NOMBRE DEL TRABAJO

DISEÑO E IMPLEMENTACIÓN DE UN SIS TEMA DE ACCESO SEGURO A INTERNET Y ENLACE DE DATOS CON ALTA DISPON I

AUTOR

CEBRIAN HERNANDEZ MARX WILIAMS

RECUENTO DE PALABRAS

13064 Words

RECUENTO DE CARACTERES

74138 Characters

RECUENTO DE PÁGINAS

85 Pages

TAMAÑO DEL ARCHIVO

2.6MB

FECHA DE ENTREGA

Apr 11, 2024 8:35 AM GMT-5

FECHA DEL INFORME

Apr 11, 2024 8:36 AM GMT-5

11% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 11% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ACCESO SEGURO A INTERNET Y ENLACE DE DATOS CON ALTA DISPONIBILIDAD MEDIANTE LOS PROTOCOLOS BGP Y VRRP PARA UNA ENTIDAD BANCARIA”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRONICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER:

MARX WILIAMS CEBRIAN HERNANDEZ

ORCID: 0009-0006-5806-5730

ASESOR:

JORGE LUIS LOPEZ CORDOVA

ORCID: 0000-0002-3817-6859

Villa el Salvador, 2023

DEDICATORIA

Dedico este trabajo a mis padres, por su apoyo incondicional, su perseverancia y por motivarme a ser mejor persona cada día.

A mi hija y a mi esposa, por ser mi soporte y fuente de inspiración en mi vida profesional y personal.

A mis hermanos, por brindarme la confianza e impulso de ser para ellos un ejemplo de superación.

AGRADECIMIENTO

A Dios y mi hermano que siempre me están guiando y cuidando.

A mis padres, les estoy completamente agradecido, por su amor incondicional y su constante esfuerzo. ¡Los amo viejitos!

A mi hija y a mi esposa, por ser el motivo de mi felicidad.

A mi asesor, Jorge López, por la orientación y paciencia a lo largo del desarrollo del presente trabajo.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El presente trabajo de suficiencia profesional titulado “Diseño e implementación de un sistema de acceso seguro a internet y enlace de datos mediante los protocolos BGP y VRRP para una entidad bancaria”. Realizado en la empresa WIN EMPRESAS, en el área de TST (Telecom Specialist Team).

Actualmente, la entidad bancaria cuenta con una agencia en Lima que cumple el rol de agencia principal, adicional a ello, la entidad bancaria cuenta con tres agencias remotas tanto en Lima como en Cañete. Estas agencias remotas se interconectan con la agencia principal a través de un proveedor de servicios TDP (Telefónica del Perú)

WIN EMPRESAS propone el servicio de Internet con seguridad en la nube y enlace de Datos con conexión dedicada y overbooking 1:1 para la agencia principal y las tres agencias remotas de la entidad bancaria, manteniendo la misma topología de red, el cual se otorga a través de un enlace cuyo medio será fibra óptica.

El proyecto consta de migrar los servicios actuales que ofrece TDP a WIN EMPRESAS empleando protocolos de enrutamiento dinámico BGP a nivel WAN (red de área extensa). y VRRP a nivel LAN para conmutación automática de los servicios bajo el escenario de presentarse una avería en el enlace principal.

Se espera del proyecto mejorar la disponibilidad y confiabilidad y seguridad del servicio en las agencias de la entidad bancaria, a través de una topología de red basada en alta disponibilidad.

INTRODUCCIÓN

El medio físico en las Telecomunicaciones como la Fibra óptica son susceptibles a cortes por factores climático, fauna silvestre y vandalismo como robo de este confundiendo por cable de cobre. En consecuencia, afecta la disponibilidad de los servicios de telecomunicaciones.

La entidad bancaria al contar con un proveedor de servicio sin redundancia de enlace para interconexión de sus agencias es vulnerable a un punto único de falla que al presentar una avería sea en el medio físico del enlace o en el equipamiento de comunicaciones causaría una indisponibilidad de servicio.

Este proyecto se basa en el diseño e implementación de una topología de red redundante capaz de ofrecer una alta disponibilidad a través de la red MPLS de WIN EMPRESAS, El servicio de Internet seguro e interconexión de agencias se brindará a través de enlaces y equipos dedicados o compartidos en arquitectura multiservicios en Fibra Óptica desde un nodo de acceso de la red Backbone de WIN EMPRESAS hasta la agencia del cliente.

