Según SIA Mikrotikls (1996-2020). Mikrotik RouterOS es un sistema operativo basado en el kernel de Linux 2.6 usado en el hardware de los Mikrotik RouterBOARD que es la división de hardware de la marca Mikrotik. Se caracteriza por poseer su propio S.O. de fácil configuración. Estos dispositivos poseen la ventaja de tener una relación costo/beneficio muy alto.

Ahora, lo que hace interesante a un RouterOS es que puede ser instalado en una computadora, convirtiéndola en un router con todas las características

necesarias: firewall, routing, punto de acceso wireless, administración de ancho de banda, servidor VPN y más.

1.1.2.13 Configuración RouterOS:

Según SIA Mikrotikls (1996-2020). RouterOS soporta varios métodos de configuración como son:

- Acceso local vía teclado y monitor
- Consola serial con una terminal
- Acceso vía Telnet y SSH vía una red
- Una interfaz gráfica llamada WinBox
- Desarrollo de aplicaciones propias para la configuración de sus dispositivos.
- En caso de no contar con acceso local y existe un problema con las direcciones IP RouterOS soporta una conexión basada en direcciones MAC usando las herramientas customizadas Mac-Telnet y herramientas de Winbox.

1.2 DEFINICIÓN DE TÉRMINOS BÁSICOS

1.2.1 Red de Área Local (LAN): Es una interconexión de dispositivos de red, dentro de una misma área específica.

1.2.2 Red de Área Amplia (WAN): Es una red de dispositivos que interconecta varias redes de área local (LAN).

1.2.3 Protocolo de mensajes de control de Internet (ICMP): Es un protocolo que detecta y reporta errores de red encontrados en el sistema de redes de dispositivos.

1.2.4 Protocolo de control de transmisión (TCP): Es un protocolo que pertenece a la capa de transporte del modelo TCP/IP, que permite que dos dispositivos que se encuentran comunicados controlen el estado de la transmisión.

1.2.5 Protocolo de datagramas (UDP): Es un protocolo que permite la transmisión de datos sin conexión previa, de esta manera envía información rápidamente sin un proceso de validación de conexión.

1.2.6 Tecnologías de Información y Comunicación (TIC): Son las herramientas tanto hardware como software, que gestionan, transmiten y comparten la información de datos mediante soportes tecnológicos.

1.2.7. Protocolo de Internet (IP): Es un protocolo de comunicación de datos e información, que se clasifica en la capa de red del modelo OSI.

1.2.8 Dirección IP: Es un número que identifica dispositivos de una red.

1.2.9 Dirección IP Pública: Es la Ip que nos brinda el proveedor de acceso a internet, puede ser una Ip Pública Estática o Dinámica.

1.2.10 Dirección IP Privada: Es la Ip que sirve para identificar dispositivos dentro de una Red Local (LAN).

1.2.11 Protocolo de Cubierta Segura (SSH): El protocolo SSH permite a los usuarios acceder remotamente a dispositivos de red, dentro de lo cual nos permite modificar datos de forma segura en los dispositivos.

1.2.12 Host: Es cualquier dispositivo conectado a una red a través de un dominio y un número de IP estático definido.

1.2.13 Dominio: Es un nombre asociado a una dirección IP Pública de internet.

1.2.14 Servidores: Son computadoras que permiten alojar y compartir recursos en la infraestructura de la red de una organización, con los demás dispositivos en su red.

1.2.15 Switch: Es un dispositivo conmutador de interconexión que se utiliza para conectar varios dispositivos en red, formando la Red Local (LAN).

1.2.16 Internet: Es una red de redes que permite la interconexión descentralizada de dispositivos a través de un conjunto de protocolos denominado TCP/IP.

1.2.17 Intranet: Es una red interna que admite un determinado tipo de infraestructura de red para dar acceso a los usuarios de la organización.

1.2.18 Extranet: Es una red privada que a través de internet comparte la información y operaciones de la organización, mediante una plataforma de comunicación entre las partes internas y externas.

1.2.19 Cortafuegos (*Firewall*): Sistema de seguridad que impide el acceso no autorizado a un dispositivo mientras se encuentra conectado en la red.

1.2.20 Ping: Es un comando de diagnóstico que permite realizar la verificación de correcta conexión con un determinado host local.

1.2.21 Cable UTP: Es un cable de par trenzado sin blindaje utilizado en las conexiones físicas en la Red Local (LAN).

1.2.22 Internet de las cosas (IOT): Es la interconexión de objetos físicos a través de una red, donde todos pueden ser visibles entre sí e interactuar en simultáneo.

1.2.23 Circuito Cerrado de Televisión (CCTV): Es una red de dispositivos que genera la visualización de imágenes en video dentro de un ambiente implementado.

1.2.24 Grabador de Video Digital (DVR): Es un dispositivo que centraliza la grabación de las imágenes captadas por cámaras analógicas conectadas a él, transformándose en formato digital.

1.2.25 Grabador de Vídeo en Red (NVR): Es un dispositivo que graba y administra imágenes ya digitales provenientes de cámaras IP conectadas en la red.

1.2.26 Marcadores Biométricos: Son dispositivos que sirven para marcar la asistencia o el control de acceso del personal de la organización mediante su huella dactilar.

1.2.27 Soporte Lógico inalterable (*Firmware*): Es el programa básico que se encuentra dentro de cualquier dispositivo electrónico y lo controla.

1.2.28 Dominio Nube VPN (*DOMAIN CLOUD VPN*): Es un dominio alojado en un servidor de la nube, el cual sirve como método alternativo de conexión VPN.

1.2.29 Sistema de Nombre de Dominio (DNS): Es el sistema que regula la resolución de nombres en internet, ya que traduce las direcciones IP en direcciones numéricas accesibles a los dispositivos de conexión.

1.2.30 Memoria Caché: Es el área de almacenamiento temporal de un dispositivo que guarda datos para acelerar su velocidad de operatividad.

1.2.31 WINBOX: Es una aplicación de herramienta que sirve para gestionar dispositivos Mikrotik RouterOS usando una interfaz gráfica.

1.2.32 Dirección MAC: Es un identificador único asignado por los fabricantes a una tarjeta de control de red, incorporada a todo dispositivo que se pueda conectar en red

1.2.33 Modo Puente (*BRIDGE*): Es un modo de configuración que se realiza en el enrutador para compartir la conexión y sus funciones con otro enrutador.

1.2.34 Algoritmo HASH: Es un algoritmo matemático que transforma indistintamente un bloque arbitrario de datos, en una nueva serie de caracteres que tiene una longitud de tamaño fijo.

1.2.35 Protocolo de carga útil de seguridad encapsulada (ESP): Es un protocolo usado dentro de IPSec. Consiste en que cuando deseas enviar o recibir datos a través de una interconexión de red, los convierte en paquetes de información para que pueda viajar dentro de la interconexión de red.

CAPÍTULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO PROFESIONAL

2.1 DELIMITACIÓN DEL PROYECTO

2.1.1 Delimitación Teórica

El presente proyecto tiene como desarrollo el diseño de una Red Privada Virtual orientada a organizaciones con bajos recursos, implementado en dos organizaciones de Lima Metropolitana. Dichas organizaciones se vieron en la necesidad de implementar una VPN debido a la continuidad laboral que deseaban dar a sus operaciones en la pandemia del COVID19.

2.1.2 Delimitación Espacial

EL proyecto se realizará en dos organizaciones de Lima Metropolitana las cuales son: KLIMATECHNIK S.A.C. y Q. H. S. E., Lima, Perú.

2.1.3 Delimitación Temporal

Comprende en los periodos de marzo y septiembre del 2020.

2.2 DETERMINACIÓN Y ANÁLISIS DEL PROBLEMA

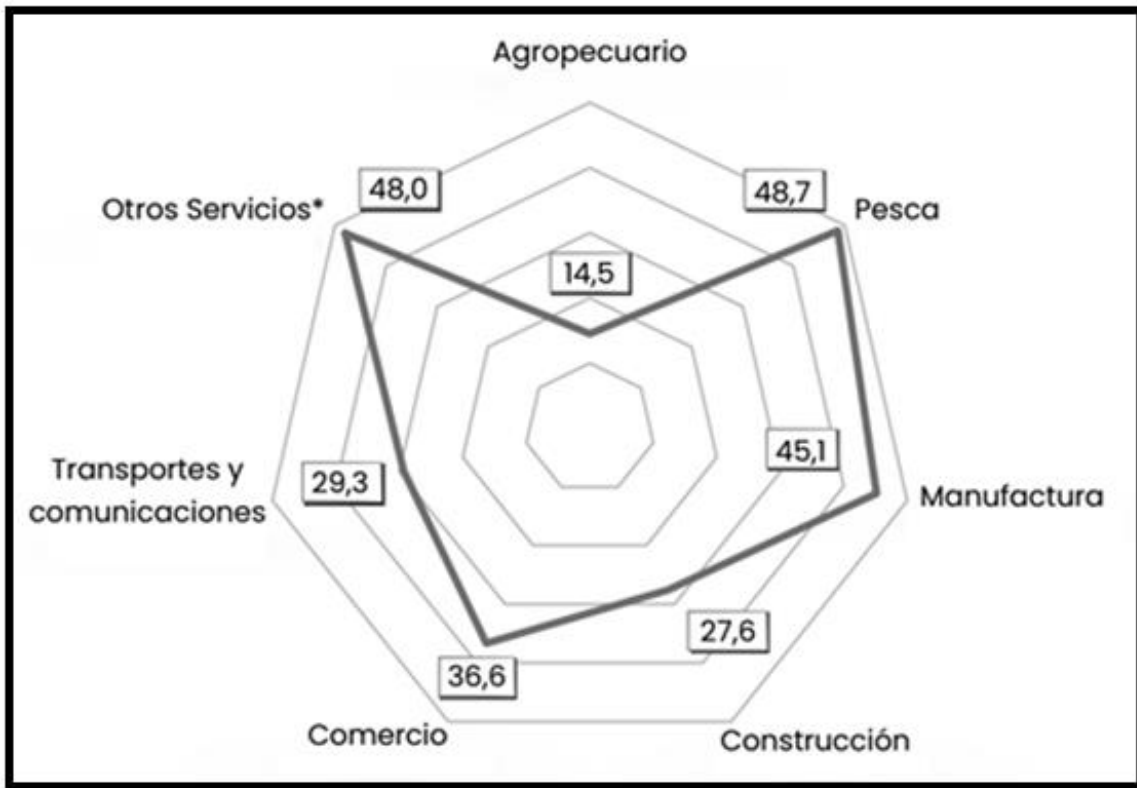
2.2.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En la actualidad, la Organización Mundial de la Salud ha calificado, con fecha 11 de marzo de 2020, el brote de Coronavirus (COVID-19) como una pandemia al haberse extendido en más de cien países de manera simultánea, tal como se señala en la Resolución Ministerial N°239-2020-MINSA. Causando no solo afectaciones en la salud y el bienestar público a nivel mundial, sino también interrupción en la continuidad laboral para las organizaciones empresariales y gubernamentales.

Un plan de contingencia que el Estado Peruano implementó, para evitar la propagación del COVID-19 entre las personas, fue el aislamiento y distanciamiento social obligatorio, como se indica en el DECRETO SUPREMO N°044-2020-PCM, lo cual propició una incertidumbre que recae sobre las organizaciones, de enfrentar con los recursos tecnológicos que tienen, los desafíos y consecuencias de la interrupción laboral que se presenta actualmente y se presentará en los meses venideros.

Teniendo en consideración la problemática descrita en el ámbito mundial y nacional, vemos que nos enfrentamos como país a un decrecimiento inminente de producción en varios sectores industriales. La caída de la producción traerá como correlato el descenso en la cantidad, así como la calidad del empleo. A nivel nacional, el empleo formal es de alrededor de 3,8 millones de trabajadores, de los cuales el 56,8% se encuentra en Lima. (Instituto de Economía y Desarrollo Empresarial – CCL, 2020).

Tabla 1: Empleo formal en Lima Metropolitana según sectores económicos, 2019 – Porcentaje de la población ocupada en cada sector.



Fuente: Instituto Nacional de Estadística e Informática (INEI) – Elaboración: Instituto de Economía y Desarrollo Empresarial (IEDEP).

Por lo mencionado anteriormente, Lima es el departamento donde la crisis sanitaria del COVID-19 está causando mayor afectación laboral, debido a que las organizaciones de bajos recursos no contemplan un plan de contingencia que pueda asegurar su continuidad de producción y operación, o en su defecto no tienen los medios económicos, ni asesoría profesional que pueda respaldar una implementación tecnológica efectiva para sobrellevar la interrupción laboral que se está presentando y seguirá, hasta que se logre superar en su totalidad esta crisis sanitaria.

Hoy en día existen herramientas tecnológicas que contribuyen al desarrollo y la continuidad del trabajo colaborativo no presencial, tales como los diferentes tipos de Redes Privadas Virtuales (VPN), pero estas implican una inversión de recursos

de hardware y software de alto presupuesto, para lo cual se busca el diseño de una Red Privada Virtual a bajo costo, pero que a su vez cumpla con los estándares óptimos para el teletrabajo de los colaboradores.

En el apartado de Resultados del Capítulo II, se pondrá como ejemplo dos empresas de Lima Metropolitana, en las que se requiere una Red Privada Virtual. La primera es KLIMATECHNIK S.A.C. | KT PERU SAC, empresa dedicada a la carpintería metálica, enfocada en desarrollar planos de estructuras metálicas personalizadas para empresas mineras, empresas de laboratorios de fármacos, etc. Esta empresa se vio sumamente afectada en la pandemia, debido a que sus colaboradores sean operarios como administrativos, no podían movilizarse en su totalidad a la sede de la empresa, perdiendo así el acceso a su servidor principal de diseño de planos, equipo fundamental en su labor diaria. La segunda empresa es QUALITY, HEALTH, SAFETY AND ENVIRONMENT SERVICES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA, dicha empresa se dedica a dar consultoría, auditorías y gestión en Calidad, Prevención de Riesgos, Salud Ocupacional y del Medio Ambiente, la cual también se vio muy afectada debido a que cuenta con un servidor de archivos y controlador de dominio de aplicaciones de gestión para sus colaboradores, lo cuales brindan las certificaciones a sus clientes, y al estar en estado de inmovilización las consultas a nivel red local que se realizaban con destino a su servidor de dominio, se cancelaron totalmente, teniendo un déficit en certificación actualizada para sus clientes.

2.2.2 JUSTIFICACIÓN DEL PROBLEMA

La presente investigación se enfocará en el diseño e implementación de una Red Privada Virtual a bajo costo de inversión, debido a que el modo de trabajo presencial se ha visto afectado y forzado a cambiar a un modo teletrabajo, esto por los recientes acontecimientos del COVID-19 en la coyuntura actual, siendo el aislamiento social y la inmovilización, dos medidas fundamentales para evitar la propagación del coronavirus que nuestro gobierno peruano ha indicado en la población, tal como lo señala el DECRETO SUPREMO N°044-2020-PCM .

Es por ello que se desarrollará un diseño de Red Privada Virtual basado en tecnología Mikrotik RouterBOARD (SIA Mikrotikls, 1996-2020), como una medida de contingencia acorde a las necesidades y posibilidades de organizaciones con bajos recursos, integrando las particularidades de confiabilidad, efectividad y seguridad, por sobre los datos e información que se transmita en la misma.

El proyecto resulta ser viable, ya que una Red Privada Virtual a bajo costo daría solución al problema principal de interrupción de continuidad laboral, por lo que se ven afectadas organizaciones de bajos recursos en esta pandemia del COVID-19, logrando los resultados de ahorro en capital económico, facilidad de una conexión rápida y segura, para los colaboradores a sus sedes de trabajo de manera remota, así como de poder compartir información vital de la organización, de manera encriptada, tal cual estuvieran en su misma red local.

2.2.3 FORMULACIÓN DEL PROBLEMA

2.2.3.1 Problema General

No se realiza continuidad laboral en las organizaciones de bajos recursos, debido a la coyuntura actual del COVID-19, por la falta de un plan de contingencia laboral acorde a sus necesidades y posibilidades adquisitivas.

2.2.3.2 Problemas Específicos

- Existen diferentes infraestructuras ya implementadas de hardware y software para redes locales (LAN), en las organizaciones de bajos recursos.
- No existe un modelo de diseño de Red Privada Virtual (VPN), que permita interconectar a los colaboradores y sus centros de trabajo, en las organizaciones de bajos recursos.
- No se cuenta con un presupuesto de inversión económica, acorde a los costos altos que conlleva implementar una Red Privada Virtual (VPN), en las organizaciones de bajos recursos.

2.3 MODELO DE SOLUCIÓN PROPUESTO

El proyecto realizado se estructura en tres fases: Análisis, Planteamiento y Configuración Mikrotik.

Tabla 2: Cronograma de ejecución de actividades del Proyecto.

ACTIVIDADES	TIEMPO (Días)									
	1	2	3	4	5	6	7	8	9	10
Fase Análisis	x	x	x							
Fase Planteamiento				x	x					
Fase Configuración						x	x	x	x	x

Fuente: Propia

Se presenta también la Estructura del Desglose del Trabajo (EDT), donde veremos los detalles de lo que se realizará en las tres fases del modelo de solución propuesto.

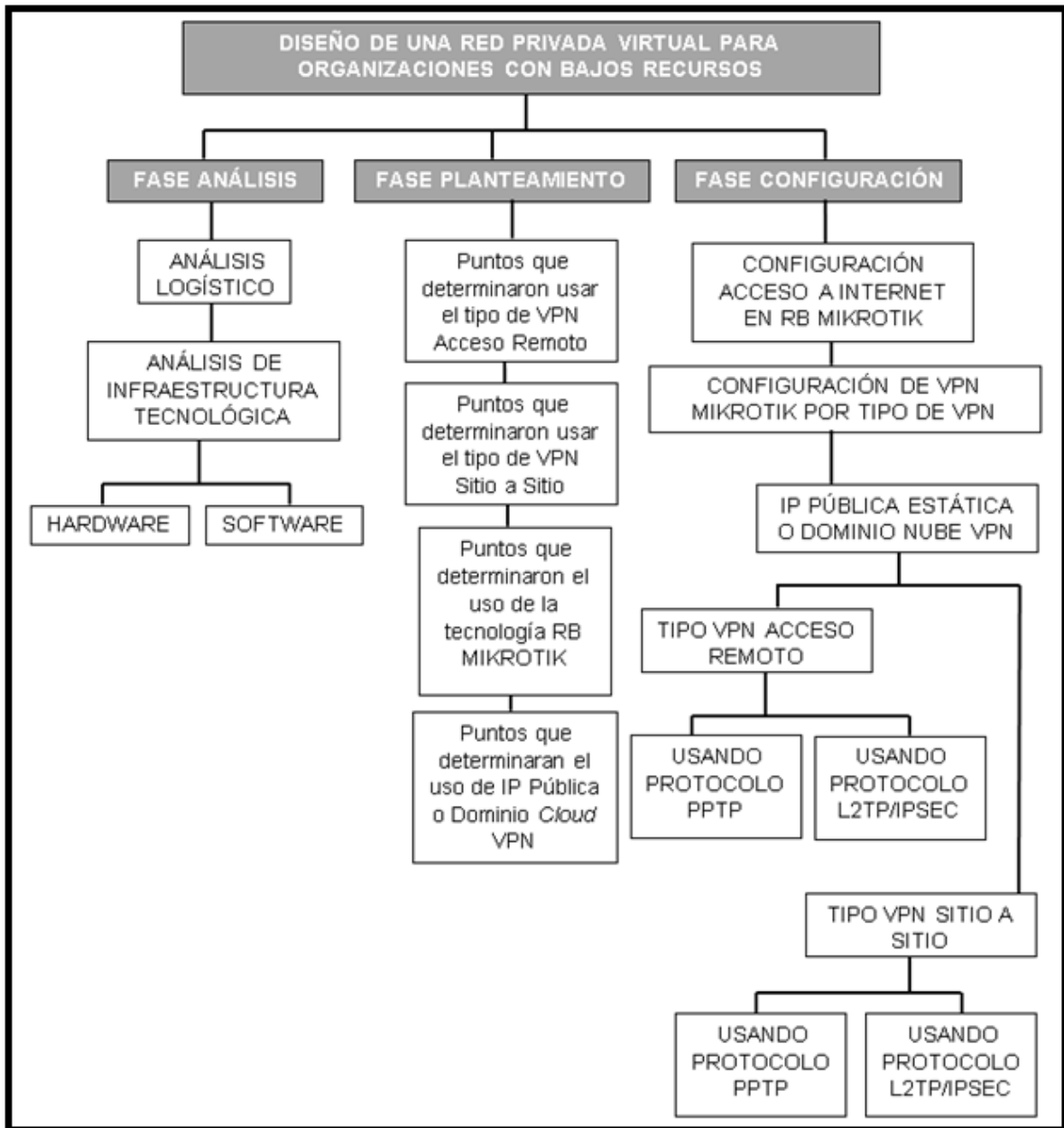


Figura 4: EDT del Diseño de una VPN para Organizaciones con Bajos Recursos.

Fuente: Propia

2.3.1 Fase de Análisis

Es necesario llevar a cabo un análisis previo de cada sede de trabajo, para poder implementar de manera óptima la Red Privada Virtual a bajo costo, utilizando tecnología Mikrotik RouterBOARD (SIA Mikrotīkls, 1996-2020), debido a que nos permitirá tener una imagen clara de cómo se dará la optimización de los procesos en cada sede y sus áreas de trabajo correspondientes, permitiéndonos integrar y automatizar cada parte de la organización. Para ello se subdividió en Análisis Logístico y Análisis de Infraestructura Tecnológica.

a. Análisis Logístico

En esta parte del análisis vemos en qué Áreas, se realizan funciones administrativas y logísticas de la organización, sean empresariales o entidades del estado, dichas áreas pueden estar subdivididas de la siguiente forma:

- Área de Gerencia General.
- Área de Administración y Finanzas.
- Recursos Humanos.
- Área de Soporte técnico.
- Área Comercial.
- Área de Contabilidad.
- Área de Almacén y Despacho.
- Área de Diseño e Imagen.

b. Análisis de Infraestructura Tecnológica

Aquí analizamos que tipo de infraestructuras tecnológicas, son las existentes y que se encuentran en vigente utilización por parte de la organización, sean empresariales o entidades del estado, dichas infraestructuras se encuentran subdivididas en hardware y software:

- **Hardware:** Parte física de la infraestructura tecnológica de la organización, compuesta por:

- Servidor de datos.
- Servidor de dominio.
- Computadores de mesa.
- Computadores portátiles
- Cableado estructurado de cobre (UTP).
- Cableado estructurado de Fibra.
- Repetidores de Señal WIFI.
- DVR y NVR – Circuitos de Video Vigilancia CCTV.
- Marcadores Biométricos de asistencia y control de acceso.
- Impresoras IP.
- Maquinaria con tecnología IOT.

- **Software:** Parte lógica necesaria que hace posible la realización de las tareas específicas de la parte física (Hardware), compuesta por:

- Sistema operativo SERVER.
- Sistema operativo de computadoras de mesa y portátiles.
- Software gestor de Controlador de dominio.
- Firmware de los biométricos.
- Sistema operativo DVR – NVR, circuitos de video vigilancia CCTV.
- Firmware de Impresoras IP.
- Sistema operativo de maquinaria con tecnología IOT.

2.3.2 Fase de Planteamiento

Puntos que determinarán el tipo de VPN que se usará en la organización que lo solicite, validando lo siguiente:

a. Puntos que determinaron usar el tipo de Red Privada Virtual de acceso remoto:

- Este tipo de Red Privada Virtual será usada cuando la organización tenga muchos colaboradores externos, que están ubicados en diferentes puntos de ubicación geográfica y desea interconectarlos con su única sede.
- Teniendo como clientes acceso a los usuarios administrativos y operativos de manera remota, donde cada uno tendrá su respectivo perfil de acceso y seguridad, estableciéndose así una Red Privada Virtual con todos los protocolos de seguridad que se soliciten por la organización.

b. Puntos que determinaron usar el tipo de Red Privada Virtual de sitio a sitio:

- Este tipo de Red Privada Virtual se usará para interconectar dos o más enrutadores entre sí, cuando la organización tenga más de dos sedes, conectando la red local de la sede principal de la organización con sus otras sedes aledañas o socios que deseen formar parte de su red.
- En la implementación se utilizará procesos de cifrado de enrutamiento, entre los túneles de interconexión de sede a sede, direccionamiento, codificación y decodificación que se realiza tanto en el hardware y software de los enrutadores instalados en cada sede.

c. Puntos que determinaron el uso de la tecnología Mikrotik Routerboard:

- La inversión en el dispositivo de red VPN, debe ser accesible para la organización.
- El rendimiento del dispositivo de red VPN, debe ser óptimo.
- La configuración debe ser de fácil acceso y comprensión, por lo tanto, un entorno gráfico y de comandos en una sola línea es lo ideal.
- Es una marca fiable en hardware y software con años de renombre en el mercado de telecomunicaciones.
- El dispositivo de red VPN, debe tener estabilidad para continuidad de trabajo 24/7, así como bajo consumo de energía.
- Estructura robusta del dispositivo que permita una estabilidad de funcionamiento.

d. Puntos que determinarán si se usará la IP Pública del proveedor de Internet que se tiene contratado en la Organización o un dominio Cloud VPN, en la configuración.

- Se usará en la configuración del dispositivo VPN, la Ip Publica que el proveedor de Internet asignó a la organización, si esta es una Ip Pública que pertenece a un plan de internet corporativo, es decir una Ip Pública estática.
- Se usará en la configuración del dispositivo VPN, un Dominio Nube VPN, si la Ip Publica que el proveedor de Internet asignó a la organización, pertenece a un plan de internet hogar, es decir tiene una Ip Pública dinámica, la cual cada vez que se reinicia el equipo enrutador suministrador por el proveedor cambia automáticamente de número.

2.3.3 Fase de configuración Mikrotik

Para esta fase, tendremos en consideración los siguientes pasos:

- Configuración acceso a internet en Router Mikrotik
- Configuración VPN Mikrotik por tipo de VPN.

2.3.3.1 Configuración de acceso a internet en RB Mikrotik

Esta configuración se dará teniendo presente que la topología básica de implementación en toda organización será la siguiente:

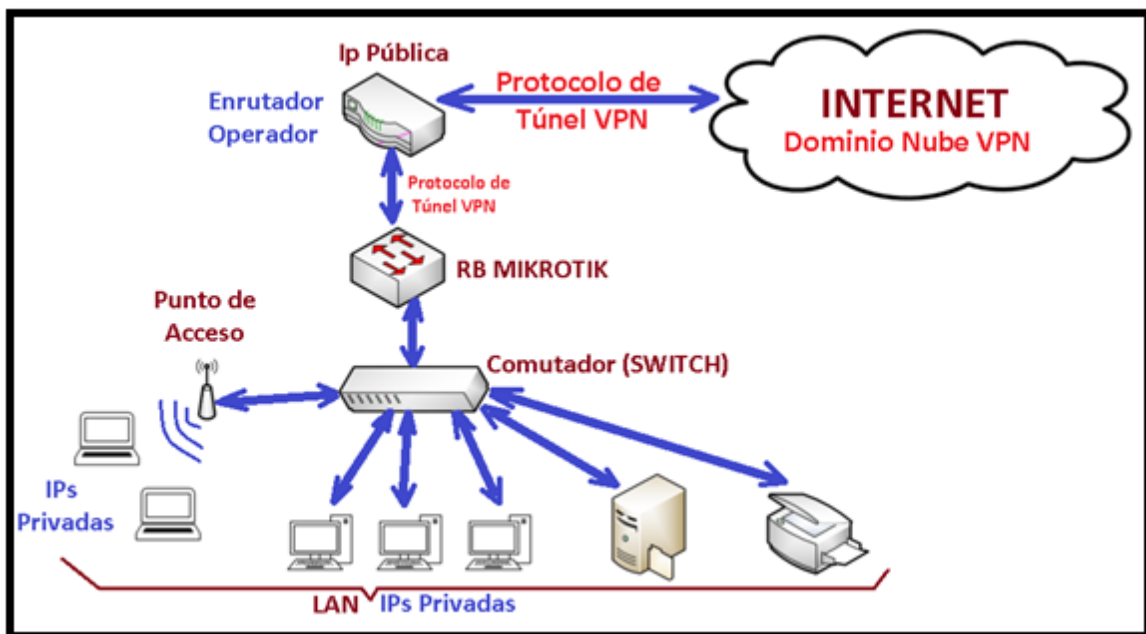


Figura 5: Topología de implementación VPN Básica en una Sede.

Fuente: Propia

Donde se ve que el enrutador Mikrotik, se encuentra en consecutivo del enrutador suministrado por el proveedor de Internet que la organización contrato, y siguiendo la topología se ve que todos los dispositivos de la Red Local (LAN) de la organización se encuentran bajo el enrutador Mikrotik, por lo tanto, cualquier dispositivo de la Red Local (LAN) deberá tener acceso a internet sin que se modifique su configuración particular de red, debido a que la implementación de la VPN será transparente para dichos dispositivos en la Red Local (LAN).

Iniciaremos la configuración del enrutador Mikrotik:

- a. Se utilizará Winbox, herramienta para la configuración de dispositivos Mikrotik, predeterminada por Mikrotik RouterBOARD.



Figura 6: Icono de Herramienta WINBOX

Fuente: Propia

- b. Se ejecuta la herramienta y seguidamente podremos ver el modo de acceso donde identificamos que equipos enrutador Mikrotik tenemos conectado, mediante su dirección MAC.

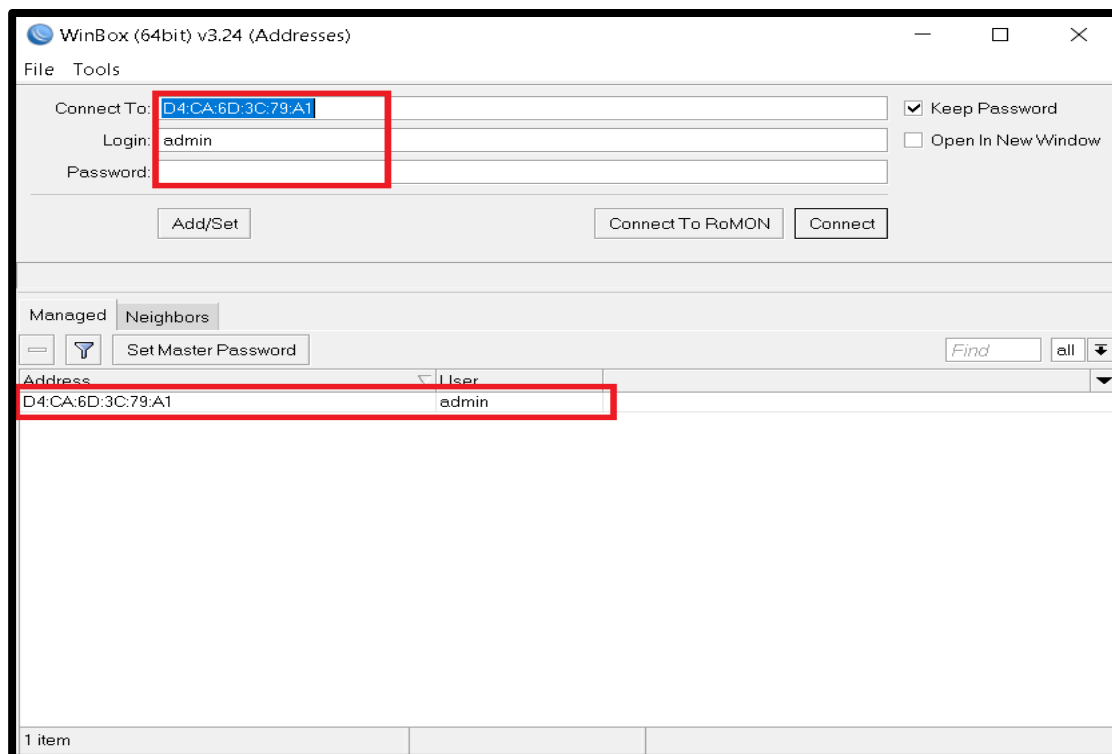


Figura 7: Ventana principal de Inicio WINBOX

Fuente: Propia

- c. Por defecto el enrutador Mikrotik no viene con contraseña de fábrica, la cual se podrá configurar a elección de la organización.
- d. Se procede a configurar el puerto *ethernet* donde se conectará la Red Local (LAN) de la Organización, en modo PUENTE (*BRIDGE*).

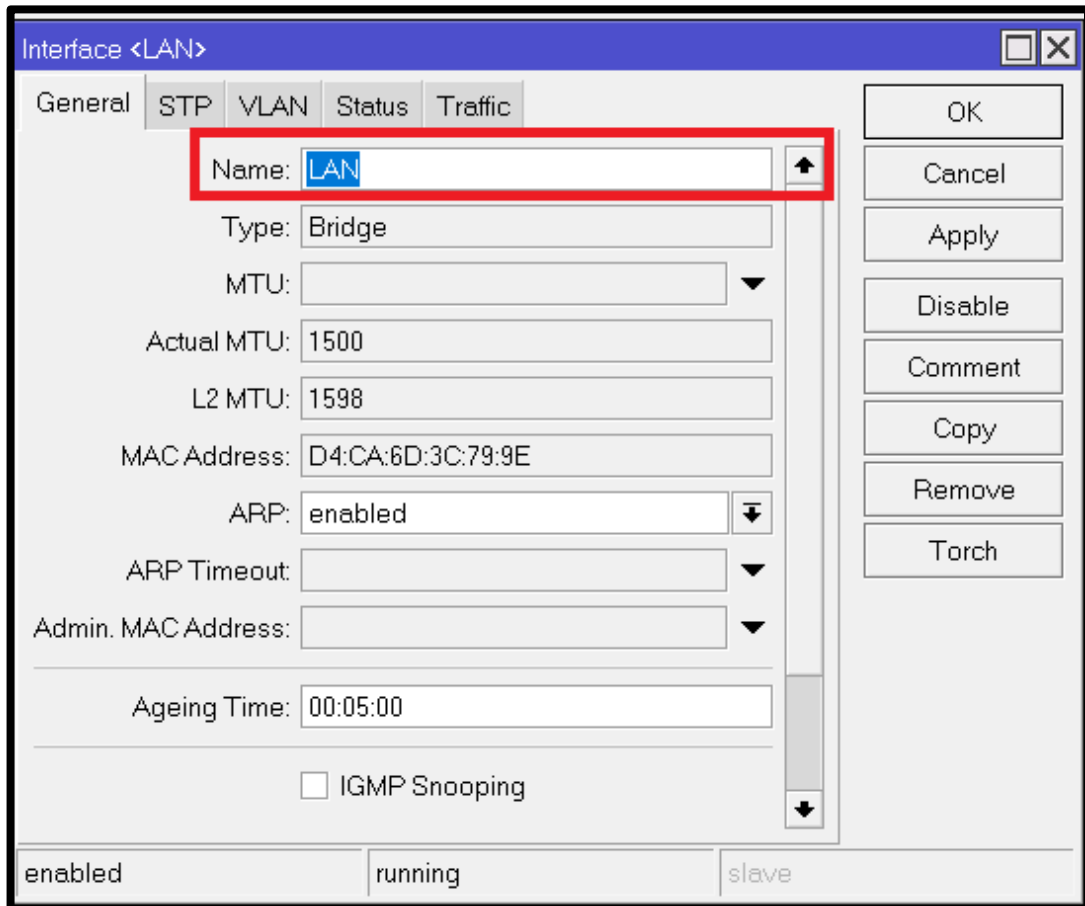


Figura 8: Ventana de configuración de nombre de interfaces - WINBOX

Fuente: Propia

- e. Se procede a configurar el puerto *ethernet* donde se conectará el *SWITCH* LAN en la Red Local (LAN) de la Organización.

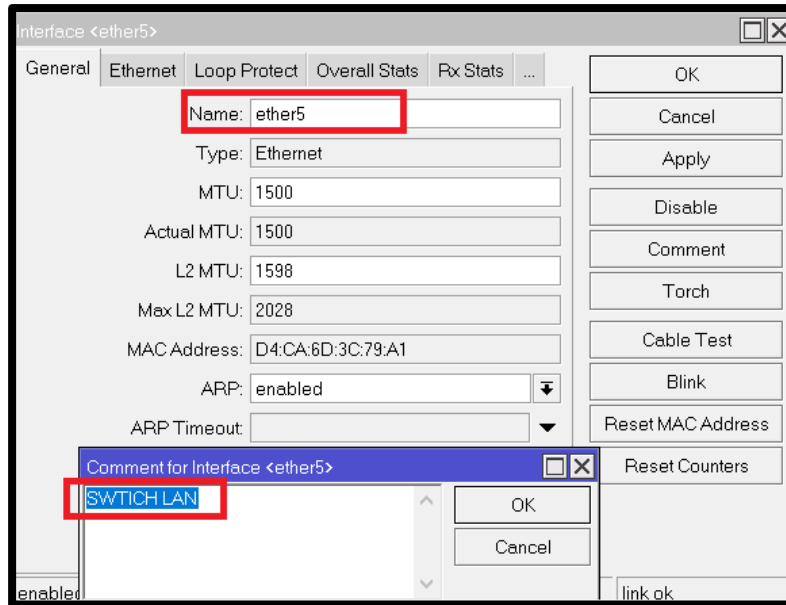


Figura 9: Ventana de configuración de nombre de interfaces - WINBOX

Fuente: Propia

- f. Se procede a configurar el puerto *ethernet* donde se conectará el Servidor de Archivos de la Organización (*FILE SERVER*), en la Red Local (LAN) de la Organización.

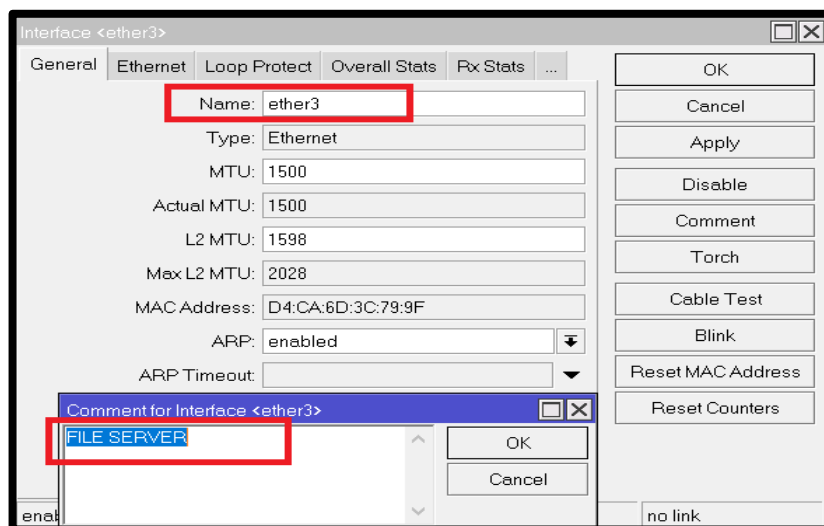


Figura 10: Ventana de configuración de nombre de interfaces - WINBOX

Fuente: Propia

g. Se procede a configurar el puerto *ethernet* donde se conectará la Red de Área Ampla (WAN) de la Organización.

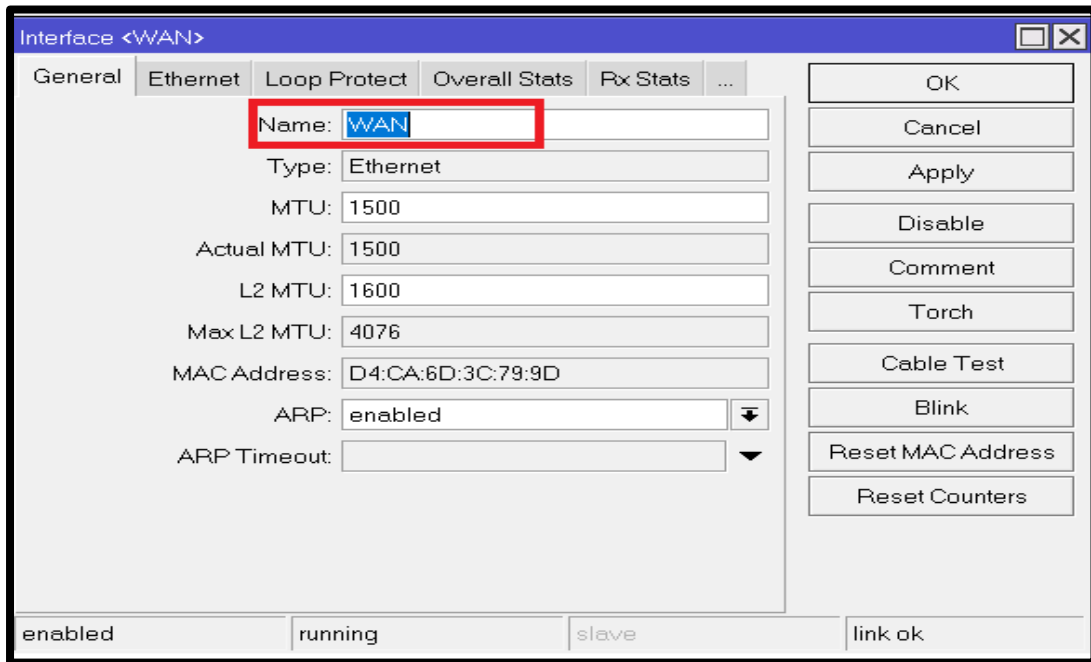


Figura 11: Ventana de configuración de nombre de interfaces - WINBOX

Fuente: Propia

h. La lista de interfaces queda entonces configurada de la siguiente forma:

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)
R	LAN	Bridge	1500	1598	720 bps	368 bps	
	ether1						
R	WAN	Ethernet	1500	1600	25.6 kbps	16.3 kbps	
\$	ether2	Ethernet	1500	1598	0 bps	0 bps	
	FILE SERVER						
\$	ether3	Ethernet	1500	1598	0 bps	0 bps	
\$	ether4	Ethernet	1500	1598	0 bps	0 bps	
	SWTICH LAN						
\$S	ether5	Ethernet	1500	1598	0 bps	0 bps	

Figura 12: Lista de interfaces - WINBOX

Fuente: Propia

i. Se procede a configurar la dirección IP en nuestro puerto LAN.

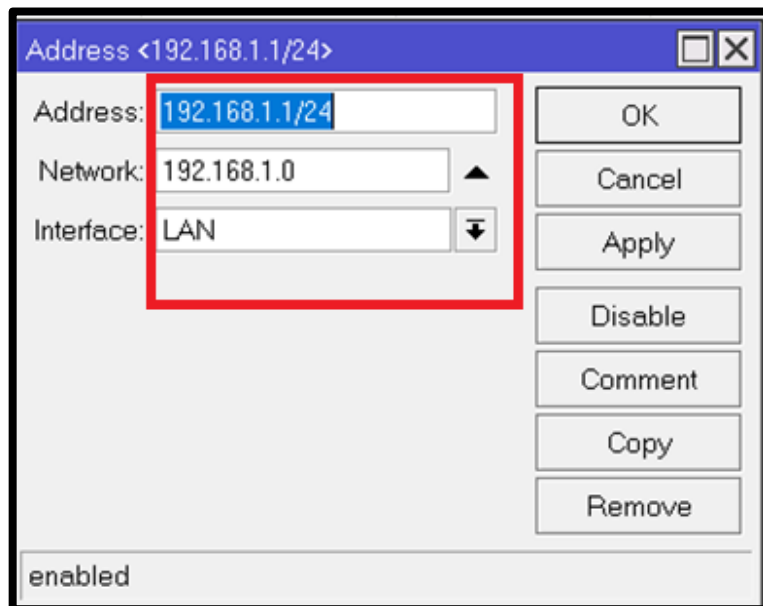


Figura 13: Configuración IP LAN - WINBOX

Fuente: Propia

j. Se procede a configurar la dirección IP en nuestro puerto WAN.

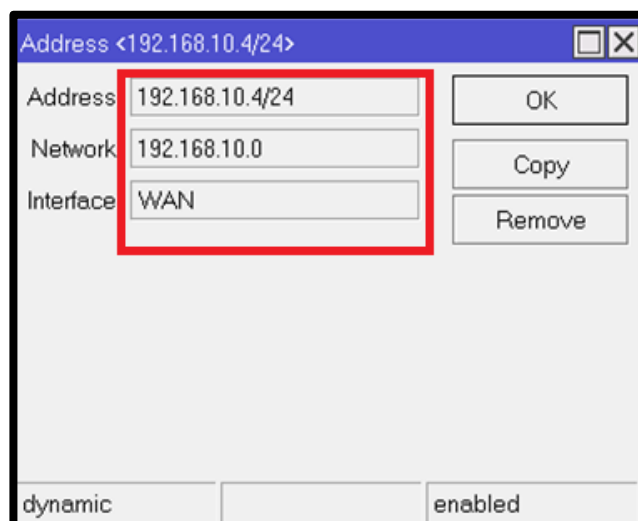
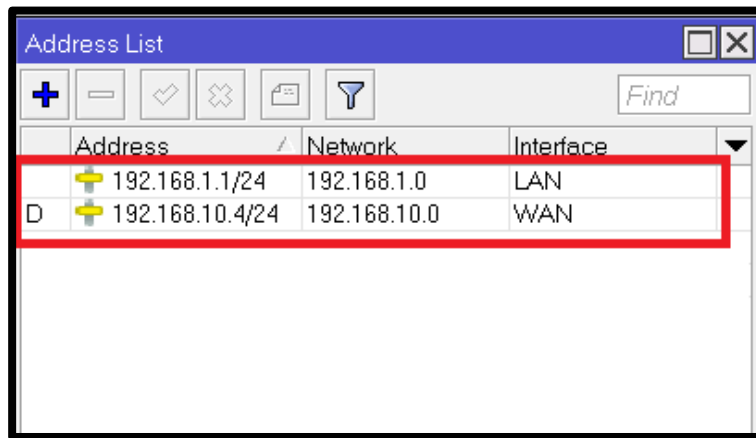


Figura 14: Configuración IP WAN - WINBOX

Fuente: Propia

- k. Después de configurar ambas direcciones IP, se valida que la lista de direcciones queda de la siguiente forma:

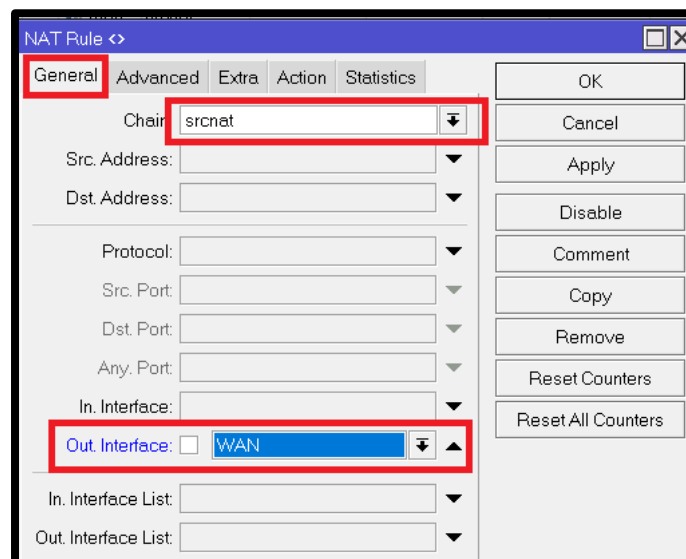


Address	Network	Interface
192.168.1.1/24	192.168.1.0	LAN
192.168.10.4/24	192.168.10.0	WAN

Figura 15: Lista de direcciones IPs - WINBOX

Fuente: Propia

- l. Se procede a enmascarar las direcciones IPs privadas de nuestra Red Local (LAN) orientada hacia la IP Pública del servicio de internet contratado por la organización, teniendo en consideración que “*Out Interface*” será la interfaz que se encuentra conectada al enrutador proporcionado por el proveedor de internet.