WIN EMPRESAS a través de su red BACKBONE brindara interconectividad entre las agencias remotas y la agencia principal ubicados en el centro de datos (data center), las agencias remotas saldrán a internet a través del enlace de datos, la alta disponibilidad se basa en mantener el servicio operativo por uno de los enlaces con conmutación automática.

El Internet Seguro consta de crear una VDOM (Instancia o cortafuego virtual de la marca Fortinet) en la backbone de Win empresas, los enrutadores dedicados para el servicio de internet tendrán conectividad a esta instancia virtual, de esta forma la navegación de los host o terminales internos de entidad bancaria serán seguros.

CAPÍTULO I. ASPECTOS GENERALES

1.1 Contexto

WIN Empresas cuenta con una topología de red mixta en malla o mesh y en anillo redundante, el cual permite tener más de un enlace de contingencia entre nuestros nodos por el cual redundar en caso fortuito de que alguna conexión caiga o se corte, lo que asegura el servicio brindado a nuestros clientes. así también, equipos de transmisión que soportan enlaces Gigabit Ethernet para brindar conexiones rápidas. Mediante el uso del encapsulamiento 802.1q, a través de vlans, aseguramos la independencia y seguridad de la señal de cada uno de nuestros usuarios.

La misión de la empresa es Impulsar el progreso de las empresas en el Perú a través del acceso a nuevas tecnologías, y como visión ser la empresa tecnológica más confiable y respetada del Perú. Convirtiéndonos en el referente local en innovación para empresas en sector gobierno y privado. (Win empresas, 2023)

Los Servicios de Win empresas cuenta con el un alto portafolio que impulsan la transformación digital, una de ellas es la conectividad a internet, telefonía con centrales físicas y virtuales, asimismo, se ofrece seguridad gestionada como es la seguridad perimetral, seguridad en la nube y ciberseguridad.

1.2 Delimitación temporal y espacial del trabajo

1.2.1 Delimitación Espacial

La implementación del servicio se dará en las siguientes agencias:

- Agencia principal: Av. Juan Pablo S/N, Callao, Callao, Lima.
- Agencia remota 1: Av. Sáenz Peña S/M, Callao, Callao, Lima.
- Agencia remota 2: Jr. Antonio Miró Quesada S/N, Callao, Callao, Lima.
- Agencia remota 3: Av. Mariscal Benavides S/N, San Vicente de Cañete, Cañete, Lima.

1.2.2 Delimitación Temporal

Las fases del proyecto conforman levantamiento de información, diseño, implementación de configuración y pruebas de redundancia.

Fecha de inicio: 07/08/2023

Fecha de Fin: 30/09/2023

1.3 Objetivos

1.3.1 Objetivos General

Diseñar e implementar un sistema de acceso seguro a internet y enlace de datos con alta disponibilidad, mediante los protocolos BGP y VRRP para una entidad bancaria.

1.3.2 Objetivos específicos

- Diseñar un sistema de alta disponibilidad para interconexión de agencias y navegación a internet.
- Implementar la configuración de los equipos de red para interconectar las agencias y el Firewall.
- Implementar la configuración de firewall para la navegación a internet.
- Validar la conmutación automática de los servicios simulando caída del enlace principal a nivel WAN.
- Validar la limitación hacia destinos maliciosos a través del internet seguro.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes

Se ha realizado un análisis de varios trabajos relacionados con la solución propuesta para este proyecto, llegando a conclusiones relacionadas con el objetivo del proyecto.

2.1.1 Antecedentes Nacionales

Ciriaco (2021) en su tesis titulada “Optimización del servicio de red con respaldo del enlace a internet WAN y la seguridad perimetral para la empresa Sonepar sede lima” UNTELS. Diseña e implementa una solución de navegación con respaldo a nivel de interproveedor a través de un equipo balanceador de la marca Fortinet, adicional a ello, implementa un sistema de seguridad perimetral con otro equipo físico de la marca Fortinet con la intención de que los dispositivos de la empresa sonepar naveguen con seguridad, el aporte a mi trabajo de investigación se basa en los mecanismos que uso como configuración de filtros web, IPS y políticas de navegación estrictas para limitar destinos con riesgo alto.