NAT Rule <>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

Any. Port: []

In. Interface: []

Out. Interface: WAN

In. Interface List: []

Out. Interface List: []

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Figura 16: Configuración de enmascaramiento para WAN- WINBOX

Fuente: Propia

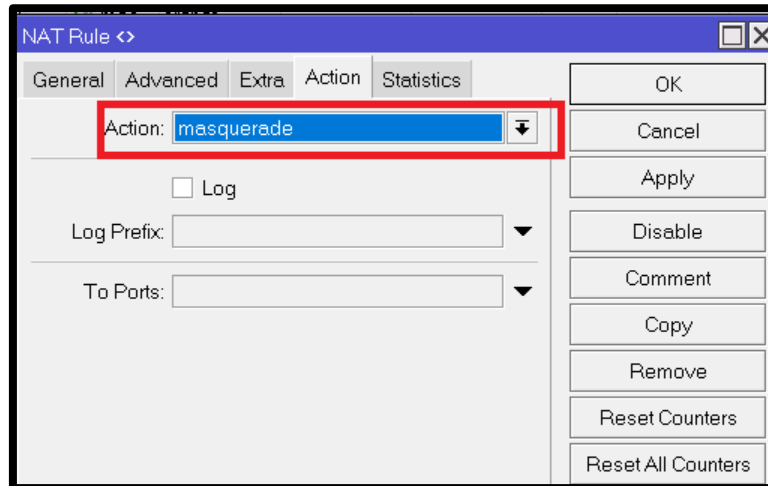


Figura 17: Enmascaramo WAN- WINBOX

Fuente: Propia

- m. Se procede a configurar la dirección IP del enrutador del proveedor de internet en la opción “GATEWAY”, para redirigir las peticiones de internet hacia la IP del mismo. Teniendo en cuenta que por defecto el enrutador Mikrotik crea rutas dinámicas en cada una de las redes configuradas

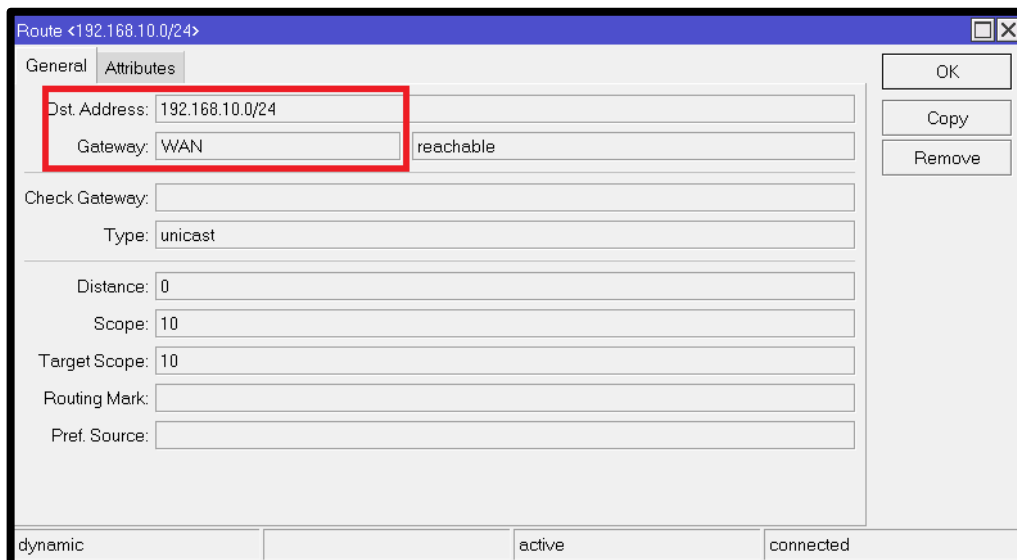
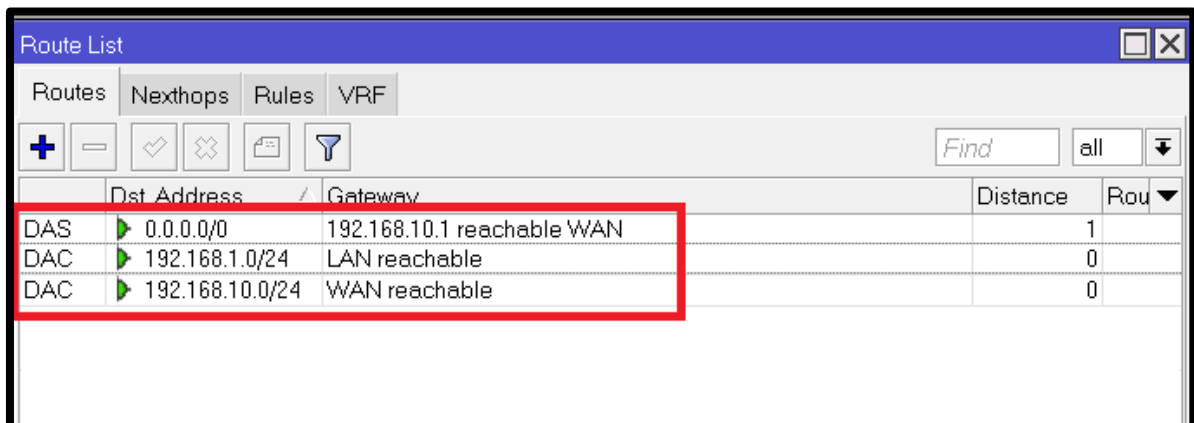


Figura 18: Configuración GATEWAY con la dirección IP de enrutador Proveedor – WINBOX

Fuente: Propia

n. Validamos que la lista de rutas (ROUTE LIST), queda de la siguiente forma:

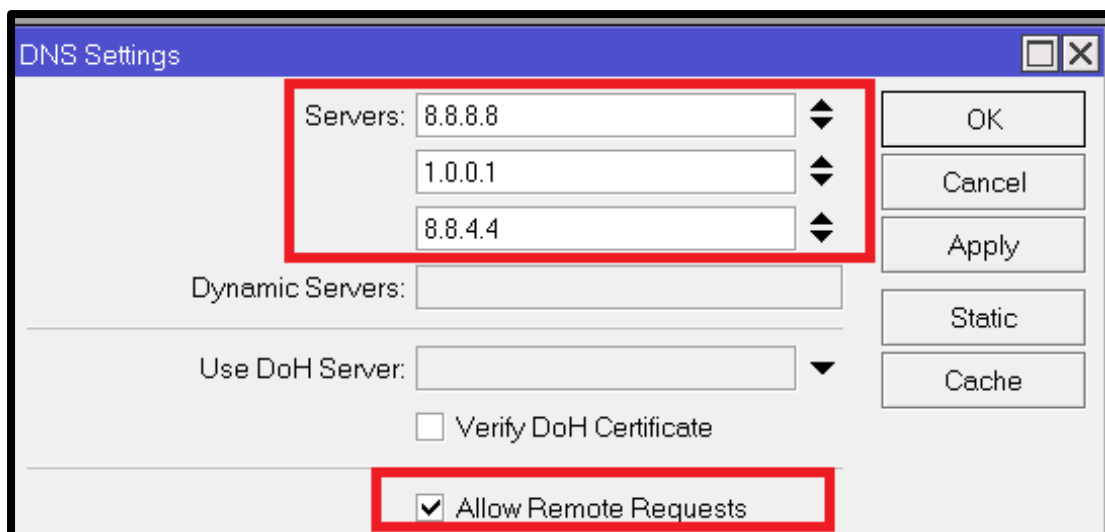


	Dist Address	Gateway	Distance	Rou
DAS	0.0.0.0/0	192.168.10.1 reachable WAN	1	
DAC	192.168.1.0/24	LAN reachable	0	
DAC	192.168.10.0/24	WAN reachable	0	

Figura 19: Lista de rutas - WINBOX

Fuente: Propia

o. Se procede a configurar los DNS.



DNS Settings

Servers: 8.8.8.8
1.0.0.1
8.8.4.4

Dynamic Servers:

Use DoH Server:

Verify DoH Certificate

Allow Remote Requests

OK
Cancel
Apply
Static
Cache

Figura 20: Configuración DNS - WINBOX

Fuente: Propia

2.3.3.2 Configuración de Red privada Virtual Mikrotik por tipo de VPN

Tenemos dos tipos de implementación VPN: Acceso Remoto y de Sitio a Sitio, para las cuales se podrán usar los tipos de protocolo:

- PPTP
- L2TP/IPsec

Los cuales proporcionan autenticidad de origen, integridad y protección de la confidencialidad de un paquete, en conjunto con el protocolo ESP que soporta configuraciones de un solo cifrado y autenticación. Estos protocolos se usarán dependiendo del requerimiento de la organización, además también se tendrá en cuenta si se desea usar su propia Ip Pública Estática del operador o decidirá optar por un Dominio Nube VPN.

Teniendo en cuenta los dos tipos de Red Privada Virtual (VPN) ya mencionados anteriormente se procede con la configuración VPN:

a. Configuración – Tipo VPN de Acceso Remoto:

i. Escenario: Ip Pública Estática - Protocolo PPTP

- Ingresamos a la opción PPP, hacemos click en la opción PPTP Server, hacemos click en “Enabled”, y activamos las 4 casillas de *mschap2*, *mschap1*, *chap* y *pap*.

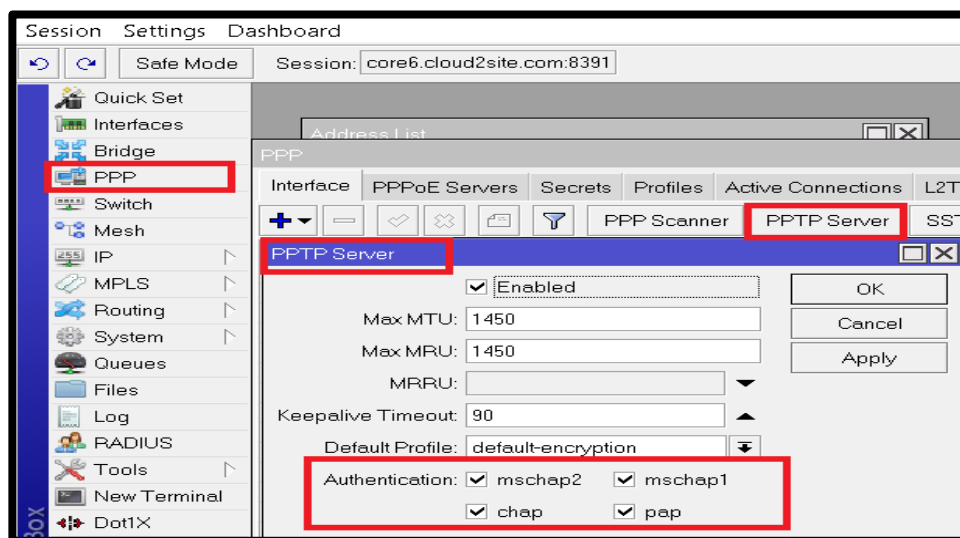


Figura 21: Configuración PPP - WINBOX

Fuente: Propia

- Visualización de configuración PPP.

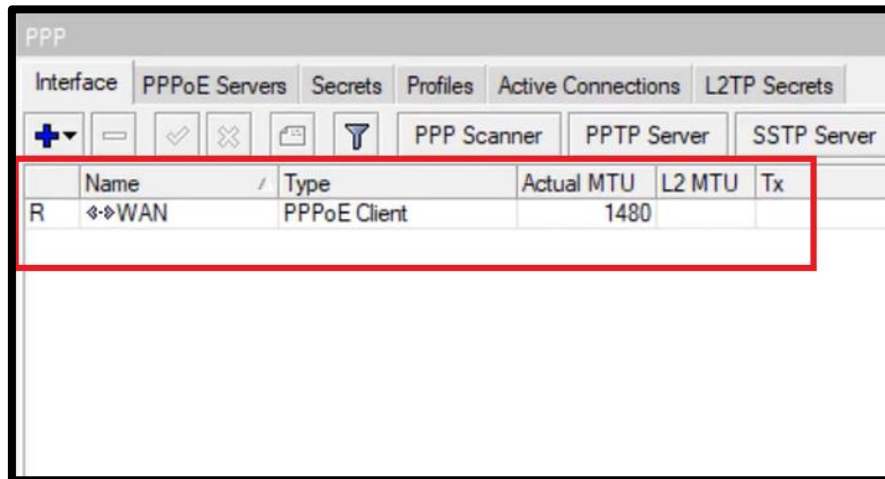


Figura 22: Configuración PPP - WINBOX

Fuente: Propia

- Configurando el IP Pool para la VPN, hacemos clic en IP, después en Pool, seguidamente etiquetamos el nombre de pool que deseamos y el rango de IPs de dicho pool.

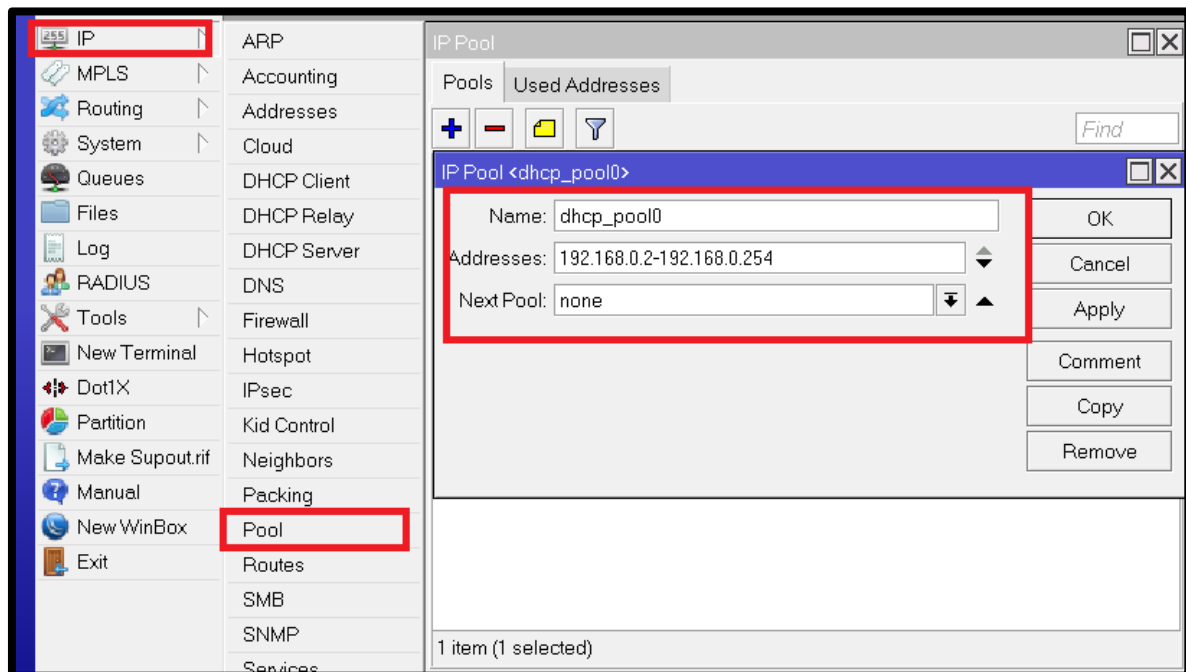


Figura 23: Configuración IP Pool VPN - WINBOX

Fuente: Propia

- Visualización de configuración Ip Pool VPN:

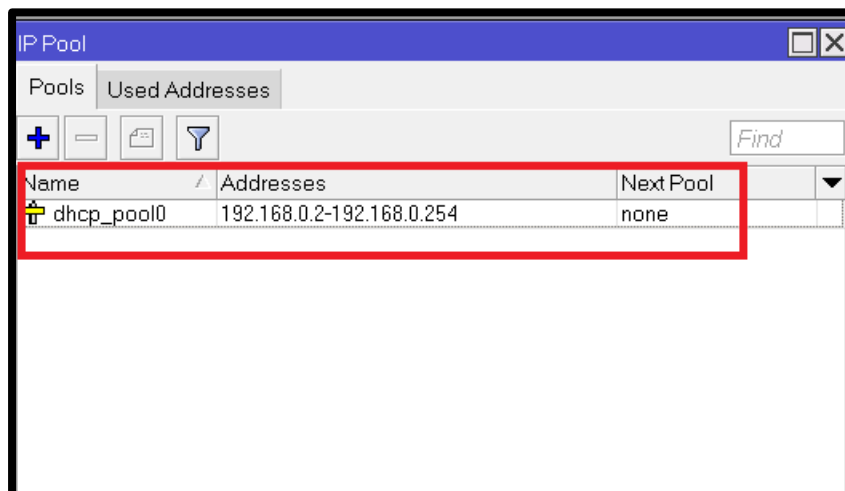


Figura 24: Configuración IP Pool VPN - WINBOX

Fuente: Propia

- Tomamos en cuenta la dirección IP de la Red Local (LAN).

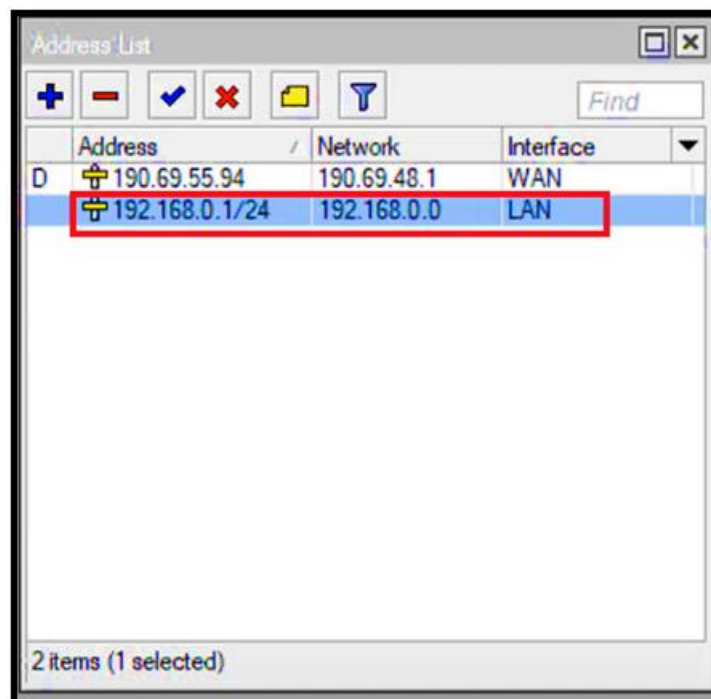


Figura 25: Lista de direcciones IP LAN / WAN - WINBOX

Fuente: Propia

- Configuramos el Perfil VPN en la pestaña PPP, teniendo como observación que la dirección local, es la misma dirección ip de la interfaz LAN.

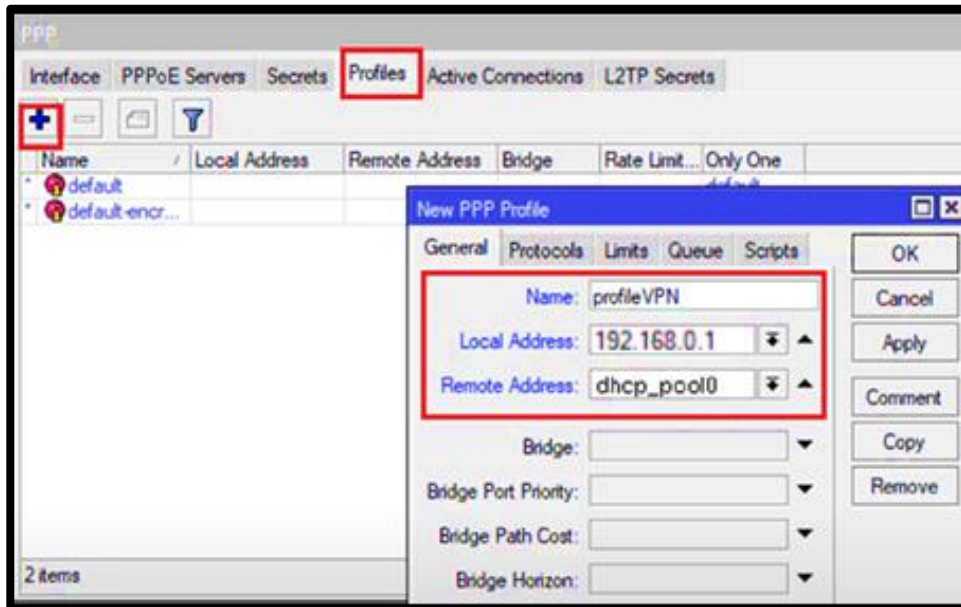


Figura 26: Perfil PPP - WINBOX

Fuente: Propia

- Seleccionamos en la pestaña de protocolos, compresión y encriptación.

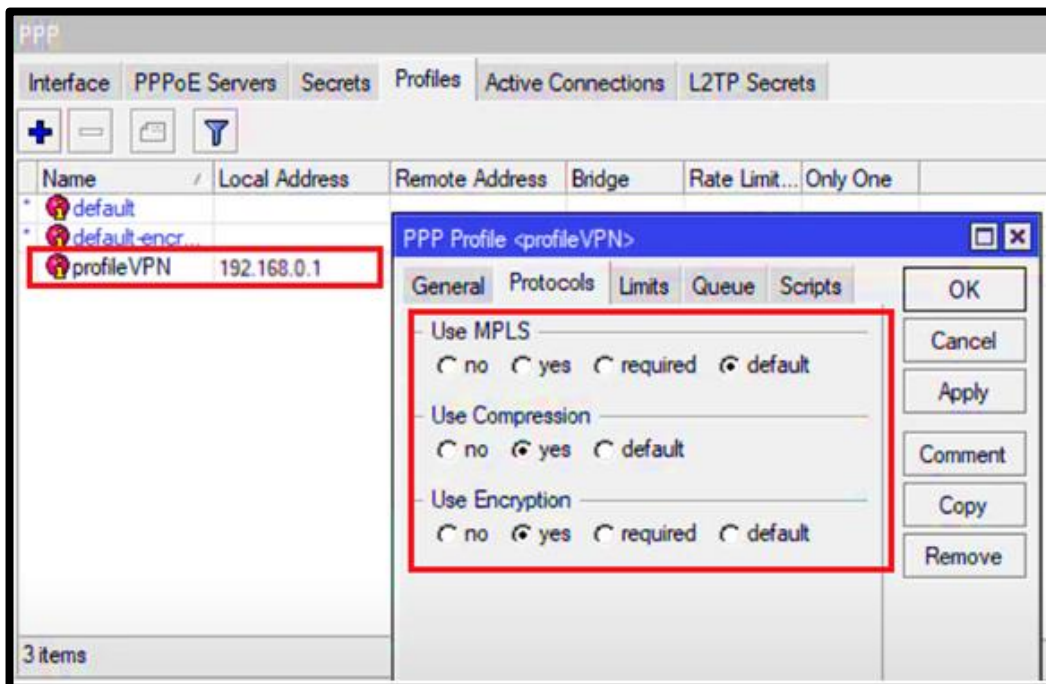


Figura 27: Perfil PPP – Pestaña Protocolos - WINBOX

Fuente: Propia

- Seleccionamos la pestaña “Secrets”, y colocamos el usuario, tipo de servicio y el perfil asignado.

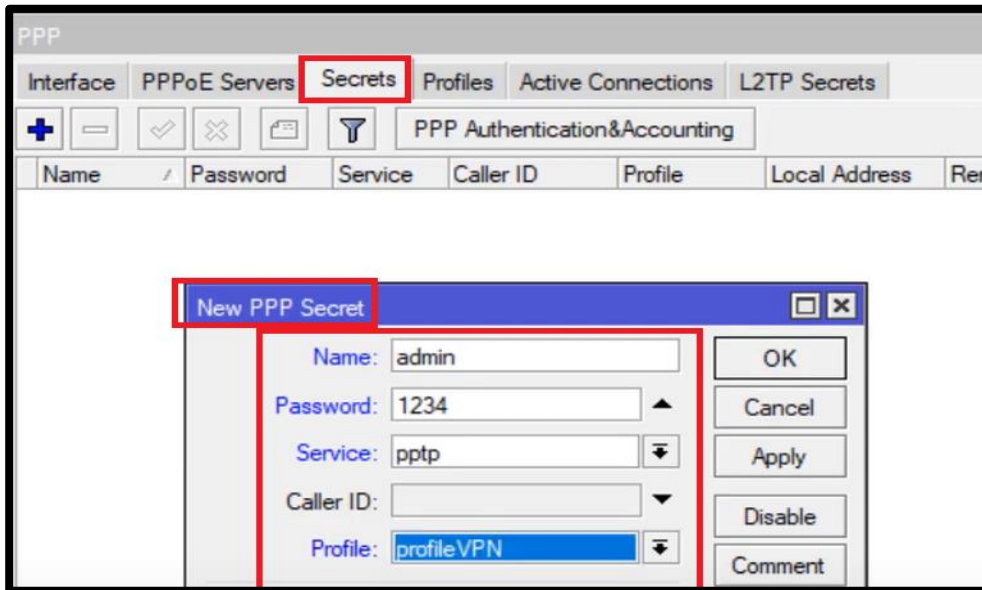


Figura 28: Perfil PPP - Pestaña “Secrets” - WINBOX

Fuente: Propia

- Visualización final de la pestaña “Secrets”

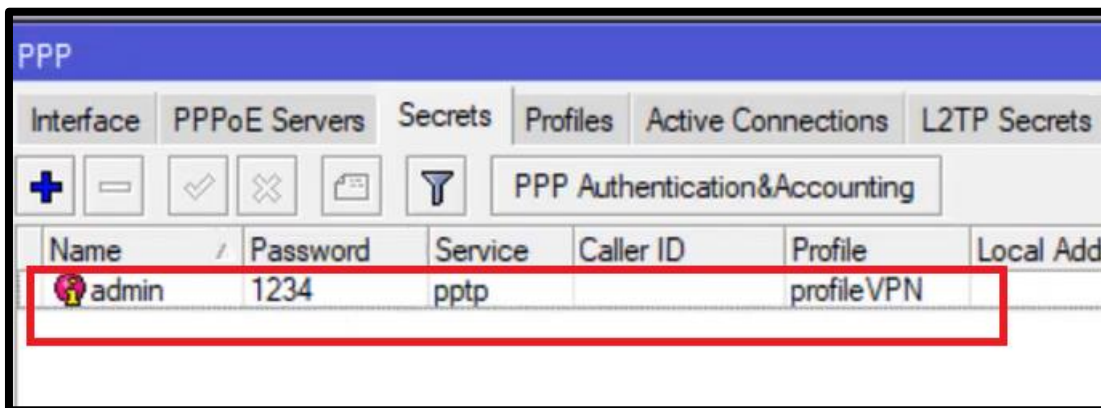


Figura 29: Perfil PPP - Pestaña “Secrets” - WINBOX

Fuente: Propia

ii. Escenario: Ip pública Estática – Protocolo L2TP/IPsec

- Ingresamos a la opción PPP dentro de la pestaña “*Interface*”, hacemos clic en la opción L2TP Server, click en “*Enabled*”, y activamos las 2 casillas de *mschap2*, *mschap1*. Seguidamente activamos “*Use IPsec*” y colocamos una contraseña en “*IPsec Secret*”.

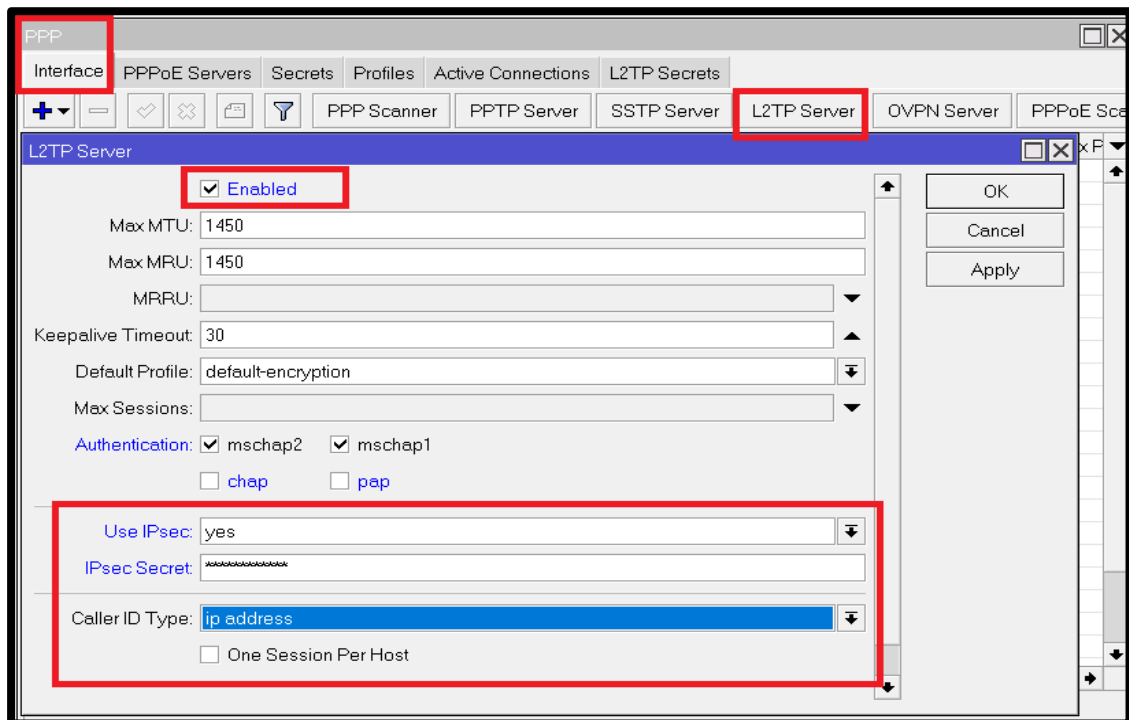


Figura 30: Pestaña “*L2TP Server*” - WINBOX

Fuente: Propia

- Seleccionamos la pestaña “*Secrets*”, y colocamos el usuario, tipo de servicio l2tp, en este caso perfil por defecto, además se utiliza un rango de IP que no coincidan con el rango de las IP de los dispositivos que se interconectan tanto en el origen como en el destino.

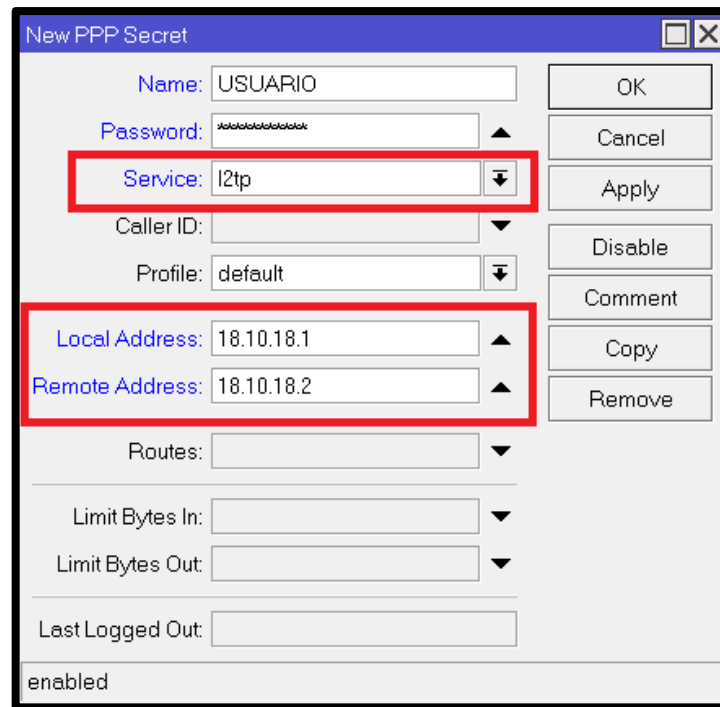


Figura 31: Pestaña “New PPP Secret” - WINBOX

Fuente: Propia

- Visualización final de configuración de la pestaña “Secrets” para L2TP.

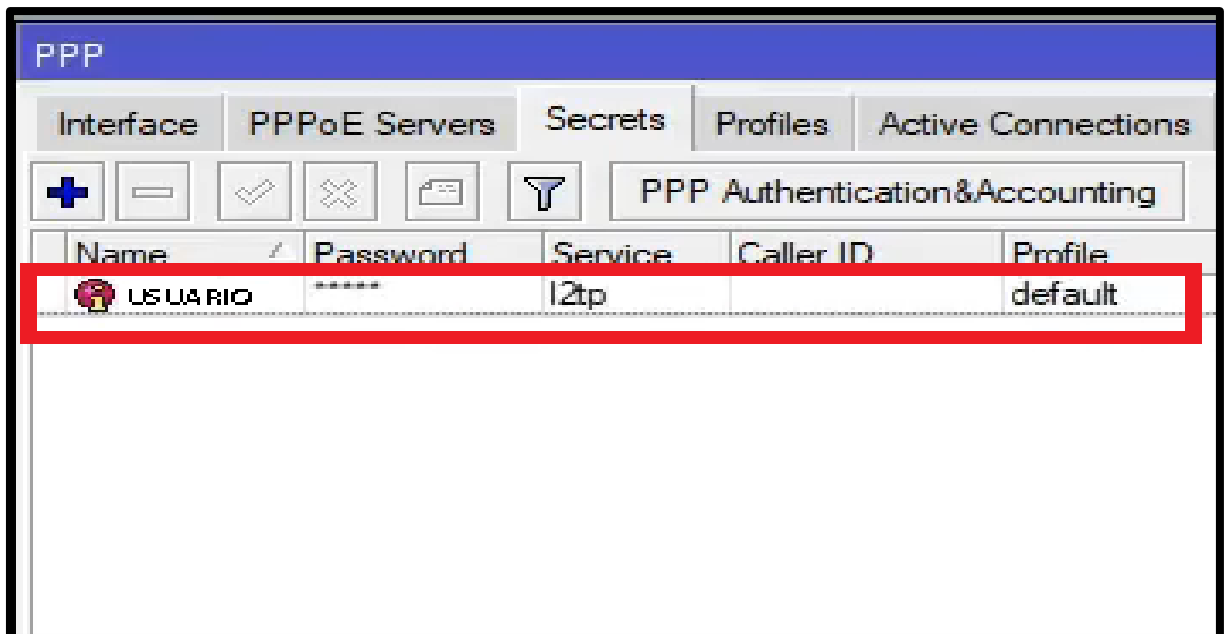


Figura 32: Pestaña “New PPP Secret” - WINBOX

Fuente: Propia

- Se habilita la siguiente regla en el cortafuego (*Firewall*), dando permiso a todas las entradas del protocolo UDP, a los puertos 500, 1701 y 4500.

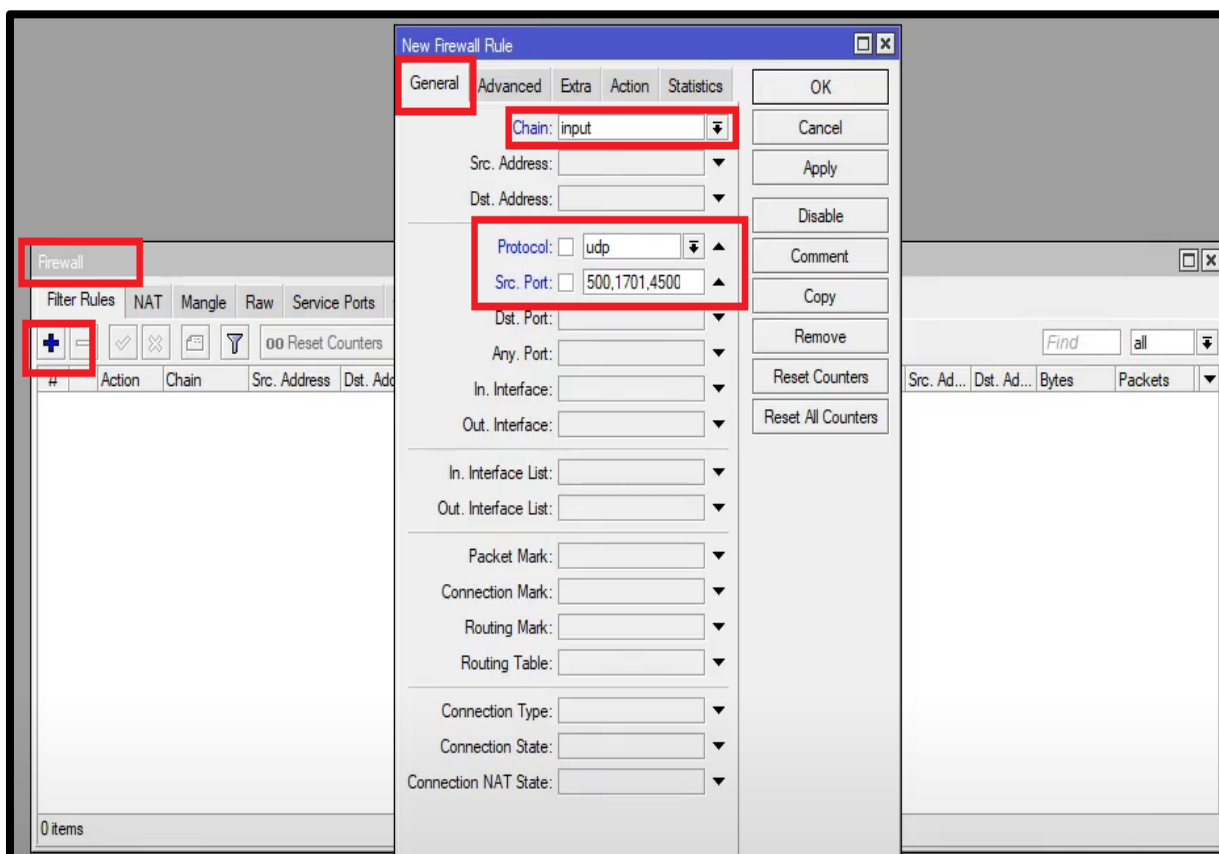


Figura 33: Pestaña “*New Firewall Rule* “- Protocolo UDP - WINBOX

Fuente: Propia

- Se habilita la siguiente regla en el cortafuego (*Firewall*), dando permiso a todas las entradas que vayan al protocolo IPsec-esp.

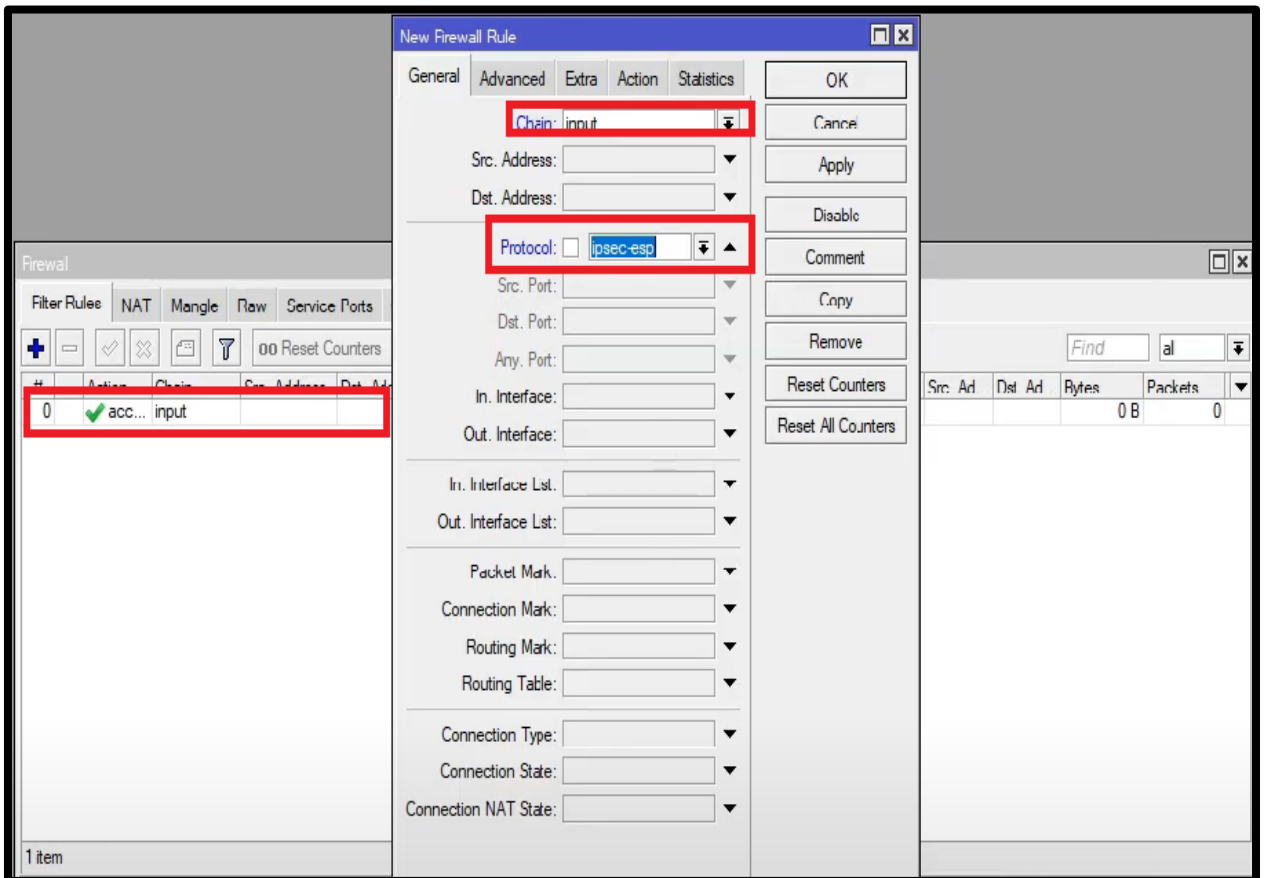


Figura 34: Pestaña “New Firewall Rule - Protocol IPsec” - WINBOX

Fuente: Propia

- Para terminar de aceptar los protocolos habilitados en ambos casos se procede aplicando y aceptando según lo indicado.

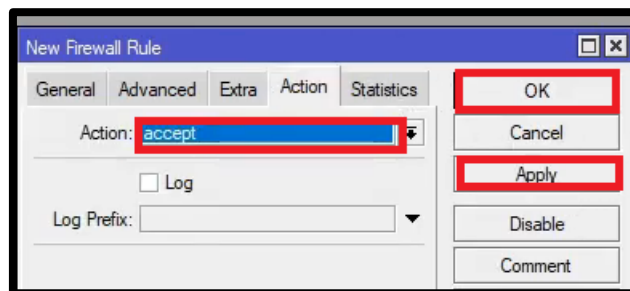


Figura 35: Aplicando protocolos - WINBOX

Fuente: Propia

- Visualización final de reglas configuradas en el cortafuego (*Firewall*)

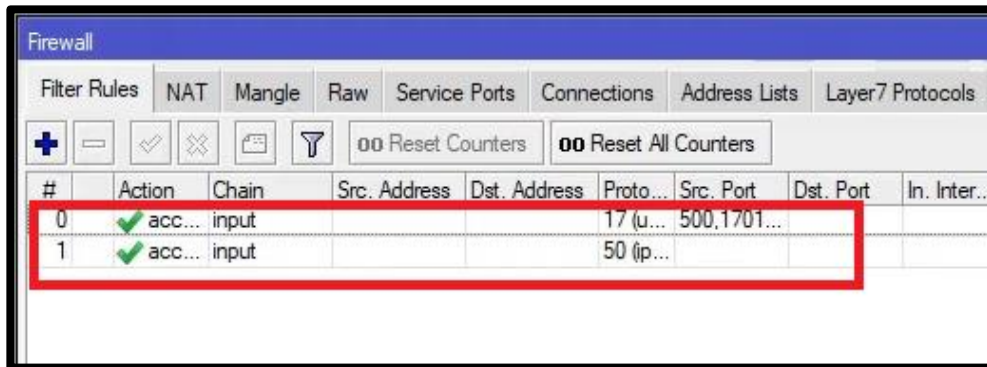


Figura 36: Reglas en Pestaña Cortafuego (*Firewall*) - WINBOX

Fuente: Propia

b. Configuración – Tipo VPN de Sitio a Sitio:

i. Escenario: Ip Pública Estática - Protocolo PPTP

- **RB Mikrotik – Sede Principal – PPP**

❖ Ingresamos en el primer enrutador RB Mikrotik utilizando la consola de WINBOX y nos dirigimos a la opción IP – *Adresses*, donde agregamos la Ip Pública de la sede secundaria y a su vez visualizamos la Ip Privada de la Red Local (LAN) de la Sede Principal.

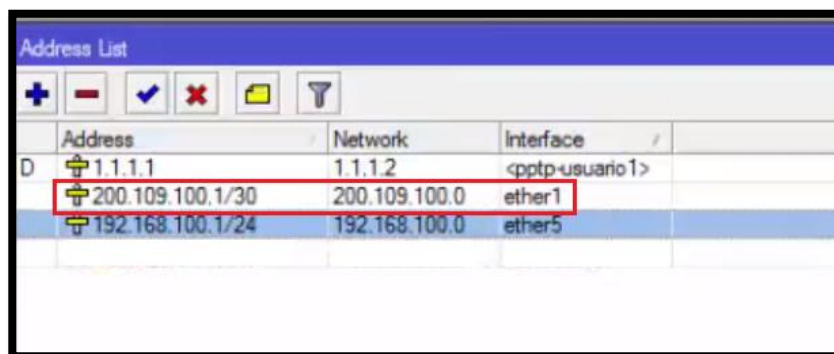


Figura 37: Lista de dirección que incluye Ip Pública de sede secundaria - WINBOX

Fuente: Propia

- ❖ Se configura una ruta por defecto que contenga la Ip Pública de la sede secundaria.

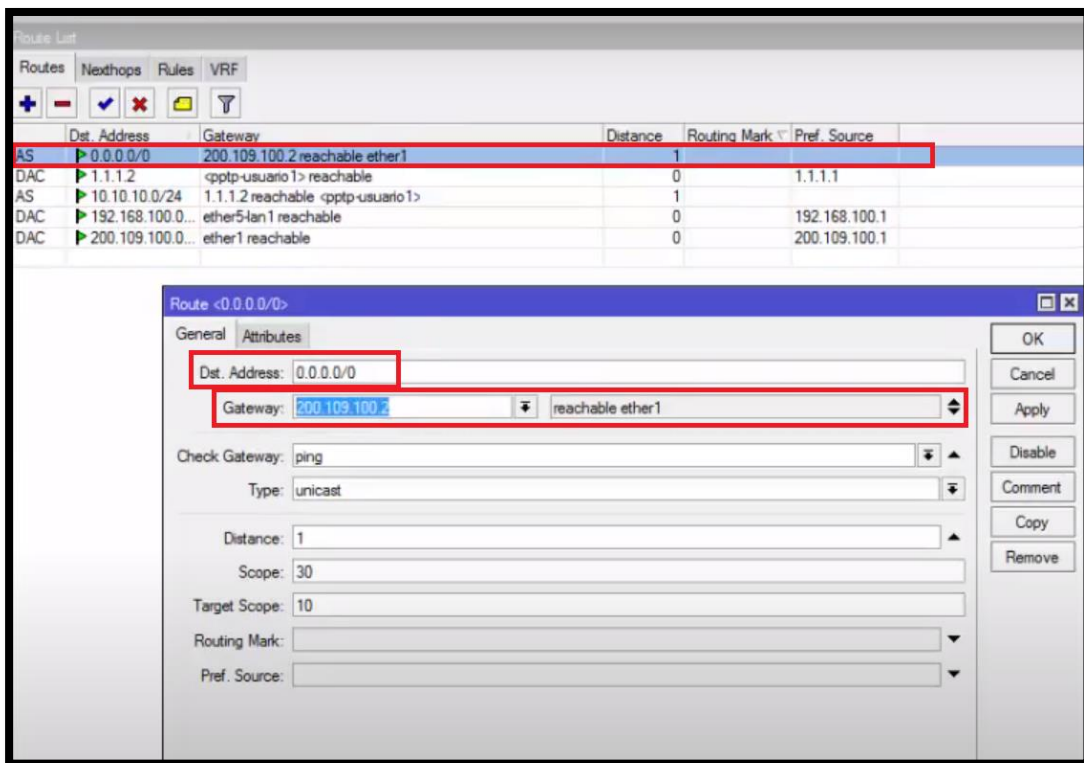


Figura 38: Lista de rutas que incluye Ip Pública de sede secundaria - WINBOX

Fuente: Propia

- ❖ Luego se procede habilitar el servicio en la opción PPP, dentro de la pestaña “Interface – PPTP Server”.

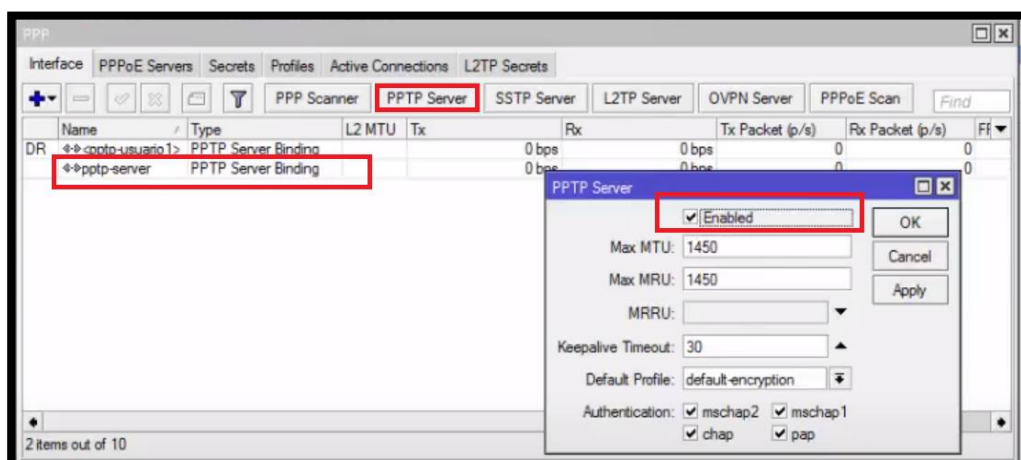


Figura 39: Pestaña PPP donde se habilita el “PPTP Server” - WINBOX

Fuente: Propia

❖ Luego se procede habilitar “*PPTP Server Binding*”

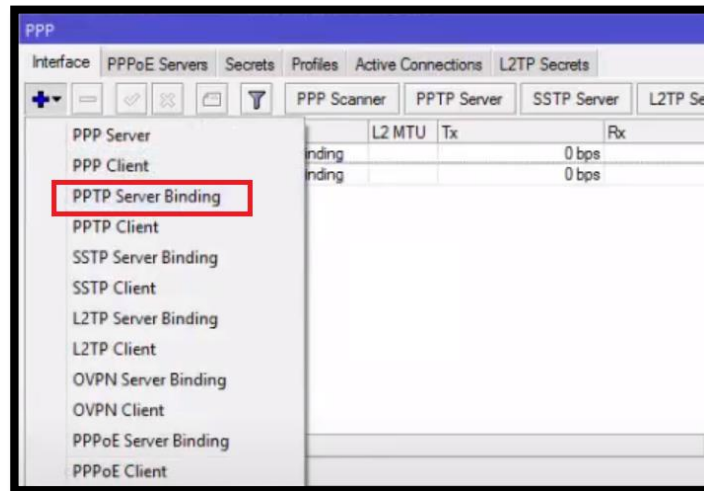


Figura 40: Pestaña PPP donde se habilita el “*PPTP Server Binding*” - WINBOX

Fuente: Propia

❖ Donde se coloca un nombre, ejemplo: “*pptp-server*” al servicio habilitado.

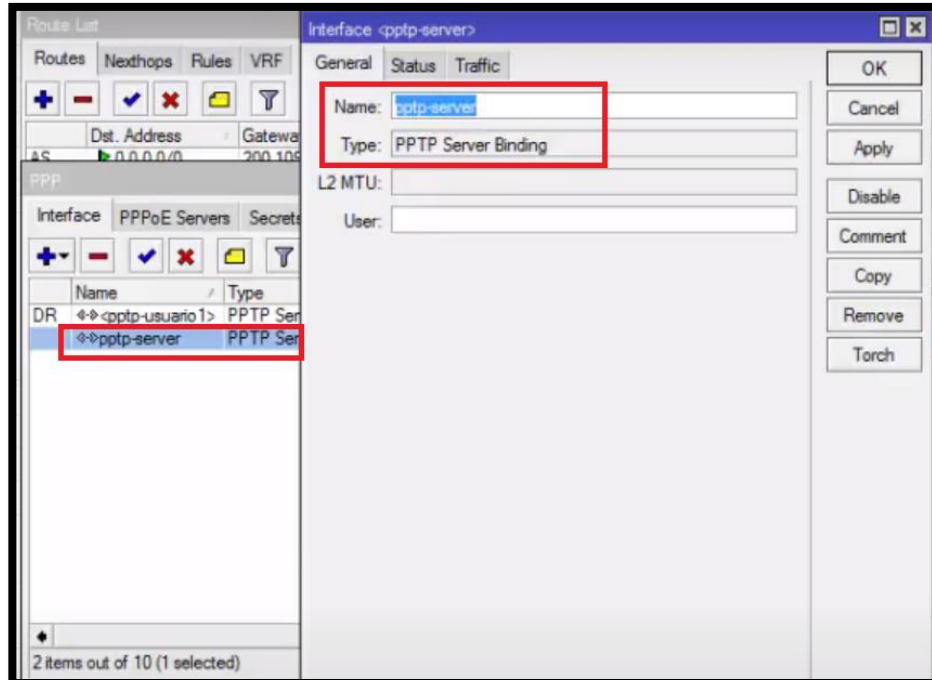


Figura 41: Pestaña PPP donde se coloca el nombre del servicio habilitado – WINBOX

Fuente: Propia

- ❖ Ahora se configuran dos direcciones estáticas que comunicaran los dos puntos del túnel VPN de Sitio a Sitio, dentro de la pestaña “*Profiles*” de PPP.