Perez (2023) en su tesis titulada “Solución Integral de networking y seguridad en alta disponibilidad en Zegel Ipae año 2020” Universidad Nacional San Ignacio de Loyola. Aborda la problemática que la institución ZEGEL IPAE maneja un modelo convencional de su red interna, por lo tanto, plantea una topología de red redundante. Realizó una solución integral con la intención de que ZEGEL IPAE migre sus servicios a un proveedor con una arquitectura MPLS para la interconexión de sus sedes. El aporte a mi trabajo de suficiencia profesional consta del uso de protocolos BGP y VRRP para diseñar una topología de red redundante con conmutación automática de enlace.

Ramírez (2011) en su proyecto de tesis titulado: “Diseño de la solución de seguridad y administración de tráfico wan del enlace de internet dedicado con alta disponibilidad para un campus universitario” UNI, Lima. Propone optimizar la navegación a internet en un campus universitario diseñando una solución administrativa y segura en la red WAN.

El objetivo es satisfacer las necesidades de los clientes de velocidad de internet de alta calidad y protección del servicio de información. El siguiente trabajo aporte a mi proyecto una perspectiva de como beneficiar a los usuarios con calidad de navegación a internet y respaldo ante una caída.

2.1.2 Antecedentes Internacionales

Benavides, E. y Olaya, D. (2018) en su proyecto de posgrado "Diseño de un plan de contingencia para un enlace crítico del banco financorp", utilizaron un mecanismo virtual configurado llamado HSRP para respaldar los enlaces de internet del banco, tanto el principal como el backup. Esta metodología hará que ambos enrutadores trabajen como un solo enrutador. Nuestro trabajo de suficiencia se beneficia de la demostración respaldando la navegación a internet enfocado en una sede corporativa.

Muñoz (2019) en su tesis titulada “Protocolo de enrutamiento dinámico BGP en redes de alta disponibilidad” Instituto Politécnico Nacional, México. Propone en sus tesis implementar BGP como protocolo de puerta de enlace en su enrutador perimetral para tener salida a Internet a través de un ISP con alta disponibilidad, este trabajo aporta con la toma de decisión en la aplicación de filtros BGP como es prefix list y route-map aplicando buenas prácticas para el anuncio o recepción de prefijos de red para evitar problemas de enrutamiento por error humano.

Mullo (2019) en su artículo titulado “Firewall para la seguridad de la red en los laboratorios de la universidad estatal de bolívar” UNIANDES, ecuador. Realiza una investigación sobre la seguridad de red en la universidad de Bolivar, hallando déficit en la seguridad de la información sin políticas de restricción y firmware desactualizado en el firewall actual, el aporte que genera a mi trabajo es la propuesta de implementación de un firewall más robusto con políticas de navegación bajo filtros de tipo WEB-HTTPS, filtrado SPAM e IPS aplicados en las políticas de mi proyecto.

2.2 Bases teóricas

2.2.1. Topología de Redes

Las diferentes topologías que detallaré a continuación indican la forma en la que se interconectan los dispositivos y/o componentes de red en capa 1. Dordoigne (2006)

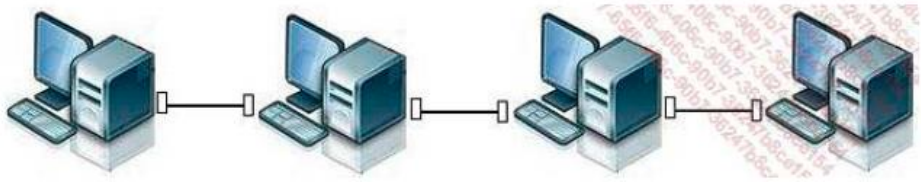
2.2.1.1. En bus

Topología en Bus (soporte lineal) se basa en un cableado como único elemento que constituye la red que conectan nodos (periféricos, puestos de trabajo y equipos de interconexión) el problema principal se dará cuando exista un corte en el cable lo cual afectaría el intercambio de información en toda la red. Dordoigne (2006).

En la Figura 1, se muestra la Conexión de periféricos sobre una misma línea de comunicación.

Figura 1

Topología de red en bus



Nota. Tomado de Redes informáticas. (p. 144), por Dordoigne, J (2006). Editions ENI.

2.2.1.2. En estrella

La topología en estrella se basa en componentes activos, las señales son regeneradas y restablecidas por el componente activo o llamado hubs teniendo la capacidad de crear una estructura jerárquica limitada. Dordoigne (2006).

En la Figura 2, se verifica la Conexión centralizada de periféricos con un conmutador.