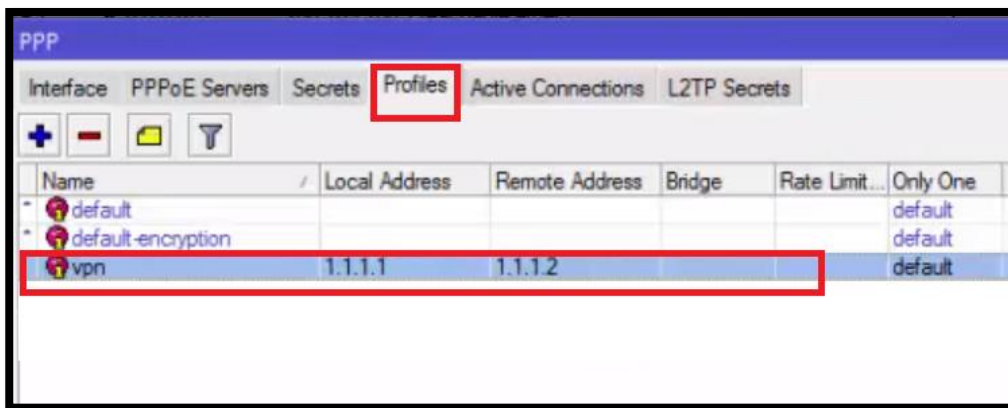


Figura 42: Pestaña “*Profiles*” donde se configuran IP Estática de punto a punto – WINBOX

Fuente: Propia

- ❖ Donde la configuración de perfil, se dará de la siguiente forma, tomando Ip Estática de punto a punto.

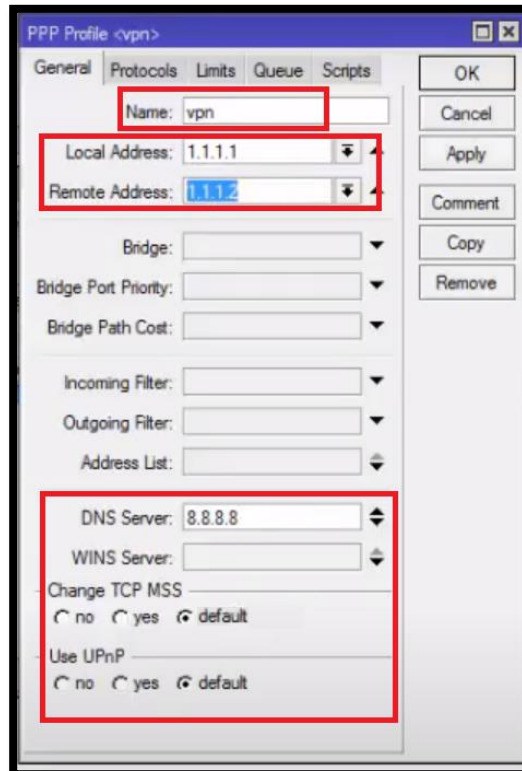


Figura 43: Configuración de perfil - Ip Estática de punto a punto – WINBOX

Fuente: Propia

- ❖ Después procedemos en crear un usuario de acceso en el túnel PPTP, dentro del apartado “Secrets”.

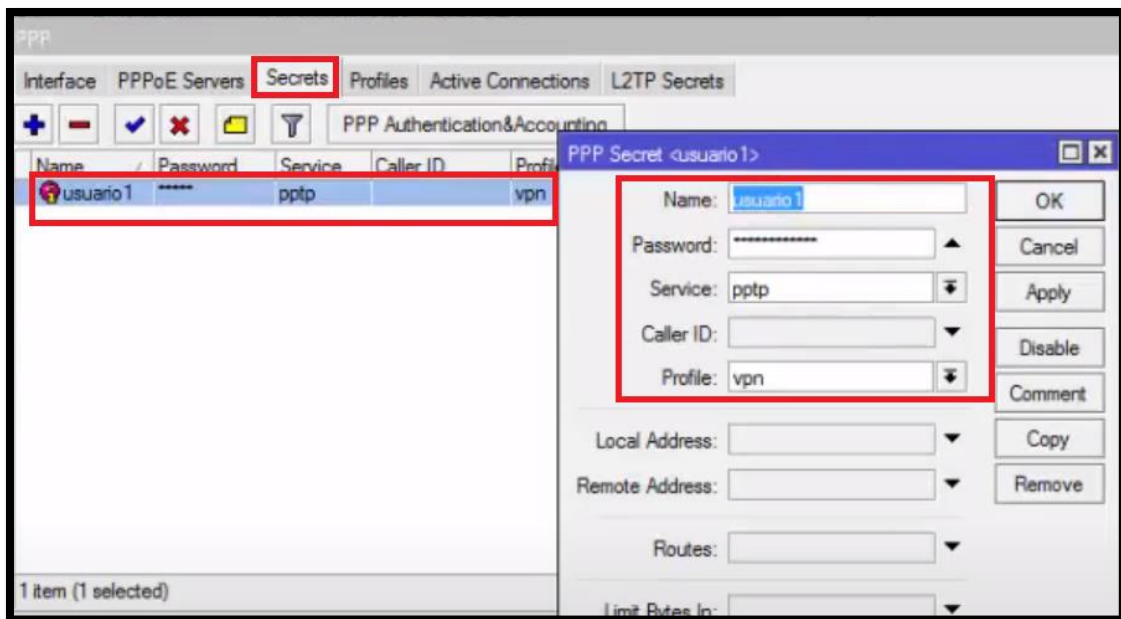


Figura 44: Configuración usuario de acceso en el túnel PPTP - WINBOX

Fuente: Propia

- ❖ Seguidamente vamos al apartado de “Firewall” y aceptamos el puerto mediante el cual se conecta el servicio PPTP – Protocolo TCP.

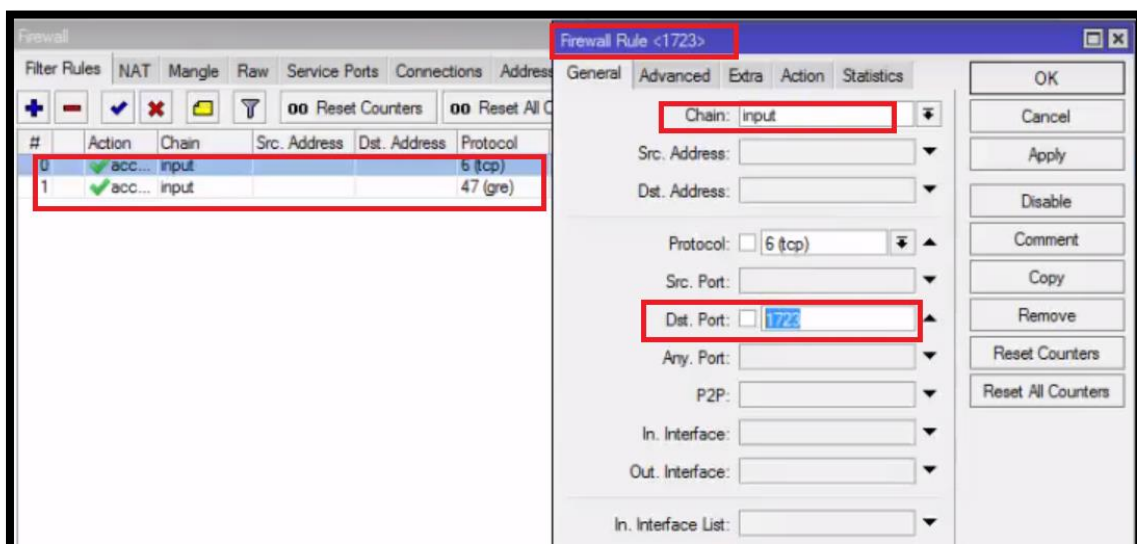


Figura 45: Firewall, puerto de conexión del servicio PPTP - Protocolo TCP – WINBOX

Fuente: Propia

- ❖ Seguidamente vamos al apartado de “*Firewall*” y aceptamos el puerto mediante el cual se conecta el servicio PPTP – Protocolo GRE.

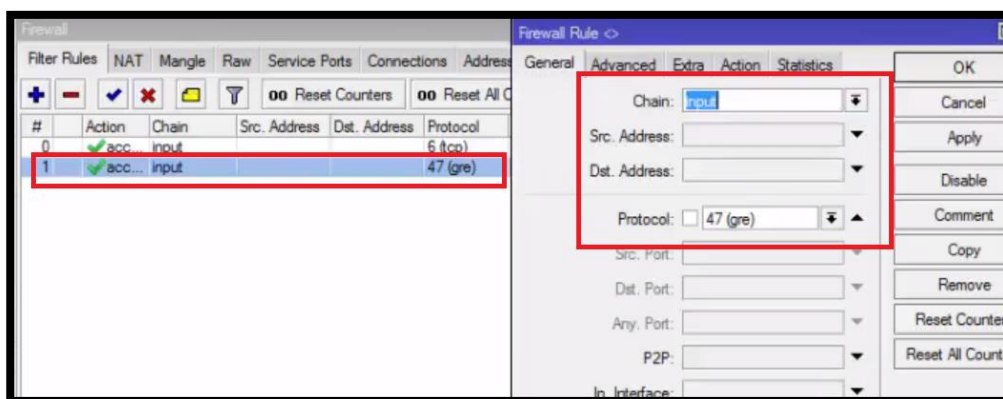


Figura 46: “*Firewall*”, puerto de conexión del servicio PPTP - Protocolo GRE – WINBOX

Fuente: Propia

- ❖ Creamos una ruta estática dirigida a la red interna de la sede secundaria, en este caso como ejemplo 10.10.10.0/24, esto para que cuando un equipo de la sede principal desee hacer una consulta a un equipo de la sede secundaria, dicha consulta se realice por el túnel VPN con su seguridad de cifrado respectivo.

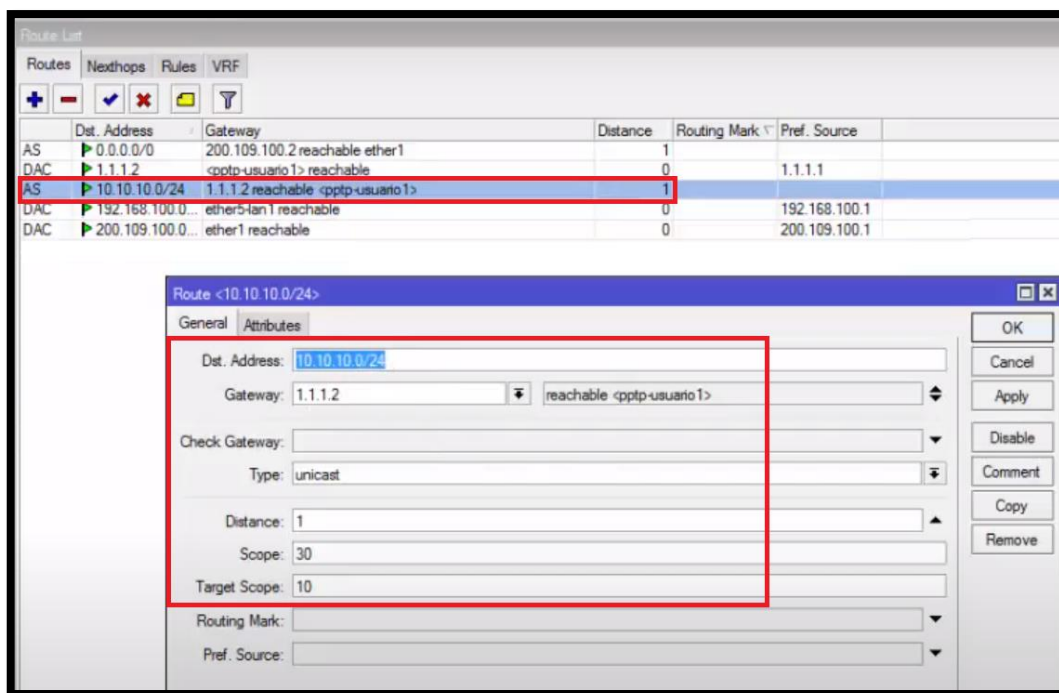


Figura 47: Lista de rutas – agregando ruta de Sede Secundaria - WINBOX

Fuente: Propia

- **RB Mikrotik – Sede Secundaria - PPP**

❖ Se configura la lista de direcciones, empezando por la IP que está conectada directamente a la Sede Principal en el servidor PPTP (200.109.100.2), y la dirección IP de la interfaz que está conectada a la Red Local (LAN), de la Sede Secundaria (10.10.10.1). Además, teniendo en cuenta que la primera dirección IP, es una dirección dinámica que aparece al conectarse al servidor PPTP (1.1.1.2).

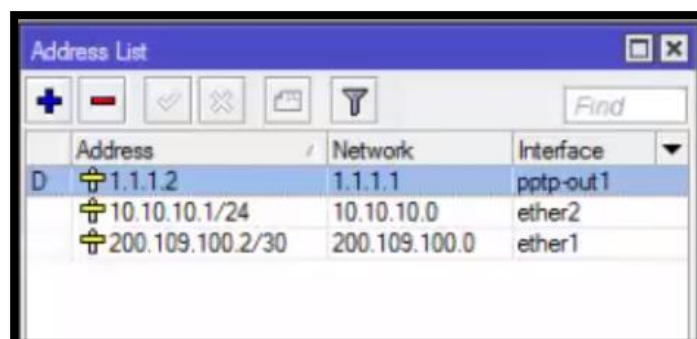


Figura 48: Lista de direcciones de la Sede Secundaria – WINBOX

Fuente: Propia

- ❖ Se configura la lista de rutas de igual forma que se configuro en la Sede Principal teniendo en cuenta la puerta de enlace de las misma para el ejemplo (1.1.1.1).

	Dist. Address	Gateway	Distance	Routing
AS	0.0.0.0/0	200.109.100.1 reachable ether1	1	
DAC	1.1.1.1	pptp-out1 reachable	0	
DAC	10.10.10.0/24	ether2 reachable	0	
AS	192.168.100.0/24	1.1.1.1 reachable pptp-out 1	1	
DAC	200.109.100.0/30	ether1 reachable	0	

Figura 49: Lista de rutas de la Sede Secundaria - WINBOX

Fuente: Propia

- ❖ Se configura el cliente PPTP dentro de la pestaña PPP y escogemos PPTP Cliente.

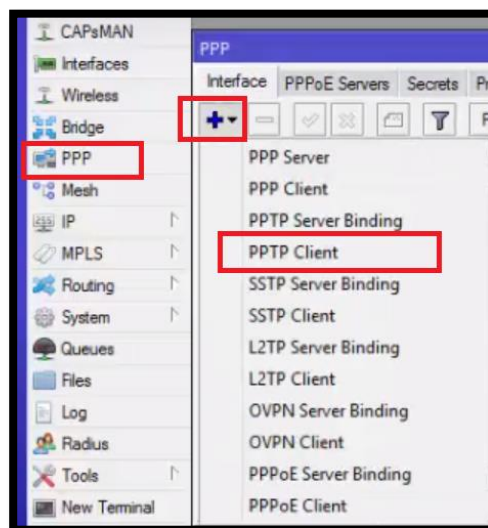


Figura 50: Pestaña PPP – *Interface* – PPTP *Client* - WINBOX

Fuente: Propia

- ❖ En la pestaña “*Dial Out*” colocamos la siguiente configuración, teniendo en cuenta la dirección IP de la Sede Principal, como el usuario y contraseña que se desea colocar.

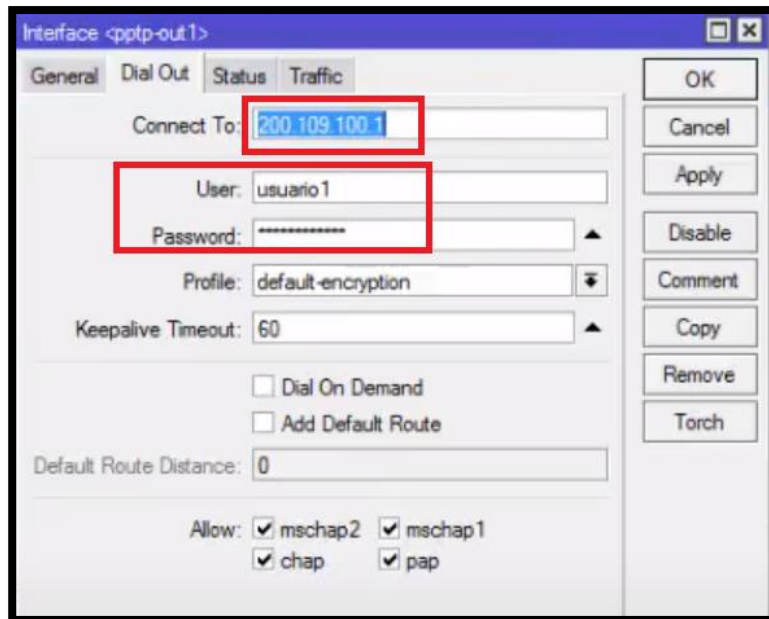


Figura 51: Pestaña “Dial Out” – Sede Secundaria - WINBOX

Fuente: Propia

- ❖ En la pestaña “General” colocamos el nombre correspondiente o si desea se deja por defecto.

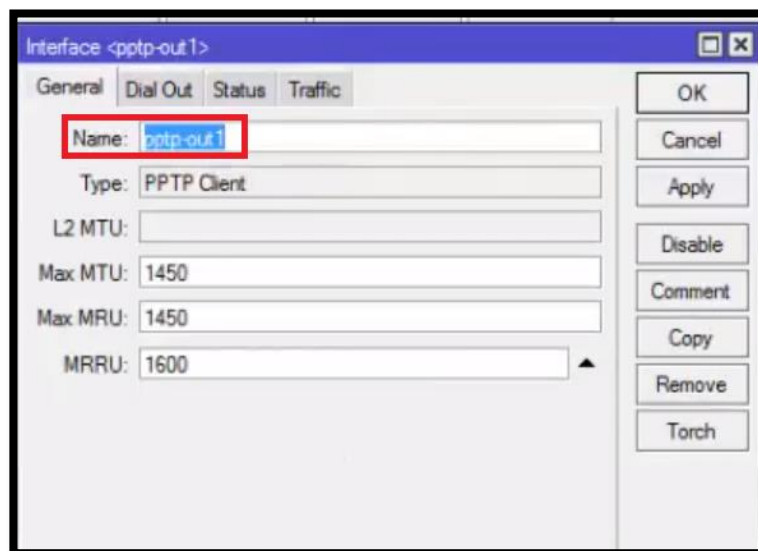


Figura 52: Pestaña “General” – Sede Secundaria - WINBOX

Fuente: Propia

- ❖ Después de lo realizado en el cuadro de PPP, debe aparecer una “R” indicando que el servicio está conectado.

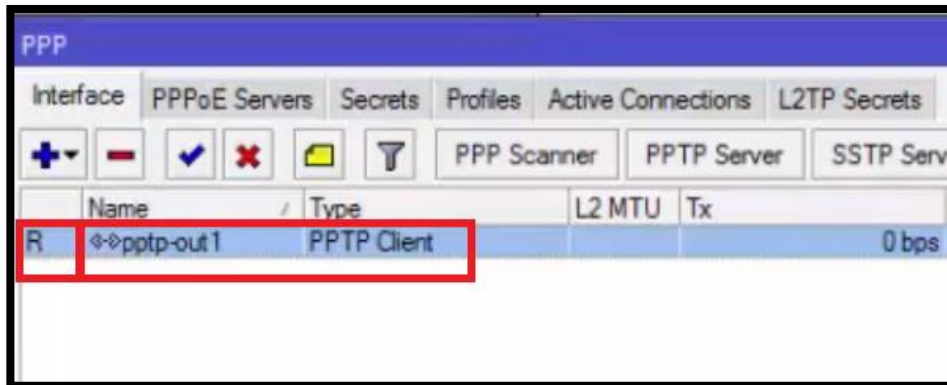


Figura 53: Configuración PPTP en la pestaña PPP de la Sede Secundaria - WINBOX

Fuente: Propia

ii. Escenario: Ip Pública Estática - Protocolo L2TP/IPsec

Para esta configuración se tomará en cuenta el procedimiento realizado en el “Escenario Ip Publica – Protocolo PPTP”, cambiando solo los indicados a continuación:

- **RB Mikrotik – Sede Principal - L2TP/IPsec**

- ❖ En la pestaña PPP, para el apartado “L2TP Server” se configura lo siguiente, teniendo en cuenta que se debe habilitar la opción “Use IPsec” y colocar una contraseña respectiva para el mismo.

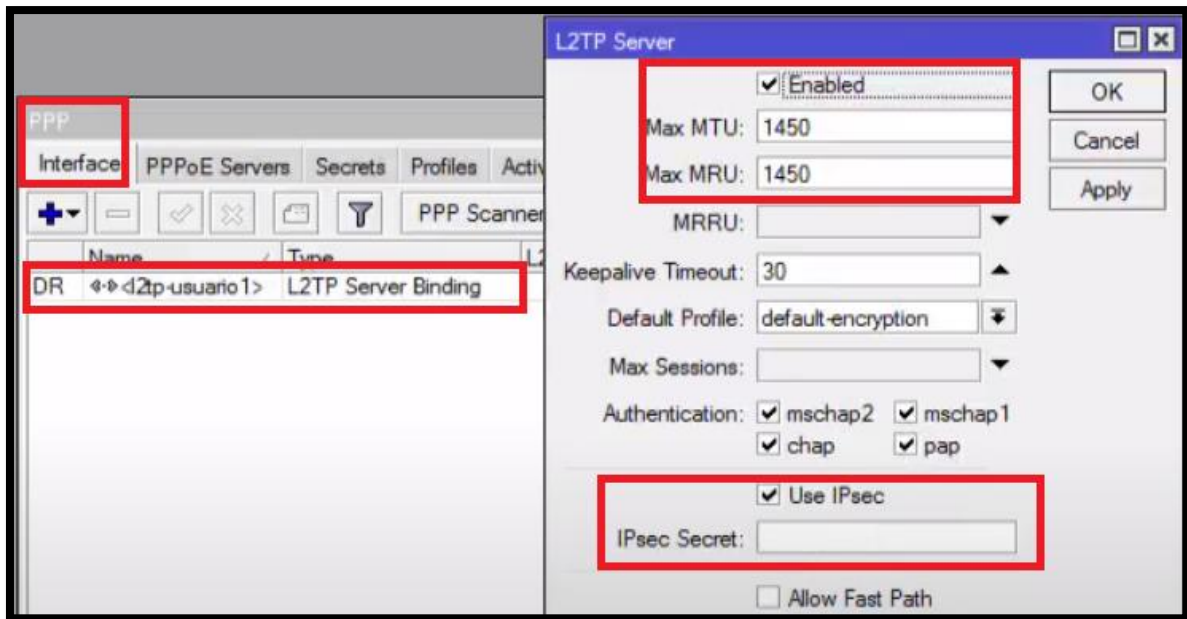


Figura 54: Pestaña “PPP – L2TP Server” – Sede Principal - WINBOX

Fuente: Propia

- ❖ Seguidamente se valida que en el apartado “IP-IPsec”, por defecto ya aparece en la pestaña “Peer” la contraseña que se colocó para el “IPsec”, así como sus demás parámetros.

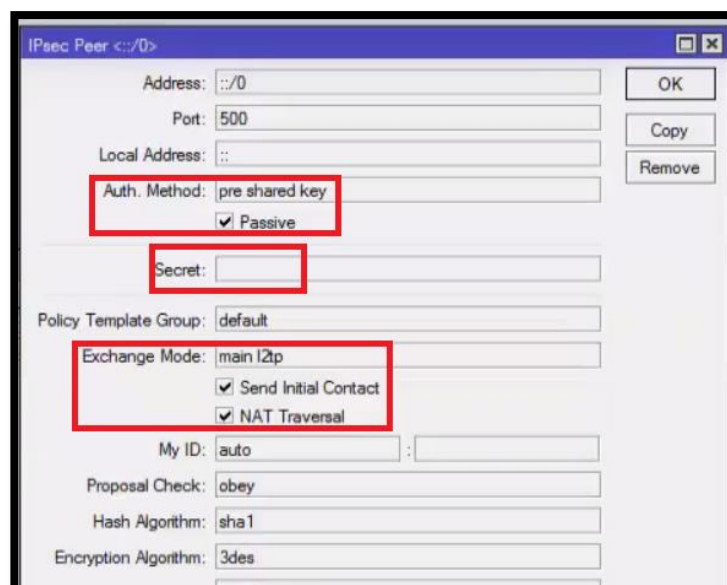


Figura 55: Pestaña “IP – IPsec - Peer” – Sede Principal - WINBOX

Fuente: Propia

- ❖ Se configura un usuario con perfil VPN y servicio L2TP, teniendo en cuenta que se puede colocar IP Estática local y remota para interconectar ambas sedes.