Figura 2

Topología de red en estrella

Nota. Tomado de Redes informáticas. (p. 144), por Dordoigne, J (2006). Editions ENI.

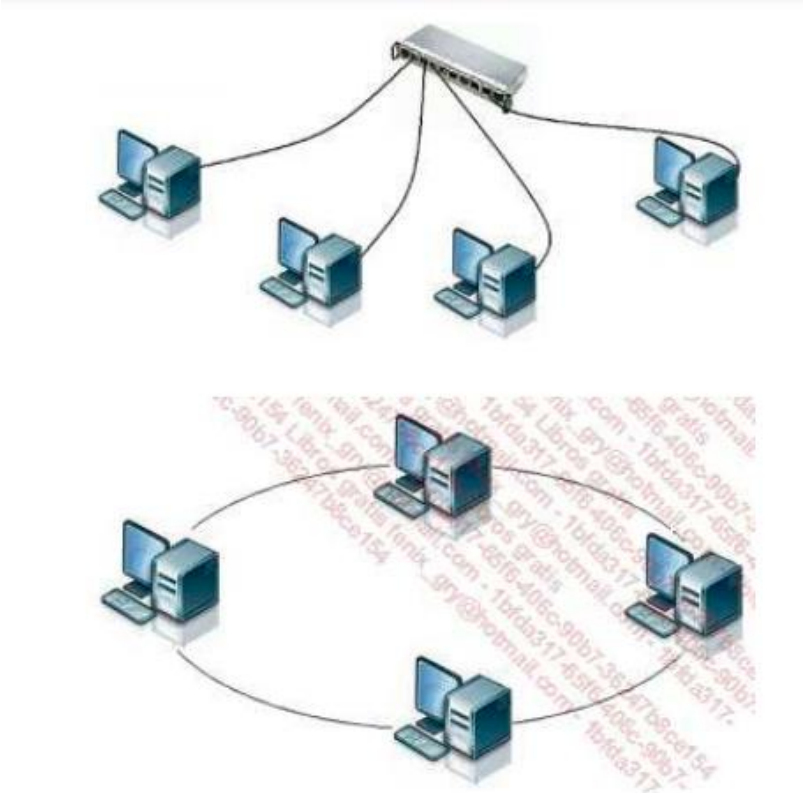
2.2.1.3. En anillo

Esta topología se basa en un anillo o bucle cerrado que incluye conexiones punto a punto entre los dispositivos. Cada nodo recibe tramas, que actúan como un repetidor (elemento activo). Los equipos se pueden conectar a la red mediante hubs en anillo. Contienen dos conectores macho/hembra llamados R/I (Ring In) y R/O (Ring Out) para realizar bucles entre elementos, además de puertos. Permite conectar cables de cobre (RJ45) o fibra. Dordoigne (2006)

En la Figura 3, apreciamos la Conexión de periféricos sobre varias líneas de comunicación.

Figura 3

Topología de red en anillo



Nota. Tomado de Redes informáticas. (p. 145), por Dordoigne, J (2006). Editions ENI.

2.2.1.4. En malla

Según su definición, es una topología de red en la que cada dispositivo de red se conecta directamente a varios otros dispositivos, lo que crea una red en la que la información puede fluir por varias rutas. Esta es especialmente útil en entornos donde la conectividad puede ser intermitente o inestable, como en el caso de organizaciones humanitarias que trabajan en áreas remotas o en situaciones de emergencia. Una malla ofrece varias ventajas sobre otras topologías de red.

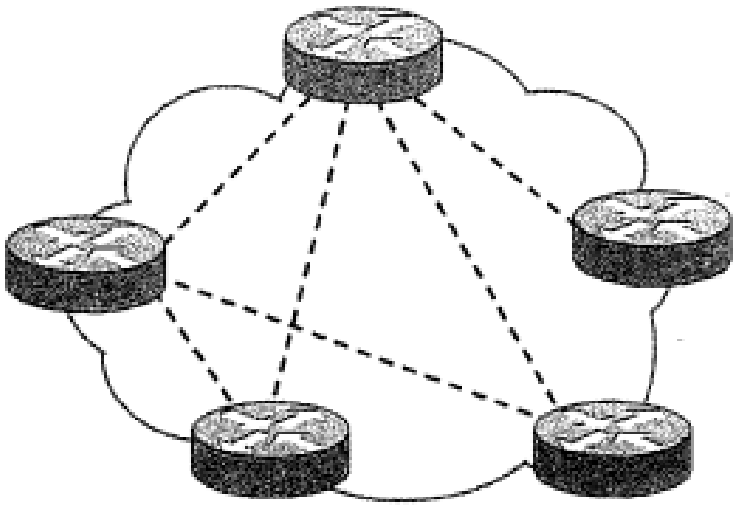
En primer lugar, el uso de enlaces dedicados evita que varios dispositivos compartan los enlaces, ya que cada conexión solo transmite la carga de datos de los dispositivos conectados.

En segundo lugar, la topología de malla es sólida. No inhabilita todo el sistema si falla un enlace. En tercer lugar, se encuentran los beneficios de la seguridad o la privacidad. Solo el destinatario adecuado puede ver un mensaje cuando pasa por una línea dedicada. Méndez (2010).

En la Figura 4, se muestra una interconexión física de enrutadores full mesh o todos contra todos.

Figura 4

Topología de red en malla



Nota. Tomado de Ariganello & Barrientos (2010)

2.2.1.5. LAN y WAN

Una red de área local (LAN) es una agrupación de dispositivos conectados en un lugar físico, como un edificio, una oficina o una casa. Una LAN puede ser pequeña o grande, desde una red doméstica con solo un usuario hasta una red comercial con miles de usuarios y dispositivos en una oficina o escuela. Una LAN no tiene tamaño porque conecta dispositivos en un área limitada.

WAN (Red de área amplia) es un conjunto de redes LAN u otro tipo de redes que se comuniquen entre sí, se le describe también como una red de redes siendo la internet la WAN más grande del mundo. Cisco. (2023).

2.2.2. Enrutamiento estático y dinámico

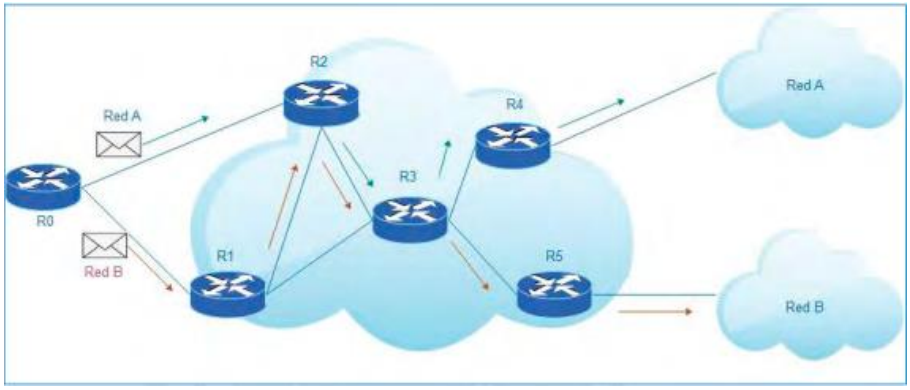
2.2.2.1 Algoritmos Dinámicos.

Cada protocolo de enrutamiento dinámico se basa en un algoritmo. El algoritmo describe la secuencia de acciones necesarias para resolver un problema. Un algoritmo de enrutamiento debe incluir al menos: cómo compartir información de rutas alcanzables con otros dispositivos, qué hacer con la información que proviene de otros enrutadores, cómo encontrar la ruta óptima y cómo reaccionar a los cambios en la topología de la red. (Paredes, 2021)

En la Figura 5, se muestra cómo el enrutador puede elegir el camino más optimo a través de la red, de acuerdo con la dirección destino (indicada en el encabezado del paquete), y luego lo envía al siguiente salto, que puede ser otro enrutador o, finalmente, el dispositivo destino. El enrutador crea una tabla de enrutamiento para que pueda listar todos los segmentos destino. Cada entrada de la tabla de enrutamiento contiene el segmento de destino, el protocolo, la distancia administrativa del protocolo, el costo del punto de vista del enrutador, el IP del siguiente salto y la interfaz de salida.