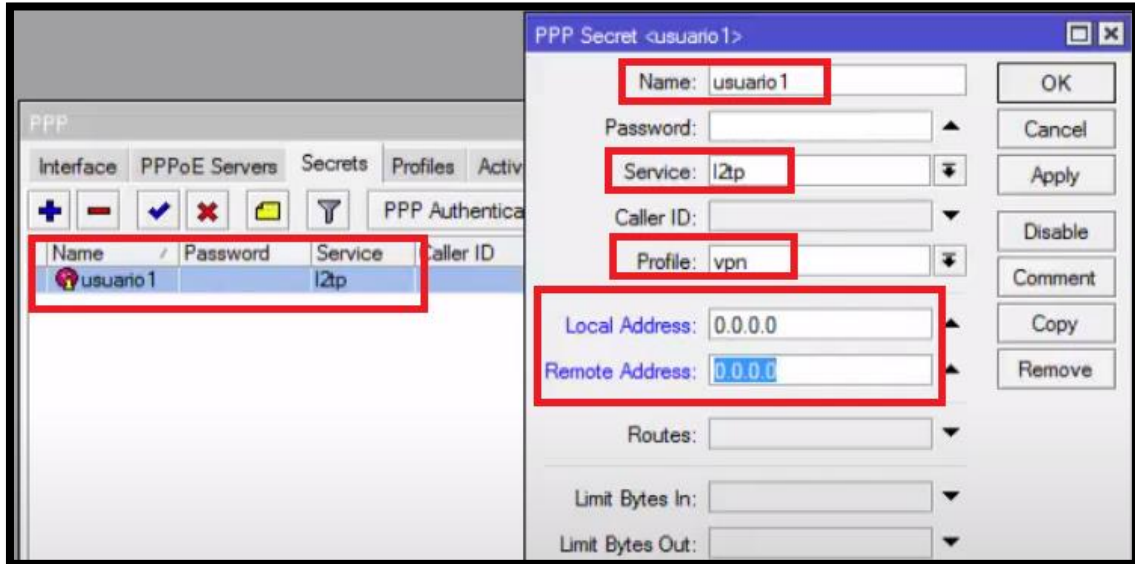


Figura 56: Pestaña “PPP – Secrets” – Sede Principal - WINBOX

Fuente: Propia

- **RB Mikrotik – Sede Secundaria - L2TP/IPsec**

- ❖ Se configura “L2TP Client” para interconectar ambas sedes por el túnel VPN L2TP/IPsec.

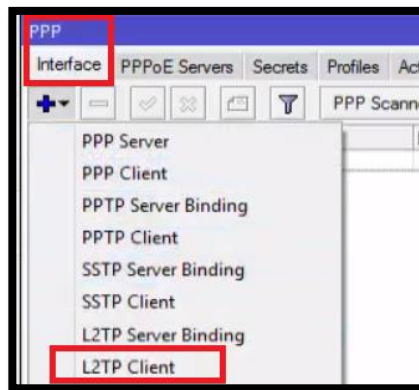


Figura 57: Pestaña “PPP – Interface – L2TP Client” – Sede Secundaria – WINBOX

Fuente: Propia

- ❖ En la pestaña “*Dial Out*” se configura la IP Pública del Servidor VPN de la Sede Principal, también usuario y contraseña, tanto de la conexión como del IPsec.

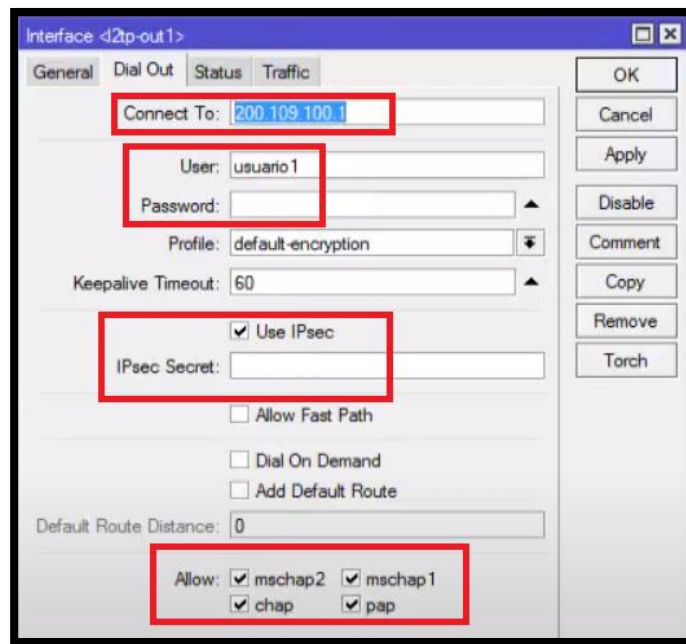


Figura 58: Pestaña “*Interface – Dial Out*” – Sede Secundaria – WINBOX

Fuente: Propia

- ❖ Se visualiza una letra “R” en la pestaña “*PPP – Interface*”, que nos indica una conexión exitosa entre las dos sedes del túnel VPN L2TP.

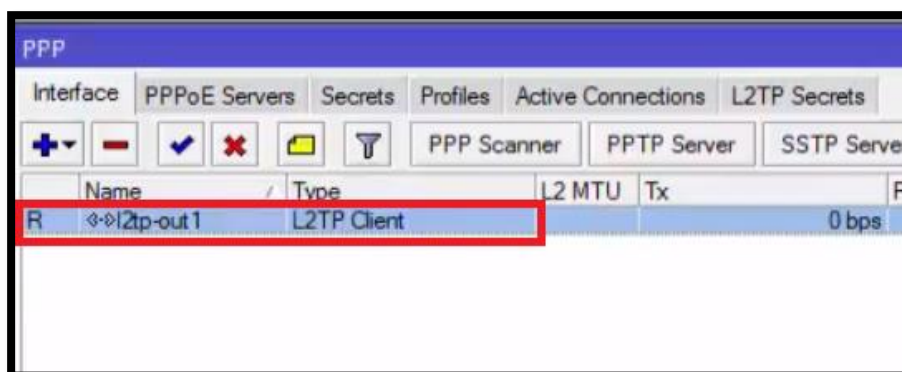


Figura 59: Visualización pestaña “*PPP – Interface*” Sede Secundaria – WINBOX

Fuente: Propia

- ❖ Se visualiza una ruta dinámica en la lista de rutas, que valida la conexión exitosa entre las dos sedes del túnel VPN L2TP.

	Dist. Address	Gateway	Distance	Routing
AS	0.0.0.0/0	200.109.100.1 reachable ether1	1	
DAC	1.1.1.1	l2tp-out 1 reachable	0	
DAC	10.10.10.0/24	ether2 reachable	0	
AS	192.168.100.0/24	1.1.1.1 reachable l2tp-out 1	1	
DAC	200.109.100.0/30	ether1 reachable	0	

Figura 60: Visualización pestaña “Route List” Sede Secundaria – WINBOX

Fuente: Propia

2.4 RESULTADOS

Como resultado final se logró implementar el diseño de Red Privada Virtual a bajo costo, en dos organizaciones de Lima Metropolitana, debido a la necesidad que dichas organizaciones tenían y por la cual estaban adoptando formas poco usuales para dar continuidad alternativa a su trabajo en esta pandemia. Las organizaciones en que se implementó con éxito el diseño de Red Privada Virtual propuesto fueron:

- QUALITY, HEALTH, SAFETY AND ENVIRONMENT SERVICES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA (Q. H. S. E.)
- KLIMATECHNIK S.A.C. (KT PERÚ)

2.4.1 RESULTADO DE ANÁLISIS Y DIAGNÓSTICO

2.4.1.1 Resultados de Análisis y Diagnóstico para la Organización Q. H. S. E.

Para la empresa Q. H. S. E., se realizó el tipo de implementación de “Red Privada Virtual de acceso remoto”, usando un servidor de dominio *Cloud* y el protocolo PPTP, esto permitió interconectar a los colaboradores externos en localidades remotas (Hogares y locales de clientes en visita comercial), con la sede principal y viceversa, sin importar las limitaciones geográficas, debido a los beneficios de la Red Privada Virtual de acceso remoto”.

Según lo mencionado anteriormente, para lograr la implementación de esta VPN, se tuvo presente los recursos ya existentes de la infraestructura tecnológica en la organización Q. H. S. E., realizándose un análisis y diagnóstico según los requerimientos de la organización, dado de la siguiente forma:

- **Análisis:**

- **Requerimiento de mejora para la velocidad de interconexión dentro de la Red Local (LAN) de la organización:** Se tuvo en cuenta que toda su conectividad física actual se realiza sobre cableado UTP Categoría 5, equipos conmutadores *Fast Ethernet* y tarjetas de red *Fast Ethernet* dentro de sus equipos computadores estáticos. Es decir, toda su conectividad se basaba en velocidades de 10/100 Mbps.
- **Requerimiento de una forma de conexión VPN que no implique Ip Pública estática en el Enrutador del Operador contratado:** Se validó que el servicio de internet contratado por la organización, era un servicio que no les brindaba una IP Pública Estática, y que además de ello tratar de que la empresa operadora lo brinde, implicaría un costo mensual sobrevaluado para la cantidad de megas que la empresa tiene en la contrata con la organización Q. H. S. E.

- **Diagnóstico:**

- **Requerimiento de mejora para la velocidad de interconexión dentro de la Red Local (LAN) de la organización:** Se diagnosticó brindar la solución de cambiar el cableado UTP Categoría 5 a Categoría 6, también de cambiar sus dos conmutadores (*Switches*) que tenían puertos 10/100 Mbps a enrutadores con puertos 100/1000 Mbps, y por último las tarjetas 10/100 Mbps de sus computadores estáticos a tarjetas 100/1000 Mbps

Todo lo mencionado anteriormente en paralelo con la implementación de un equipo RB Mikrotik modelo RB450Gx4, el cual también tiene puertos 100/1000 Mbps y un procesador de alto rendimiento de 4 núcleos. Conservando así los equipos computadores de la organización y evitando gastos innecesarios en hardware total y software, además de logrando como resultado una infraestructura de red basada en velocidad de transferencia 100/1000 (*Gigabit Ethernet*) en toda su interconexión, tanto en su Red Local (LAN), como en la implementación de su Túnel VPN usando el protocolo PPTP.



Figura 61: Topología Organización Q. H. S. E.

Fuente: Propia

- **Requerimiento de una forma de conexión VPN que no implique Ip Pública estática en el Enrutador del Operador contratado:** Se diagnosticó brindar la solución de utilizar un servicio de dominio de Servidor Nube VPN, el cual tiene un costo muy accesible, siendo eficaz y seguro, logrando como resultado evitar cambiar equipo enrutador de operador de internet, así como de no acceder a el costo sobrevaluado que dicho operador quería imponer a la empresa, para obtener una Ip Pública Estática.

2.4.1.2 Resultados de Análisis y Diagnóstico para la Organización KT PERÚ

Para la empresa KT PERÚ, se realizó el tipo de implementación de "Red Privada Virtual de sitio a sitio", usando un servidor de dominio *Cloud* y el protocolo IPsec / L2TP, esto permitió interconectar su sede principal ubicada en el parque industrial de Villa el Salvador (donde se encontraba su Servidor de datos), con un local

cercano en Villa María del Triunfo (donde se encontraba su Servidor de dominio) que aloja programas de facturación online, así como brindar la factibilidad para sus colaboradores externos en localidades remotas (hogares), en interconexión con la sede principal y viceversa, sin importar las limitaciones geográficas, debido a los beneficios de la “Red Privada Virtual de sitio a sitio”.

Según lo mencionado anteriormente, para lograr la implementación de esta VPN, se tuvo presente los recursos ya existentes de la infraestructura tecnológica en la organización KT PERÚ, realizándose un análisis y diagnóstico según los requerimientos de la organización, dado de la siguiente forma:

- **Análisis:**

- **Requerimiento de interconexión entre sus dos sedes al menor costo posible:** Se tuvo en cuenta que el requerimiento de la empresa KT PERÚ fue de priorizar la menor inversión posible, requiriendo que sus dos sedes ubicadas en distintos distritos puedan conectarse entre sí, y que a su vez sus colaboradores puedan interconectarse a las mismas sin importar el lugar donde se encuentren. Para ello la empresa KT PERÚ indicó explícitamente que no deseaban implementar o cambiar nada por sobre su infraestructura de red ya existente en cada sede, más solo el uso de los dos RB Mikrotik que interconectan el tipo de VPN Sitio a Sitio.
- **Requerimiento de una forma de conexión VPN que no implique Ip Pública estática en el Enrutador del Operador contratado:** Se validó que el servicio de internet contratado por la organización, era un servicio que no les brindaba una IP Pública Estática, tanto en su Sede Principal como en su Sede Secundaria, y que además de ello tratar de que la empresa operadora lo brinde, implicaría un costo mensual sobrevaluado para la cantidad de megas que la empresa tiene en la contrata con la organización KT PERÚ.

- **Diagnóstico:**

- **Requerimiento de interconexión entre sus dos sedes al menor costo posible:** Se diagnosticó brindar la solución de implementar dos equipos RB Mikrotik modelo RB750 R2, que tiene 2 núcleos en su procesador, el cual es un modelo de gama media que no implica un gasto considerable en la implementación del túnel VPN Sitio a Sitio. Además, se tomó en cuenta que toda su infraestructura de red es de velocidad 10/100 Mbps (*Fast Ethernet*) y se mantuvo con la misma sin cambios, es decir su cableado de red UTP es de Categoría 5, su conmutador principal tiene puertos 10/100 Mbps (*Fast Ethernet*), y sus tarjetas de red de equipos estáticos 10/100 Mbps (*Fast Ethernet*).

Todo lo mencionado anteriormente en paralelo con la implementación de los dos equipos RB Mikrotik modelo RB750 R2, tendrá como prioridad conservar la infraestructura de red de la empresa KT PERÚ en sus dos sedes, es decir se desarrollara un a interconexión y configuración de redes de tal manera que toda la implementación sea transparente para los usuarios internos y externos, además logrando como resultado una solución de reutilización, por sobre la infraestructura ya existente de hardware y software en la Red Local (LAN) de la empresa KT PERÚ, que es uno de nuestros objetivos específicos para la implementación.

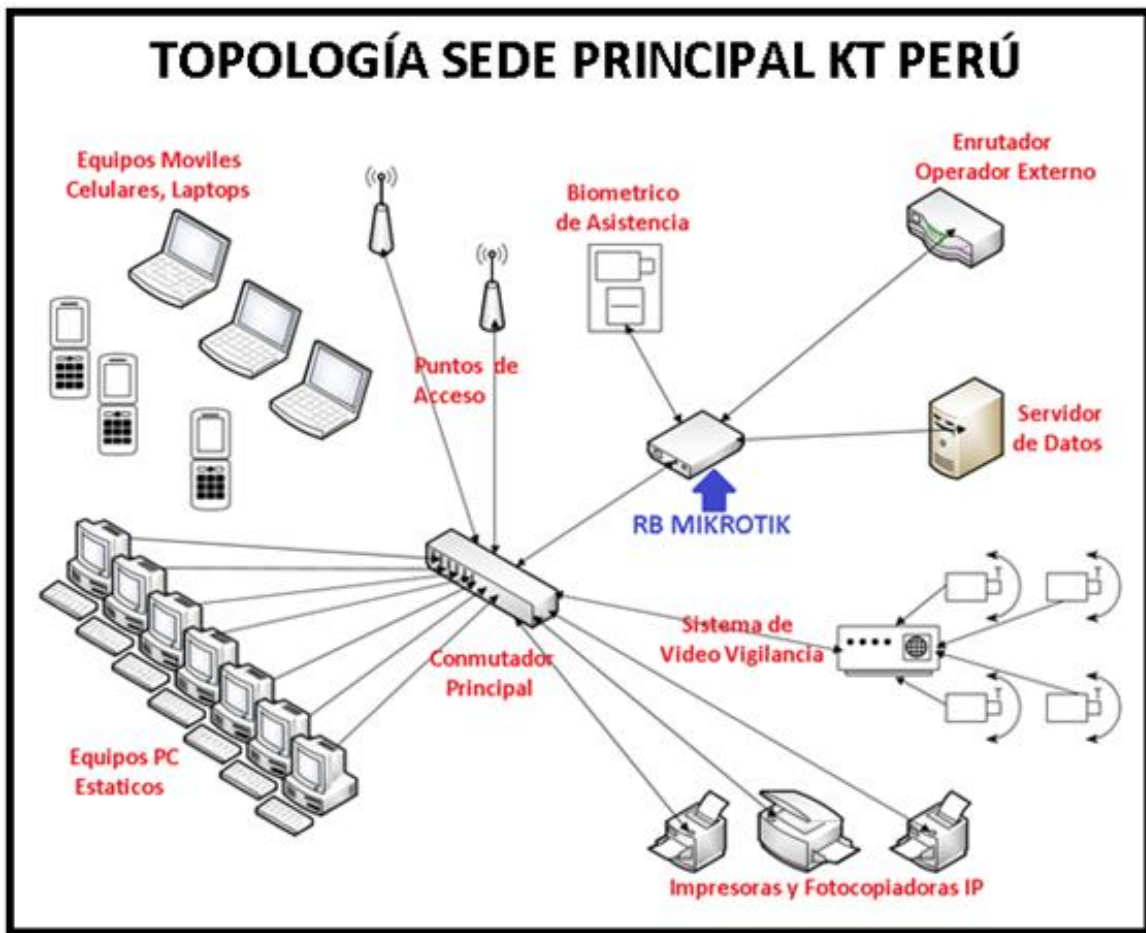


Figura 62: Topología Sede Principal KT PERÚ

Fuente: Propia

- **Requerimiento de una forma de conexión VPN que no implique Ip Pública estática en el Enrutador del Operador contratado:** Se diagnosticó brindar la solución de utilizar un servicio de dominio de Servidor Nube VPN, para el túnel de interconexión de la VPN Sitio a Sitio usando el protocolo IPsec/ L2TP, el cual tiene un costo muy accesible, siendo eficaz y seguro, logrando como resultado evitar cambiar equipo enrutador de operador de internet en las dos sedes de la empresa KT PERÚ, así como de no acceder a el costo sobrevaluado que dicho operador quería imponer a la empresa, para obtener una Ip Pública Estática en cada sede.

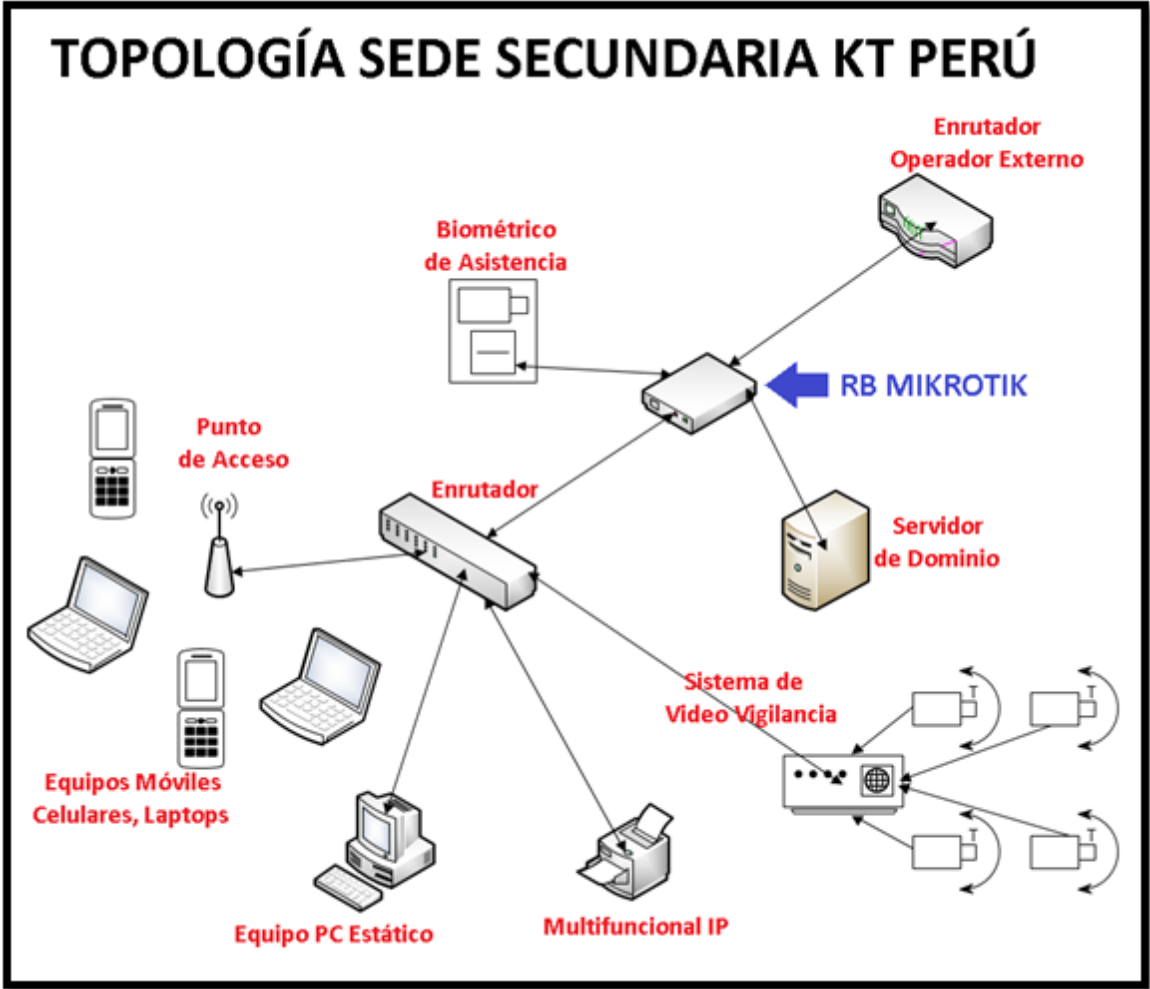


Figura 63: Topología Sede Secundaria KT PERÚ

Fuente: Propia

2.4.2 RESULTADOS DE MODELAMIENTO

2.4.2.1 Resultados de Modelamiento para la organización Q. H. S. E.

Se configuró una VPN - PPTP del Tipo de Acceso Remoto en el equipo Mikrotik, implementado para la Sede de la organización Q. H. S. E., y además de ello también se configuró los accesos a la VPN en los diversos dispositivos portátiles y estáticos de la organización. Tomando en consideración su infraestructura de redes que ya tenían implementada en su sede, así como del requerimiento de contar con una interconexión *Gigabit Ethernet* en toda la Red Local (LAN), donde dicho modelamiento quedó de la siguiente forma:

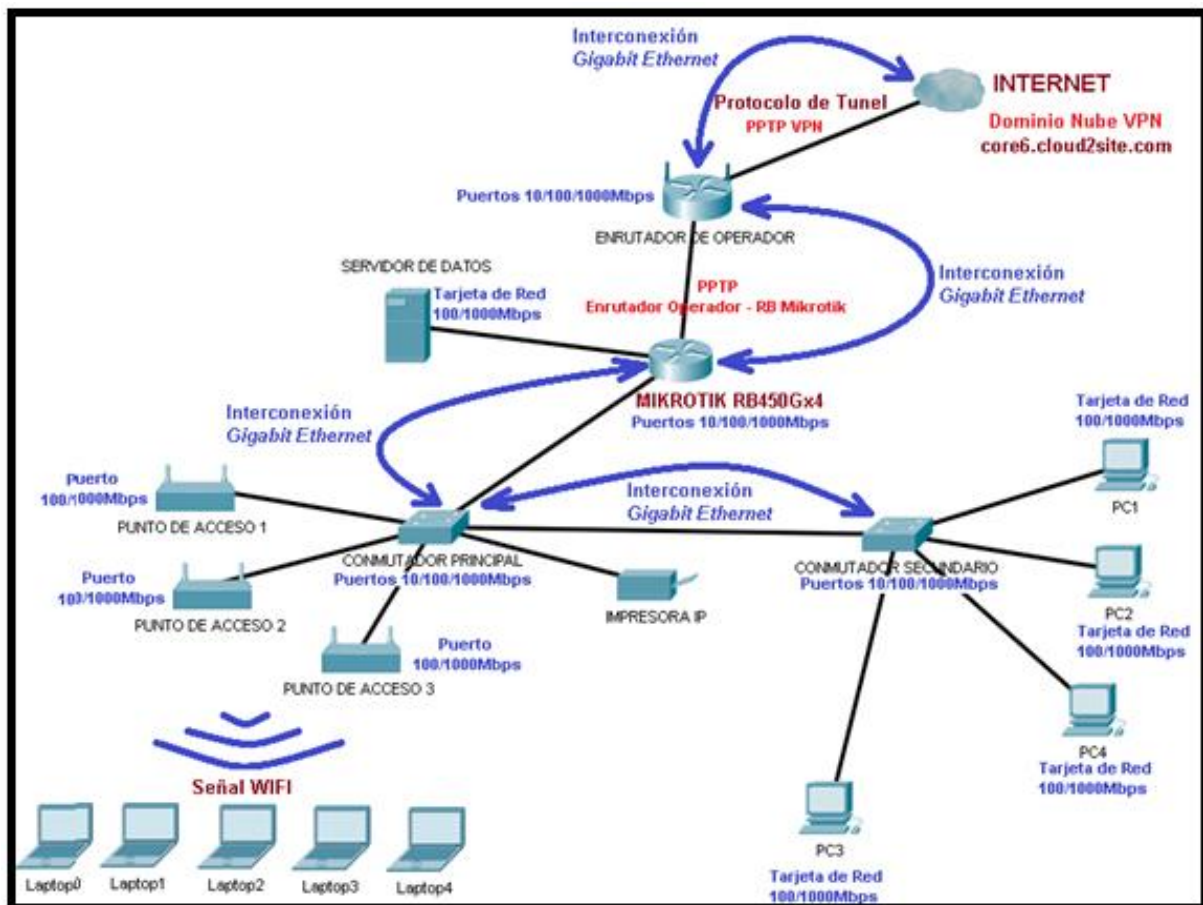


Figura 64: Modelamiento Organización Q. H. S. E.

Fuente: Propia

- **Conectividad y Calidad de Servicio(QoS) en el Modelamiento (Q. H. S. E.):**

Mediante el tablero de control de la lista de interfaces configuradas, que viene incluido en la plataforma WINBOX, se valida y certifica la calidad de tráfico transmitido y recibido en tiempo real, por sobre todas las interfaces físicas, lógicas y enlaces de VPN, dentro del equipo Mikrotik.

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)	
R	LAN	Bridge	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	
R	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	
S	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	
RS	ether3	Ethernet	1500	1598	512 bps	0 bps	1	0	0 bps	0 bps	0	0	
S	ether4	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0	
R	ether1	Ethernet	1500	1598	115.5 k...	8.4 kbps	12	10 120.2 ...	14.5 ...			17	16
R	ovpn-out1	OVPN Client	1500		105.8 k...	3.6 kbps	12	6	0 bps	0 bps	0	0	
R	WAN	Ethernet	1500	1598	115.5 k...	8.4 kbps	12	10 120.2 ...	14.5 ...			17	16
R	CLOUDSITE VPN PLUS	OVPN Client	1500		105.8 k...	3.6 kbps	12	6	0 bps	0 bps	0	0	
R	<pptp-TEST_NOVA>	PPTP Server Binding	1400		928 bps	976 bps	2	2	0 bps	0 bps	0	0	

Figura 65: Visualización de la lista de interfaces totales - Q. H. S. E. - WINBOX

Fuente: Propia

Para lo mencionado anteriormente se adjunta la siguiente tabla de valores máximos que se pueden utilizar en la transmisión de datos, en la Red Local (LAN) como en la Red de Área Ampla (WAN), para la organización Q. H. S. E.

Tabla 3

Velocidad de transferencia máxima de datos por las capas de los medios de comunicación – Modelo OSI (Q. H. S. E.)

Capa OSI	Protocolo	Antes de implementación		Después de implementación	
		LAN	WAN	LAN	WAN
Red – Capa 3	IP	100M bps	1000Mbps	1000Mbps	1000Mbps
Enlace de datos – Capa 2	Ethernet	100M bps	1000Mbps	1000Mbps	1000Mbps
Enlace de datos – Capa 2	PPTP	100M bps	1000Mbps	1000Mbps	1000Mbps
Física – Capa 1	Física – Capa 1	100M bps	1000Mbps	1000Mbps	1000Mbps

Fuente: Propia

2.4.2.2 Resultados de Modelamiento para la organización KT PERÚ

Se configuró una VPN - L2TP / IPsec del Tipo de Sitio a Sitio en los equipos Mikrotik implementados en las dos sedes de la organización KT PERÚ, y además de ello también se configuró los accesos a la VPN en los diversos dispositivos portátiles y estáticos de la organización. Tomando en consideración su infraestructura de redes que ya tenían implementada en su sede, así como del requerimiento particular de la empresa que fue de lograr la interconexión entre sus dos sedes, al menor costo posible, donde dicho modelamiento quedó de la siguiente forma:

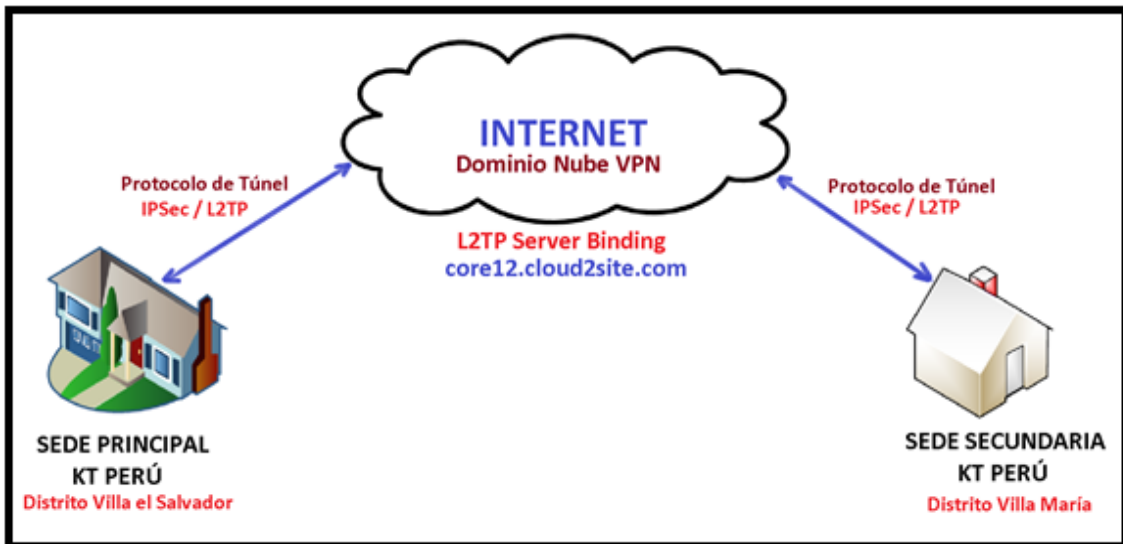


Figura 66: Modelamiento de la interconexión entre las dos sedes de KT PERÚ, usando una VPN Tipo de Sitio a Sitio

Fuente: Propia

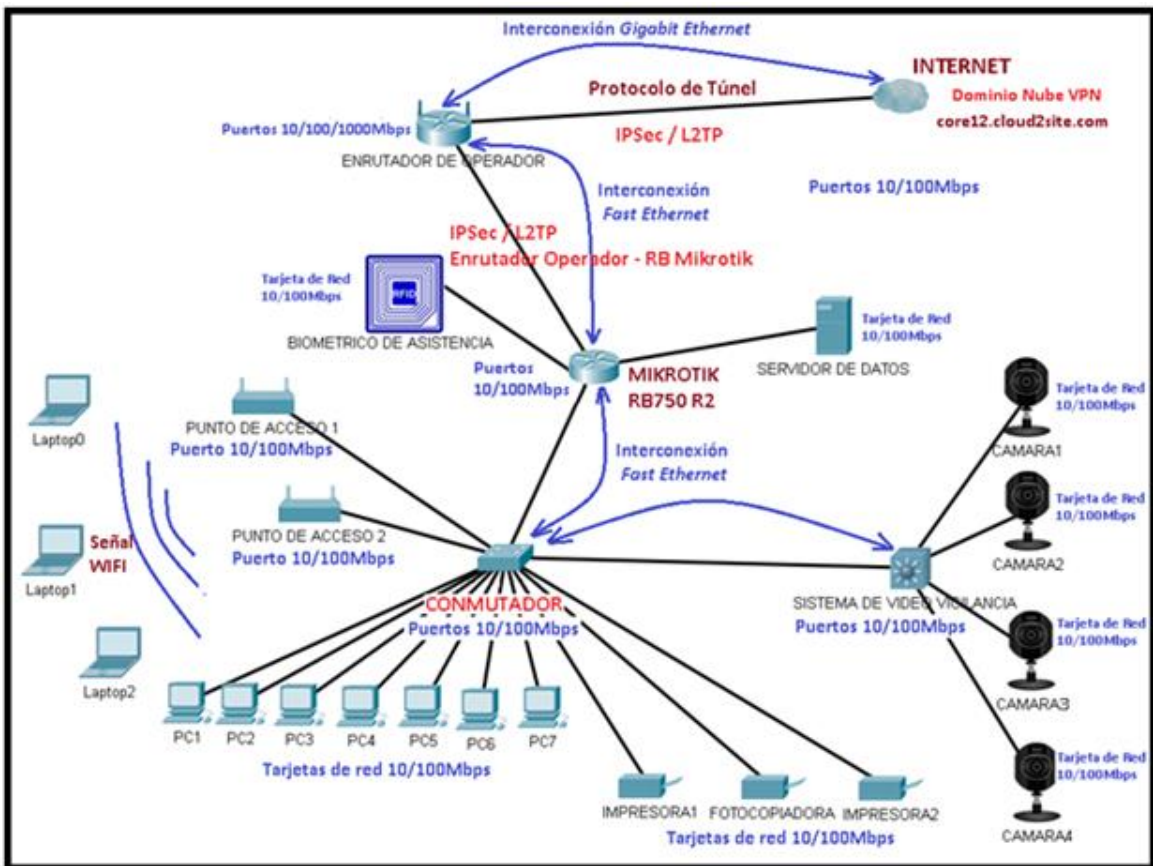


Figura 67: Modelamiento de la Sede Principal KT PERÚ.

Fuente: Propia

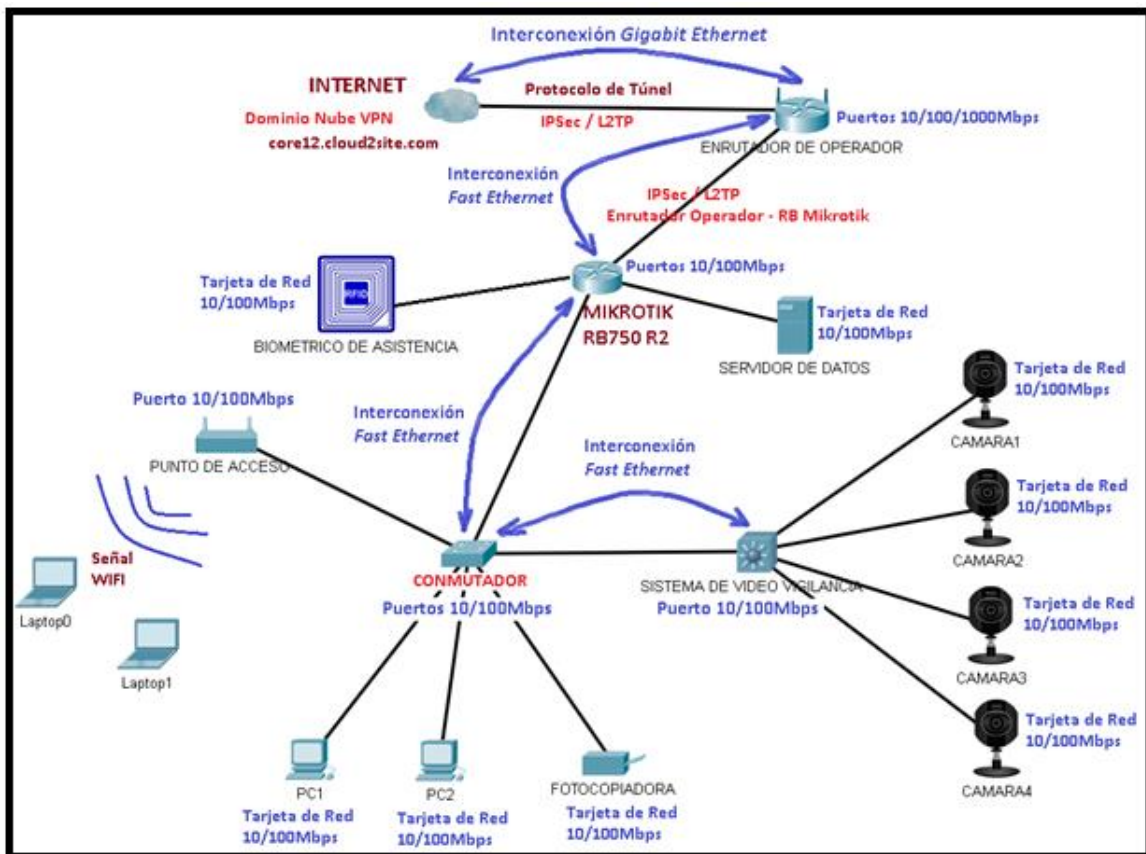


Figura 68: Modelamiento de la Sede Secundaria KT PERÚ.

Fuente: Propia

- **Conectividad y Calidad de Servicio(QoS) en el Modelamiento (KT PERÚ):**

Mediante el tablero de control de la lista de interfaces configuradas, que viene incluido en la plataforma WINBOX, se valida y certifica la calidad de tráfico transmitido y recibido en tiempo real, por sobre todas las interfaces físicas, lógicas y enlaces de VPN, dentro del equipo Mikrotik.

Name	Type	Actual MTU	L2 MTU	Tx	Rx
... Vpn site-to-site					
R <=> Cloud2site-vpn	SSTP Client	1500		768 bps	1768 bps
R <=> LAN	Bridge	1500	1598	528 bps	2.6 kbps
... ether1					
R <=> WAN	Ethernet	1500	1600	26.9 kbps	12.6 kbps
S <=> ether2	Ethernet	1500	1598	0 bps	0 bps
... FILE SERVER					
S <=> ether3	Ethernet	1500	1598	0 bps	0 bps
S <=> ether4	Ethernet	1500	1598	0 bps	0 bps
... SWTICH LAN					
RS <=> ether5	Ethernet	1500	1598	1072 bps	2.9 kbps
... Vpn Site 2 Site L2TP					
R <=> I2tp-in1	L2TP Server Binding	1450		0 bps	0 bps
... CLOUD2SITE VPN PLUS					
R <=> ovpn-out1	OVPN Client	1500		18.3 kbps	2.1 kbps

Figura 69: Visualización de la lista de interfaces totales - KT PERÚ - WINBOX

Fuente: Propia

Para lo mencionado anteriormente se adjunta la siguiente tabla de valores máximos que se pueden utilizar en la transmisión de datos, en la Red Local (LAN) como en la Red de Área Amplia (WAN), para la organización KT PERÚ.

Tabla 4

Velocidad de transferencia máxima de datos por las capas de los medios de comunicación – Modelo OSI (KT PERÚ)

Capa OSI	Protocolo	Sede Principal		Sede Secundaria	
		LAN	WAN	LAN	WAN
Red – Capa 3	IP	100Mbps	1000Mbps	100Mbps	1000Mbps
Enlace de datos – Capa 2	Ethernet	100Mbps	1000Mbps	100Mbps	1000Mbps
Enlace de datos – Capa 2	L2TP/IPsec	100Mbps	1000Mbps	100Mbps	1000Mbps
Física – Capa 1	Física – Capa 1	100Mbps	1000Mbps	100Mbps	1000Mbps

Fuente: Propia

2.4.3 RESULTADOS DE INVERSIÓN

Para los Resultados de Inversión, es necesario tener previamente en cuenta la siguiente tabla, que será fundamental en la determinación de costos para la implementación de la VPN.

Tabla 5

Comparación de precios mínimos y máximos de los equipos que se pueden utilizar en una implementación VPN, tomando en consideración principales marcas proveedoras.

Marca	Precio Mínimo (Dólares)	Precio Máximo (Dólares)	Observaciones
Cisco	675	16900	La característica de VPN dependerá de si la serie del equipo adquirido cuenta con los módulos necesarios.
Sophos	680	7000	La característica de VPN dependerá del tipo de licencias adquiridas en el dispositivo UTM.
Fortinet	290	19800	La característica de VPN dependerá del tipo de licencias adquiridas en el dispositivo <i>Firewall</i>
Mikrotik	29	4000	Todos sus modelos traen activada la característica VPN, y sus licencias están incluidas en su sistema operativo RouterOS actualizable de manera gratuita. Además es un enrutador cortafuego todo en uno.

Fuente: Propia

2.4.3.1 Resultados de Inversión para la organización Q. H. S. E.

Teniendo presente la tabla anterior, tenemos que para la implementación de la VPN en Q. H. S. E. se tuvo en cuenta que la empresa deseaba velocidad óptima en toda su red, tanto en transmisión como en recepción, para el túnel de la VPN y para la interconexión de sus equipos a nivel de Red Local (LAN), por tal motivo se contempló los siguientes gastos:

- **Equipo MIKROTIK RB450Gx4:** Equipo Mikrotik con la característica principal de poseer 4 núcleos en su procesador y puertos 100/1000 (*Gigabit Ethernet*), lo cual acelera toda ejecución de transferencia y recepción del equipo en la Red Local de la organización como para la interconexión de la VPN implementada.
Precio: \$ 95

- **Cableado UTP Categoría 6:** Esta categoría de cable de red UTP, asegura la transferencia de velocidad para puertos 100/1000 (*Gigabit Ethernet*). Se utilizaron 100 metros para cambiar el cableado de toda la infraestructura de red de la Sede de Q. H. S. E.
Precio: \$ 0.30 (1 metro)

- **Tarjetas de red 100/1000 (*Gigabit Ethernet*):** Este tipo de tarjeta es ideal para el tipo de cableado que se realizó y para percibir la transferencia de ancho de banda emitida por el equipo Mikrotik. Se utilizaron 4 tarjetas para las computadoras estáticas.
Precio: \$ 15 c/u

- **Conmutadores (*SWITCH*) 100/1000 (*Gigabit Ethernet*):** Este tipo de *Switch* provee la canalización de todo el tráfico *Gigabit Ethernet* en la infraestructura de la organización. Se utiliza dos conmutadores (*Switch*) para Q. H. S. E.
Precio: \$ 27 c/u (8 puertos)

- **Pago Anual de dominio de Servidor *CLOUD VPN*:** Debido a que el operador de internet de la organización no le brindaba una IP Pública Estática, se vio la opción de implementar un Servidor *CLOUD VPN*, que aseguró la estabilidad y seguridad encriptada de la interconexión VPN en la organización.
Precio: \$ 7 x mes

- **Pago de Mano de Obra:** Se realiza un solo pago por el trabajo intelectual del modelamiento, diseño e implementación de la Red Privada Virtual.
Precio: \$ 200

Se logró para Q. H. S E. un resultado de inversión muy por debajo del costo real de una implementación de esta magnitud, considerando que se actualizó la mayor parte de la infraestructura de red en toda la organización.

Tabla 6

Costo total de la implementación VPN - Q. H. S. E.

Descripción	Costo Unidad	Cantidad	Costo Total
RB Mikrotik RB450Gx4	\$ 95	1	\$ 95
Cable UTP Categoría 6	\$ 0.30 x m	100 m	\$ 30
Tarjeta de Red Giga	\$15	4	\$ 60
Conmutador (<i>Switch</i>)	\$ 27	2	\$ 54
Dominio Nube VPN	\$ 7 x mes	12	\$ 84
Pago de mano de obra	\$200	1	\$ 200
Inversión Total			\$ 523

Fuente: Propia

2.4.3.2 Resultados de Inversión para la organización KT PERÚ

Para la implementación de la VPN en KT PERÚ. se tuvo en cuenta que la empresa deseaba la interconexión entre sus dos sedes al menor costo posible de inversión, tanto para el túnel de la VPN, como para la interconexión de sus equipos a nivel de Red Local (LAN), por tal motivo se contempló los siguientes gastos:

- **Equipo MIKROTIK RB750 R2** : Equipo Mikrotik con la característica principal de poseer 2 núcleos en su procesador y puertos 10/100 (*Fast Ethernet*), lo cual brinda una ejecución estándar de transferencia y recepción, para la comunicación con la Red Local de la organización, como también para la interconexión de la VPN implementada Tipo Sitio a Sitio.

Precio: \$ 50

- **Pago Anual de dominio de Servidor CLOUD VPN:** Debido a que el operador de internet de la organización no le brindaba una IP Pública Estática, se vio la opción de implementar un Servidor *CLOUD VPN*, que aseguró la estabilidad y seguridad encriptada de la interconexión VPN en la organización.

Precio: \$ 7 x mes

- **Pago de Mano de Obra:** Se realiza un solo pago por el trabajo intelectual del modelamiento, diseño e implementación de la Red Privada Virtual.

Precio: \$ 250

Se logró para KT PERÚ un resultado de inversión muy por debajo del costo real de una implementación de esta magnitud, considerando la implementación de un túnel VPN de sede a sede para la organización.

Tabla 7

Costo total de la implementación VPN - KT PERÚ

Descripción	Costo Unidad	Cantidad	Costo Total
RB Mikrotik RB750 R2	\$ 50	2	\$ 100
Pago de mano de obra	\$250	1	\$ 250
Inversión Total			\$ 350

Fuente: Propia

CONCLUSIONES

- La escalabilidad y reutilización de la infraestructura de red es muy importante, por lo tanto, se logró garantizar que esta propuesta, podrá ser realizada sobre la infraestructura en redes ya existente de toda organización, tal cual se observa en la Figura 68, 71 y 72, donde se realizó previo análisis y diagnóstico, teniendo en cuenta los requerimientos solicitados por cada organización, logrando que toda infraestructura de red sea escalable.
- Una VPN podrá ser modelada sobre todo tipo de organización, obteniendo el máximo desempeño de la infraestructura de red, tanto en su topología física como lógica, no siendo un factor limitante la distancia entre una o más sedes que tenga la organización, esto se pudo lograr tal cual se observa en las tablas 3 y 4, donde sé válida también, actualizaciones en hardware de infraestructura para los modelados de las empresas Q. H. S. E. y K. T. PERÚ.
- Según las tablas 6 y 7, se logró la reducción en costos de inversión, implementando una VPN usando equipos RB Mikrotik, y por lo tanto podemos concluir que se trata de una opción excelente de tecnología para el teletrabajo en las organizaciones que tienen bajos recursos, debido a que es una alternativa viable a las marcas tradicionales. Además, la solución de tecnología Mikrotik abarca varios campos como la ciberseguridad por filtros cortafuego, que ya están incluidos y son programables, sin tener la necesidad de gastos extras en el equipo ya adquirido, a diferencia de otras marcas que solicitan más inversiones monetarias en licencias y módulos físicos.

RECOMENDACIONES

- Es recomendable estar en constante actualización de las tecnologías para dispositivos de la marca Mikrotik en las VPN, ya que es una marca que tiene variedad de soluciones en las redes interconexión para todo tipo de organización, teniendo un costo de inversión accesible y un alto rendimiento de *hardware*.
- Es importante resaltar que no todas las organizaciones tienen un operador de Internet que les brinde un servicio que incluye Ip Pública estática, por tal motivo es que en este trabajo se incluye la opción de optar por dar conexión a la VPN, usando un servicio de Dominio Nube VPN, como alternativa, y de esta forma cubrir las necesidades de toda organización, en la implementación de su VPN.
- Un inconveniente latente y crítico podría ser la ciberseguridad dentro de la Red Local (LAN) de la organización, para lo cual es recomendable que se deba establecer protocolos y políticas de seguridad en la misma, teniendo en consideración que, de no hacerlo, se corren riesgos de acceso interno malintencionado dentro de la red en la organización.
- Es recomendable que a medida que se implemente más infraestructura de red en una organización, sean dispositivos periféricos, cableado estructurado, etc. Se debe considerar también aumentar el ancho de banda contratado en la operadora de Internet, debido a que, a más infraestructura, más pérdida de calidad de experiencia de servicio, en la transmisión de datos dentro y fuera de la red se experimentará, y por ende más lentitud en el uso del túnel de la VPN.
- Se debe tomar en cuenta que la implementación de la VPN como medio para el teletrabajo en esta pandemia del COVID-19, es una forma de aplacar la masificación del virus por contagio interpersonal, pero no es una solución que no implique otros riesgos en la salud, tales como el sedentarismo, por lo tanto, es recomendable no olvidar los buenos hábitos para estar en buena salud.

REFERENCIAS BIBLIOGRÁFICAS

1. Congreso Constituyente Democrático (1993). Constitución Política del Perú. Artículo (206 artículos). de fecha 29 de diciembre de 1993.
2. Torres, J. (2016). Diseño de una Red Privada Virtual para la optimización de las comunicaciones en la empresa Comunicaciones e Informática S.A.C. Tesis para optar el Título de Ingeniero de Sistemas y Cómputo, UNIVERSIDAD INCA GARCILAZO DE LA VEGA, Lima, Perú.
3. SIA Mikrotīkls. (1996-2020). Mikrotik. Letonia, Norte de Europa.: MikroTik. Recuperado de <https://mikrotik.com/>
4. Martel, V. (2019). Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764. Tesis para optar el Título profesional de Ingeniero de Redes y Comunicaciones, UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, Lima, Perú.
5. Atencio, A. y Mamani, E. (2017). Diseño e Implementación de un prototipo de Red Privada Virtual en Capa 3 utilizando CISCO IOS para la Universidad Nacional del Altiplano. Tesis para optar el Título profesional de Ingeniero de Electrónico, UNIVERSIDAD NACIONAL DEL ALTIPLANO, Puno, Perú.
6. Favale, T., Soro, F., Trevisan, M., Drago, I., & Mellia, M. (2020). Campus traffic and e-Learning during COVID-19 pandemic. *Computer Networks*, 176(April). <https://doi.org/10.1016/j.comnet.2020.107290>
7. Prieto, Y. (2011). Implementación de la Red Privada Virtual (VPN) a las sucursales y usuarios externos de la empresa Hardsoft S.A. Trabajo de Grado para optar el Título de Ingeniero de Sistemas, UNIVERSIDAD LIBRE, Bogotá D. C., Colombia.