Figura 5

Enrutamiento de paquetes



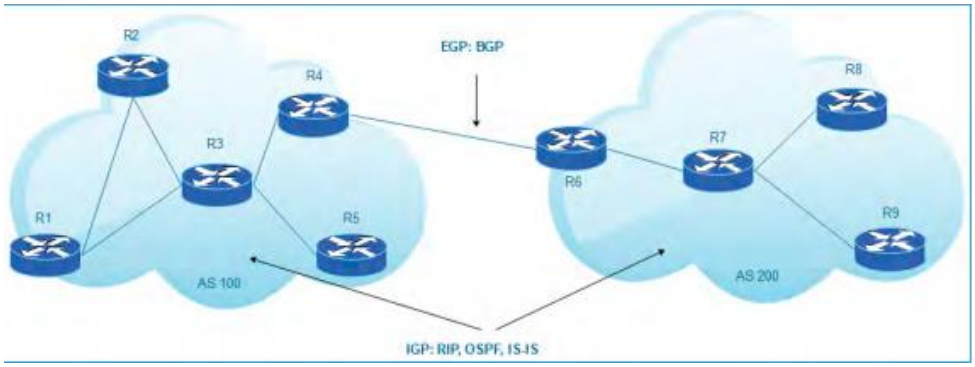
Nota. Tomado de Paredes (2021)

Los protocolos de enrutamiento se clasifican como interna (iBGP) o externa (eBGP), según el punto de vista del Sistema Autónomo (AS). El AS es un conjunto de enrutadores que están bajo una administración conjunta. Se pueden usar varios protocolos de enrutamiento en un AS. J.Moy (1998).

En la Figura 6, observamos dos sistemas autónomos AS100 y AS200. Para el intercambio de información de la tabla de rutas entre sistemas autónomos usamos eBGP para el caso de intercambio de información dentro de un mismo sistema autónomo usamos los protocolos: iBGP, RIP, OSPF e IS-IS

Figura 6

Clasificación por área de trabajo: IGP y EGP



Nota. Tomado de Paredes (2021).

2.2.2.2. Vector distancia.

Los algoritmos de enrutamiento por vector distancia hacen que cada enrutador registre en su tabla las siguientes entradas: una línea preferida de salida hacia ese destino y una estimación de tiempo o distancia a ese destino, usando métricas como cantidad de escalas, retardo de tiempo en milisegundos y número total de paquetes encolados por trayectoria. Un enrutador puede definir la mejor estimación y la línea correspondiente para su nueva tabla de enrutamiento y esta se intercambie con los vecinos. Goitia (2004).

2.2.2.3. Lista de prefijos (Prefix list)

Las listas de prefijos son listas simples que se utilizan para filtrar rutas basadas en un prefijo que consta de una dirección IPv4 o IPv6 y una máscara de red. Sin embargo, las listas de prefijos también usan configuraciones para especificar la longitud mínima (, mayor o igual) y máxima (, menor o igual) del prefijo que debe coincidir.

Por ejemplo, un prefijo 10.0.0.0/8 con ge16 coincidirá con cualquier prefijo en la red 10.0.0.0 con /8 o más; 10.10.0.0/16 coincidirá con cualquier prefijo en la red 10.10.0.0/12, pero no coincidirá con cualquier otro prefijo superior a /16 o inferior a /8. Fortinet (2023)

2.2.2.4. Mapas de ruta (Route-map)

Fortinet (2023) Los mapas de ruta son una herramienta útil para adaptar las acciones a protocolos de enrutamiento dinámicos a circunstancias particulares. Se usan principalmente en rutas BGP para manipular rutas anunciadas por FortiGate (ruta-map-out) o rutas recibidas de otros enrutadores BGP.

Un mapa de ruta puede tener múltiples reglas procesadas de arriba hacia abajo. Cada regla tiene una acción que permite o impide. Las reglas establecen normas para hacer coincidir una ruta en función de múltiples características o establecer características en función de una ruta coincidente.

2.2.2.5 BGP

Border Gateway Protocol (BGP) Los sistemas autónomos utilizan el protocolo de enrutamiento dinámico Border Gateway Protocol (BGP). Los proveedores de servicio de internet suelen usar BGP. En la actualidad se emplea la versión BGP-4, que cuenta con las siguientes características: Guedrez (2017).

- Al contrario de los protocolos IGP, como OSPF o IS-IS, BGP es del tipo EGP, el cual su objetivo es controlar y tamizar las mejores rutas entre Sistemas autónomos, más no en el descubrimiento o convergencia de la red.