8. Mar, J. (2016). Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI CASO: Servidor de Correos. Tesis para optar al Título Profesional de Ingeniero de Sistemas. UNIVERSIDAD ANDINA DE CUSCO, Cusco, Perú.
9. Bhattarai, S., & Nepal, S. (2016). VPN research (Term Paper). *Https://Www.Researchgate.Net/*, January, 1–10. <https://doi.org/10.13140/RG.2.1.4215.8160>
10. Mendoza, J. (2010). Propuesta de Implementación de un entorno de VPN Empresarial en la empresa Electro Oriente S. A. Informe de Ingeniería para optar el Título Profesional de Ingeniero de Sistemas e Informática, UNIVERSIDAD NACIONAL DE SAN MARTÍN - TARAPOTO, San Martín, Perú.
11. Castro, D. (2019). Diseño e Implementación de la Interconexión de Sucursales de HP-STORE en las ciudades de Arequipa y Cusco mediante VPN con Mikrotik Router. Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero Electrónico, UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA, Arequipa, Perú.
12. Grados, I., Vásquez L. (2012). Diseño Lógico de Interconexión entre la Sede Central de Trujillo y la Sede Valle Jequetepeque con Tecnología VPN que permita la compartición segura de Recursos Informáticos. Tesis para optar el Título Profesional de Ingeniero Informático, UNIVERSIDAD NACIONAL DE TRUJILLO, Trujillo, Perú.
13. Hauser, F., Haberle, M., Schmidt, M., & Menth, M. (2020). P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN. *IEEE Access*, 8, 139567–139586. <https://doi.org/10.1109/ACCESS.2020.3012738>

14. Caicedo-Muñoz, J. A., Ledezma Espino, A., Corrales, J. C., & Rendón, A. (2018). QoS-Classifer for VPN and Non-VPN traffic based on time-related features. *Computer Networks*, 144, 271–279. <https://doi.org/10.1016/j.comnet.2018.08.008>
15. Santos, M. (2014). Diseño de Redes Telemáticas. Madrid, España: RA-MA S.A. de fecha 02 de diciembre de 2013.
16. Ministerio de Salud del Perú (2020). Lineamientos para la vigilancia de la salud de los trabajadores con riesgo de exposición a COVID-19 2020 según la Resolución Ministerial N°239 -2020-MINSA de fecha 28 de abril de 2020.
17. Presidencia del Consejo de Ministros (2020). Decreto Supremo que declara Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19 2020 según DECRETO SUPREMO N° 044-2020-PCM de fecha 15 de marzo de 2020.
18. Instituto de Economía y Desarrollo Empresarial – CCL (2020). Los Efectos de la COVID-19 en el PBI y en el empleo según Revista LA CAMARA de fecha 15 de junio de 2020.

ANEXOS

ANEXO A: Configuración Dominio Nube VPN

Este tipo de configuración se realizará si la organización no cuenta con el servicio de Ip Pública Estática, debido a motivos circunstanciales, tales como que la operadora de internet no cuenta con el servicio, o que el servicio de Ip Publica Estática es de un costo mensual elevado. Para dar solución a este escenario que se puede presentar en la organización, se sigue la siguiente configuración en el RB Mikrotik:

- ❖ Se contrata un “Dominio Nube VPN”, el cual nos brinda un certificado que se exportara en la pestaña de “Certificates”.

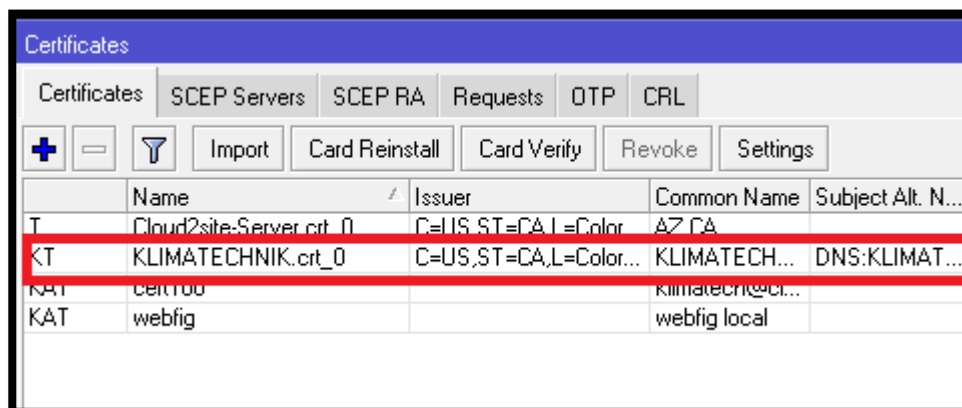


Figura 70: Pestaña “Certificates” – WINBOX

Fuente: Propia

- ❖ En la pestaña “Interfaces” se ingresa a la opción “OVPN Client”

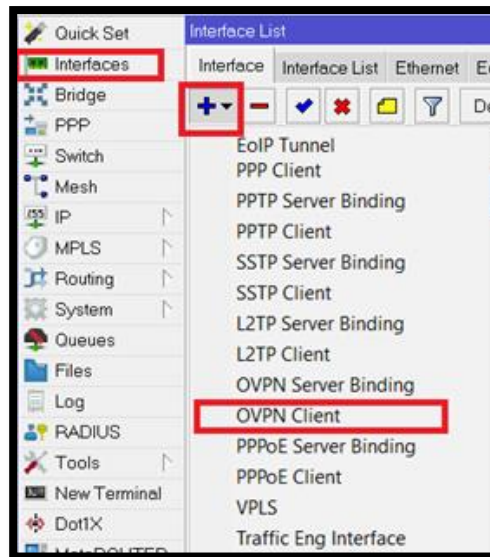


Figura 71: Visualización pestaña “*Interfaces – OVPN Client*” – WINBOX

Fuente: Propia

- ❖ Se procede a configurar el OVPN, colocando un “Dominio Nube VPN” que tengamos contratado previamente, y estableciendo los parámetros correspondientes en todas las opciones indicadas.

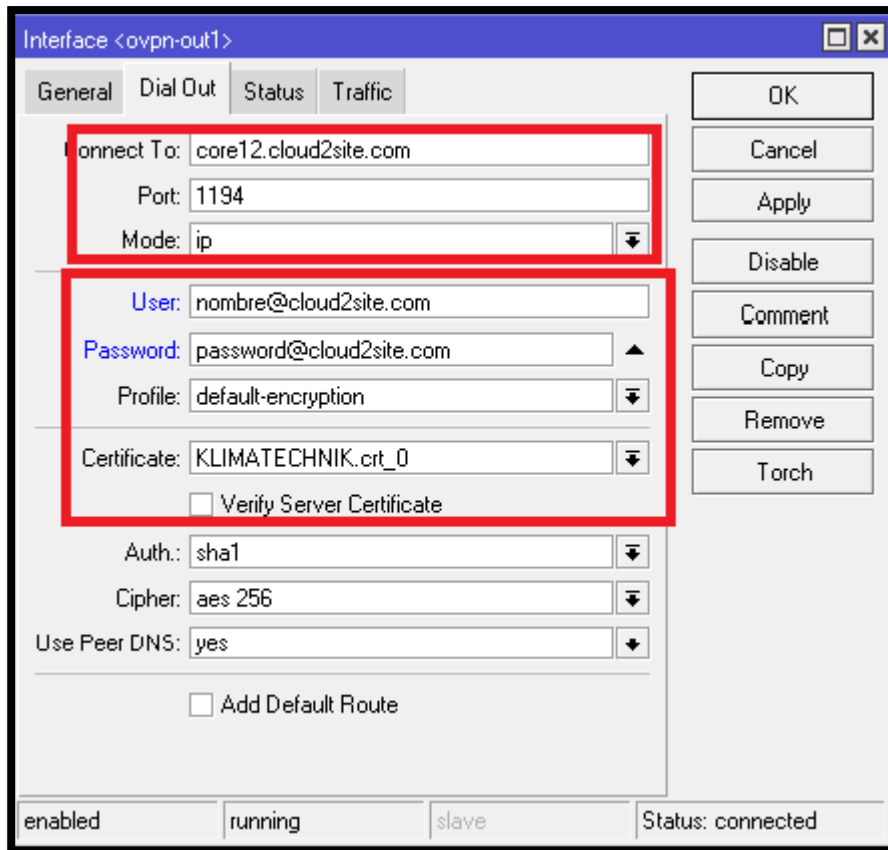


Figura 72: Configuración pestaña “Interfaces – ovpn-out1” – WINBOX

Fuente: Propia

- ❖ Se visualiza que ahora estamos usando el “Dominio Nube VPN” indicado en el ejemplo como “core12.cloud2site.com”, el cual será nuestro enlace de conexión para realizar configuraciones de VPN Tipo Acceso Remoto o Tipo Sitio a Sitio, sustituyendo así la Ip Publica Estática.

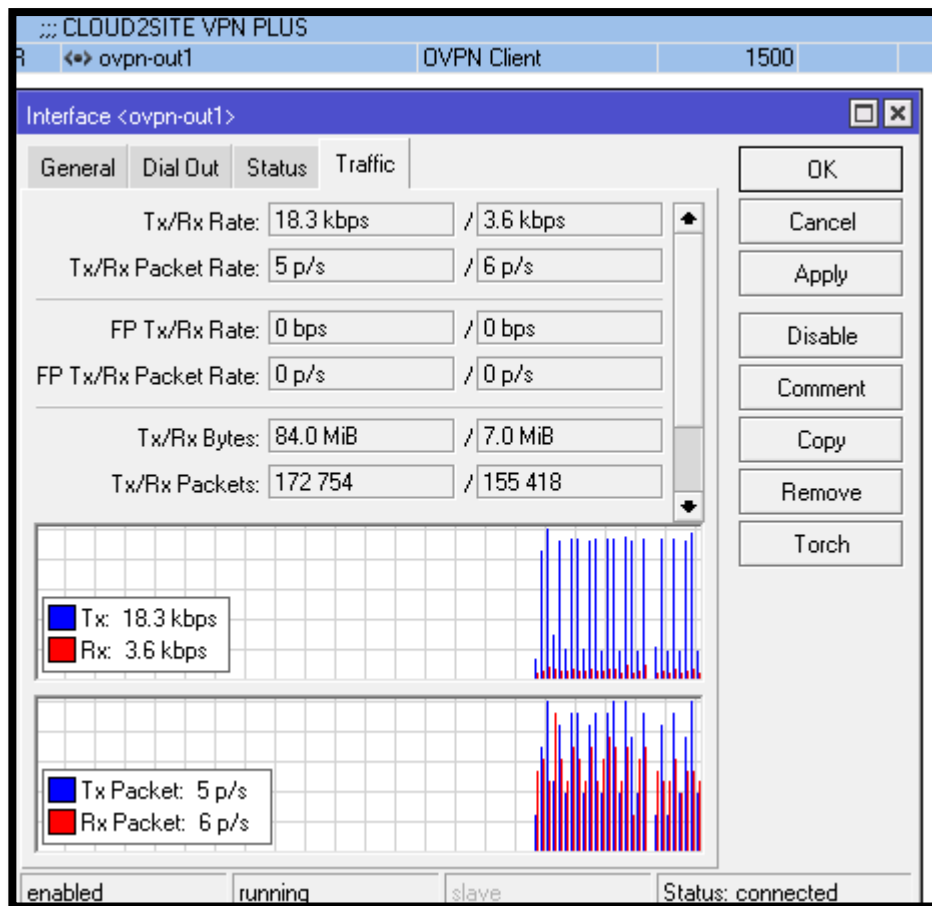


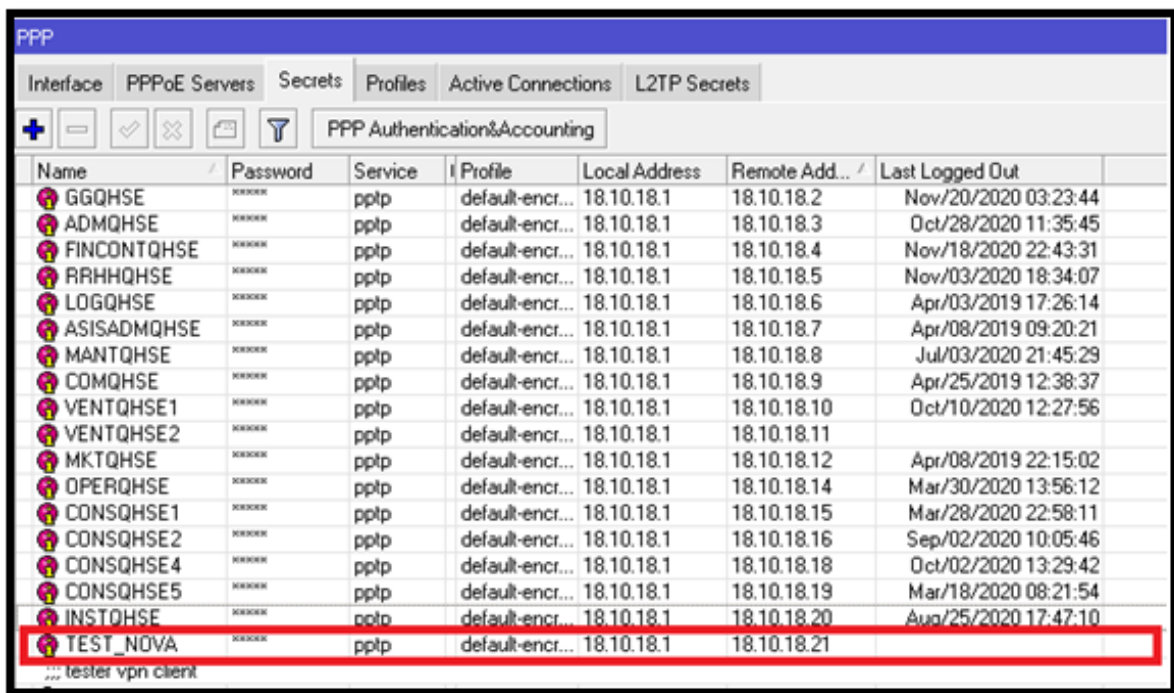
Figura 73: Trafico sobre la “ovpn-out1” configurada con el dominio “core12.cloud2site.com” – WINBOX

Fuente: Propia

ANEXO B: Pruebas realizadas en el RB Mikrotik – Q. H. S. E.

Se procede a realizar las pruebas de conectividad usando el comando “**ping**” y el comando “**tracert**”, pero antes de ello se valida lo siguiente:

- Se utilizará el usuario **TEST_NOVA**, creado previamente dentro de la pestaña “**PPP- secrets**” dentro del RB Mikrotik implementando en la Organización Q. H. S. E.



Name	Password	Service	Profile	Local Address	Remote Add...	Last Logged Out
GGQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.2	Nov/20/2020 03:23:44
ADMQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.3	Oct/28/2020 11:35:45
FINCONTQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.4	Nov/18/2020 22:43:31
RRHHQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.5	Nov/03/2020 18:34:07
LOGQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.6	Apr/03/2019 17:26:14
ASISADMQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.7	Apr/08/2019 09:20:21
MANTQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.8	Jul/03/2020 21:45:29
COMQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.9	Apr/25/2019 12:38:37
VENTQHSE1	*****	pptp	default-encr...	18.10.18.1	18.10.18.10	Oct/10/2020 12:27:56
VENTQHSE2	*****	pptp	default-encr...	18.10.18.1	18.10.18.11	
MKTQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.12	Apr/08/2019 22:15:02
OPERQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.14	Mar/30/2020 13:56:12
CONSQHSE1	*****	pptp	default-encr...	18.10.18.1	18.10.18.15	Mar/28/2020 22:58:11
CONSQHSE2	*****	pptp	default-encr...	18.10.18.1	18.10.18.16	Sep/02/2020 10:05:46
CONSQHSE4	*****	pptp	default-encr...	18.10.18.1	18.10.18.18	Oct/02/2020 13:29:42
CONSQHSE5	*****	pptp	default-encr...	18.10.18.1	18.10.18.19	Mar/18/2020 08:21:54
INSTQHSE	*****	pptp	default-encr...	18.10.18.1	18.10.18.20	Aug/25/2020 17:47:10
TEST_NOVA	*****	pptp	default-encr...	18.10.18.1	18.10.18.21	

Figura 74: “**PPP- secrets**” dentro del RB Mikrotik Q. H. S. E. - WINBOX

Fuente: Propia

- Tenemos en cuenta que la IP WAN está configurada en el RB Mikrotik Q. H. S. E. es **192.168.83.254**.

	Address	Network	Interface
D	63.10.63.8/24	63.10.63.0	ovpn-out1
	192.168.0.1/24	192.168.0.0	LAN
	192.168.10.1/24	192.168.10.0	DMZ
	192.168.83.254/24	192.168.83.0	WAN

Figura 75: Dirección IP - WAN RB Mikrotik Q. H. S. E - WINBOX

Fuente: Propia

- Tenemos en cuenta que la IP LAN, configurada en el equipo del Usuario Remoto es **192.168.43.78**.

Propiedad	Valor
Sufijo DNS específico p...	
Descripción	Realtek RTL8822BE 802.11ac PCIe Ada
Dirección física	54-13-79-4A-59-2F
Habilitado para DHCP	Sí
Dirección IPv4	192.168.43.78
Máscara de subred IPv4	255.255.255.0
Concesión obtenida	viernes, 20 de noviembre de 2020 21:27:
La concesión expira	viernes, 20 de noviembre de 2020 23:27:
Puerta de enlace predet...	192.168.43.1
Servidor DHCP IPv4	192.168.43.1
Servidor DNS IPv4	192.168.43.1
Servidor WINS IPv4	
Habilitado para NetBios ...	Sí
Vínculo: dirección IPv6 l...	fe80::383b:e8ce:d51a:d620%4
Puerta de enlace predet...	
Servidor DNS IPv6	

Figura 76: Dirección IP - LAN Usuario remoto - WINDOWS 10

Fuente: Propia

- Se realiza configuración de conexión VPN, en el equipo del usuario remoto.

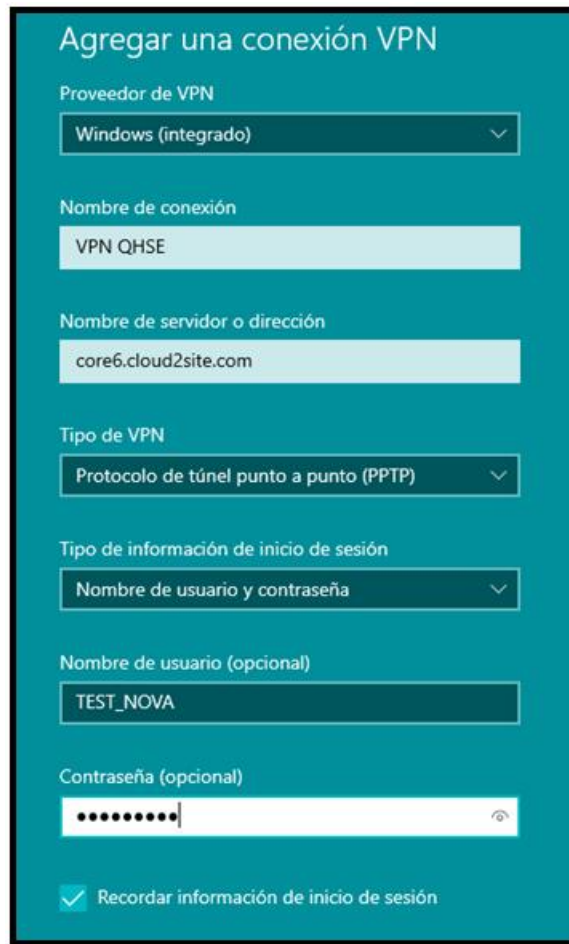


Figura 77: Agregar conexión VPN en equipo Usuario - WINDOWS 10

Fuente: Propia

- Se verifica conexión VPN QHSE en equipo de Usuario remoto.

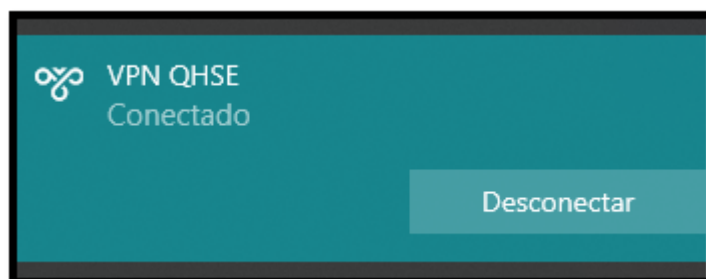


Figura 78: Agregar conexión VPN en equipo Usuario - WINDOWS 10

Fuente: Propia

- PING: Usuario Remoto (Hogar del Colaborador) a Puerto WAN del RB Mikrotik (SEDE Q. H. S. E.)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.18363.1198]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\NOVA ping -t 192.168.83.254

Haciendo ping a 192.168.83.254 con 32 bytes de datos:
Respuesta desde 192.168.83.254: bytes=32 tiempo=1029ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=444ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=454ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=655ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=520ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=672ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=566ms TTL=64
Respuesta desde 192.168.83.254: bytes=32 tiempo=367ms TTL=64

Estadísticas de ping para 192.168.83.254:
    Paquetes: enviados = 8, recibidos = 8, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 367ms, Máximo = 1029ms, Media = 588ms
Control-C
^C
C:\Users\NOVA>
```

Figura 79: CMD - PING - WINDOWS 10

Fuente: Propia

- TRACERT: Usuario Remoto (Hogar del Colaborador) a Puerto WAN del RB Mikrotik (SEDE Q. H. S. E.)

```
C:\Users\NOVA>tracert 192.168.83.254

Traza a 192.168.83.254 sobre caminos de 30 saltos como máximo.

 1  547 ms  654 ms  621 ms  192.168.83.254

Traza completa.
C:\Users\NOVA>
```

Figura 80: CMD - TRACERT - WINDOWS 10

Fuente: Propia

- Se visualiza la conexión entre Usuario Remoto (Hogar del Colaborador) y Puerto WAN del RB Mikrotik (SEDE Q. H. S. E.)

Address	Network	Interface
18.10.18.1	18.10.18.21	<pptp-TEST NOVA>
63.10.63.8/24	63.10.63.0	ovpn-out1
192.168.0.1/24	192.168.0.0	LAN
192.168.10.1/24	192.168.10.0	DMZ
192.168.83.254/24	192.168.83.0	WAN

Figura 81: Lista de direcciones - Conectividad de usuario TEST NOVA- WINBOX
Fuente: Propia

ANEXO C: Especificaciones MIKROTIK RB750R2

Details	
Product code	RB750r2
Architecture	MIPSBE
CPU	OCA9533
CPU core count	1
CPU nominal frequency	850 MHz
Dimensions	113x89x28mm. Weight without packaging and cables: 129g
License level	4
Operating System	RouterOS
Size of RAM	64 MB
Storage size	16 MB
Storage type	FLASH
Tested ambient temperature	-20C to +70C

Figura 82: - Detalles - MIKROTIK RB750R2

Fuente: Mikrotik RouterOS

Powering	
Details	
Max Power consumption	2W
PoE in	Passive PoE
PoE in input Voltage	6-30 V
Number of DC inputs	2 (DC jack, PoE-IN)
DC jack input Voltage	6-30 V

Figura 83: Potenciado de consumo - MIKROTIK RB750R2

Fuente: Mikrotik RouterOS

Ethernet	
Details	
10/100 Ethernet ports	5

Figura 84: Velocidad de puertos de interfaz - MIKROTIK RB750R2

Fuente: Mikrotik RouterOS

ANEXO D: Especificaciones MIKROTIK RB450GX4

RB450Gx4

The RB450Gx4 is an Ethernet router with five Gigabit Ethernet ports, a serial port, 512 MB NAND memory and a microSD card slot. In addition, it supports full 10 V - 57 V input by two power jacks or PoE (802.3af/ at or passive PoE) and can provide PoE output for Ethernet port #5.

It is powered by MikroTik RouterOS. It comes without an enclosure, you are free to use it in your own. The device form factor is identical to our previous RB850 and RB450 series, so you can even use the same enclosures.

The device is powered by a quad core ARM CPU, has 1 GB of RAM and supports hardware IPsec encryption. The device is powered by RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router, firewall or bandwidth manager.

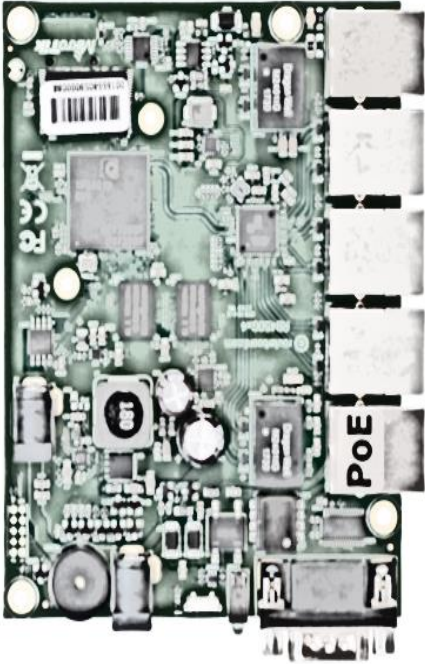


Figura 85: MIKROTIK RB450GX4

Fuente: Mikrotik RouterOS

Specifications

Product code	RB450Gx4
CPU	IPO-4019
CPU nominal frequency	716 MHz
CPU core count	4
Size of RAM	1 GB
Storage	2 MB Flash, 512 MB NAND
10/100/1000 Ethernet ports	5
PoE-in	802.3af/at
PoE-out	Passive PoE
MicroSD slots	1
Serial port	RS232
Supported input voltage	10 - 57 V (two DC jacks), 12 - 57 V (PoE-in)
Dimensions	90 x 115 mm
Operating temperature	-40°C .. +70°C tested
License level	5
Operating System	RouterOS
Max Power consumption	5 W

Figura 86: MIKROTIK RB450GX4 Especificaciones

Fuente: Mikrotik RouterOS