- BGP utiliza protocolo de control de transmisiones (TCP) como protocolo de capa de transporte, lo que mejora en la continuidad ante posibles fallos.
- Los vecinos BGP deben estar conectados de forma lógica a través del protocolo TCP, utilizando el puerto destino 179.
- BGP es aplicado a intercambiar rutas de Internet, transmitiendo muchas rutas. Como resultado, BGP transmite únicamente las rutas actualizadas cuando hay un cambio en la red o una actualización de la ruta, lo que reduce el consumo de ancho de banda durante la distribución de rutas. Paredes (2021)

2.2.2.5.1 Estados de BGP

Idle: BGP espera una fase llamada start mientras busca los vecinos, esta fase es iniciada cuando se reinicia una sesión ya existente o cuando se está estableciendo una sesión BGP. Ariganello & Barrientos (2010)

Connect: BGP espera que se complete la conexión del protocolo de trasporte TCP a través del puerto 179, si este es satisfactorio cambia de estado a open sent de lo contrario cambiará a active. Ariganello & Barrientos (2010)

Active: Este estado indica que está intentando iniciar una sesión TCP, cuando el temporizador connect relay expira BGP lo reinicia y lo vuelve a estado connect. Si un enrutador permanece entre los estados connect y active revela que la conexión TCP no se puede establecer. Ariganello & Barrientos (2010)

Open sent: BGP espera los mensajes open del vecino, estos mensajes son chequeados para verificar que los datos, versiones y el número de sistema autónomo sean correctos. Ariganello & Barrientos (2010)

Open Confirm: BGP espera los mensajes de estado keepalive, si este mensaje es recibido entonces la sesión pasa al estado established. Ariganello & Barrientos (2010)

Established: Estado final y necesario donde BGP empieza a funcionar intercambiando rutas y mensajes de estado o keepalive. Ariganello & Barrientos (2010)

2.2.2.5.2 Modos de Operación de BGP

En la Figura 7, mostramos que iBGP se usa dentro del Sistema Autónomo y eBGP se usa entre Sistemas Autónomos diferentes.

Figura 7

Despliegue de IBGP vs EBGP

Nota. Tomado de Paredes (2021)

Un conjunto de parámetros que caracterizan una ruta BGP se conoce como atributos BGP. Estos recursos permiten la aplicación de filtros y selección de rutas.

2.2.2.6 VRRP

Ariganello & Barrientos (2010). (Virtual Enrutador Redundancy Protocol), protocolo estándar definido en la RFC 2338, con funcionamiento y configuración parecida al protocolo HSRP de Cisco, se detalla una breve comparativa:

- VRRP proporciona una IP redundante o flotante entre un grupo de enrutadores, se clasifican por prioridad, el Máster es aquel con mayor prioridad en el grupo en estado activo el resto se les denomina backup.
- El valor que se asigna a un enrutador está entre 1 y 254, siendo 254 el valor más alto y 100 un valor por defecto.
- Los grupos pueden tomar valores entre 0 y 255.

- El formato que tiene la dirección MAC es el siguiente 0000.5e00.01xx donde xx es el número del grupo en formato hexadecimal.
- Los mensajes Hello de VRRP son transmitidos cada 1 segundo.

En la Tabla 1, se muestra la sintaxis de comandos e interpretación para configurar el protocolo VRRP en un enrutador cisco.

Tabla 1

Tabla comandos protocolo VRRP.

Comando	interpretación
vrrp group priority level	Asignación de la prioridad:
vrrp group timers advertise [msec]	Cambio del intervalo del temporizador
vrrp group timers learn	Para aprender el intervalo desde el enrutador principal
vrrp group authentication string	Habilita la autenticación:
vrrp group ip ip-address [secondary]	Configura la IP virtual:

Nota. Adaptado de Redes Cisco CCNP a fondo (p.420) por, Ariganello & Barrientos, 2010, Alfaomega

2.2.3. Seguridad de Red

Refiere a los procedimientos, tecnologías y normativas usadas con la finalidad de proteger el tráfico de una red, activos contra los ciberataques, tipos de redes, accesos no autorizados y pérdida de la información. Un enfoque de capas debe ser utilizado para proteger la seguridad de la red, tanto adentro como fuera de los límites permitidos de la misma. Sin embargo, las vulnerabilidades que puede presentar una red se encuentran en diferentes lugares, desde los dispositivos hasta las aplicaciones. Por ello, existen varios tipos de herramientas para la seguridad de red, que tienen por objetivo tomar las amenazas individuales, analizarlas y mitigarlas. Fortinet (2023).

2.2.3.1 Beneficios de la seguridad de red

Una empresa puede obtener una variedad de beneficios al implementar la seguridad de la red. IsoTools (2021):

- Tener una red más estable y un menor número de interrupciones comerciales, servirán para aumentar la productividad.
- Las normativas aseguran que se cumplan la seguridad de la red.
- Reducir el riesgo de acciones legales como resultado de las medidas que toma la empresa ante la seguridad, demostrando atención y cuidado con los datos de los clientes.

2.2.3.2 Norma estándar de la seguridad de red: ISO/IEC 27033

El estándar de seguridad en redes se compone de siete partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de referencia de redes, protección de las comunicaciones entre redes mediante gateways, acceso remoto, protección de las comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. ISO 27000 (2005).

Los objetivos de la normativa son los siguientes:

- Brindar directrices para definir e investigar problemas de seguridad de la red, así como una ideas y necesidades de seguridad de la red de cara al futuro.
- Proporcionar pautas para crear diseños tecnológicos, así como factores de 8 controles relacionados con escenarios de red, diseño y escenarios de red típicos.
- Abordar de manera básica los problemas relacionados con las medidas de seguridad de las operaciones de red, incluida la instalación de dichos controles y la supervisión y evaluación de su eficacia.

2.2.3.3 Filtrado de Web

El servicio de filtrado web FortiGuard proporciona protección completa contra amenazas como ransomware, robo de credenciales, suplantación de identidad y otros ataques web. utiliza el análisis y correlación del comportamiento impulsado por IA para bloquear URL maliciosas desconocidas con casi cero falsos negativos.

El servicio utiliza la inteligencia de amenazas líder de FortiGuard Labs. FortiGuard Labs bloquea aproximadamente 66 millones de URL maliciosas/suplantaciones de identidad/correo no deseado a través de 307 millones de URL categorizadas. Para habilitar controles web granulares e informes, el servicio utiliza una base de datos que contiene cientos de millones de URL agrupados en más de noventa categorías. Además, soporta el tráfico cifrado, que incluye TLS 1.3, para permitir el cumplimiento y el uso aceptable. Fortinet (2023)

Las URL o páginas web se describen por tipo de categorías y estas pueden tener una acción, en la Tabla 2, estas acciones pueden ser permitidas o bloqueadas, una vez permitidas pueden ser configurados para notificación y monitoreo

Tabla 2

Tabla de acciones de filtros web.

Acción de filtro web FortiGuard	Descripción
Permitir	Permitir el acceso a los sitios de la categoría.
Monitor	Permitir y registrar el acceso a los sitios de la categoría. Se pueden habilitar cuotas de usuario para esta opción (consulte Cuota de uso).
Bloquear	Impedir el acceso a los sitios de la categoría. Los usuarios que intentan acceder a un sitio bloqueado ven un mensaje de reemplazo que indica que el sitio está bloqueado.
Advertencia	Mostrar un mensaje al usuario permitiéndole continuar si así lo desea.
Autenticar	Requerir que el usuario se autentique con FortiGate antes de permitir el acceso a la categoría o grupo de categorías.
Desactivar	Elimine la categoría del perfil del filtro web.

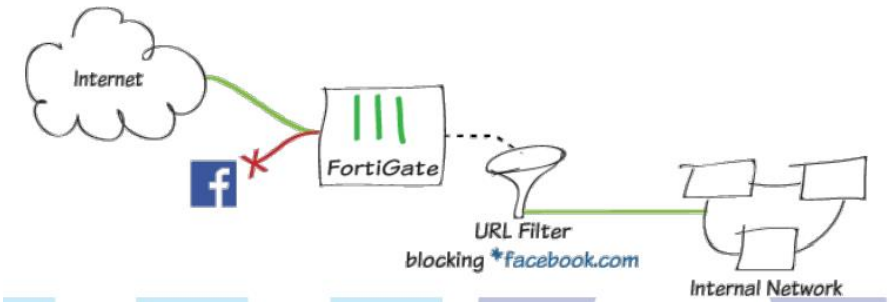
Nota. Adaptado de Fortinet (2023).

En la figura 8, El control de accesos a sitios web tiene la siguiente topología, toda consulta exterior primero consulta al equipo firewall fortigate, si la

categoría del filtro URL es permitido el firewall permitirá que resuelva la web destino, si la categoría es bloqueada no se tendrá respuesta de la URL.

Figura 8

Topología de filtros web en fortinet



Nota. Tomado de Fortinet (2023).

2.2.3.3 Prevención de intrusos (IPS)

El servicio FortiGuard IPS impulsado por IA/ML proporciona inteligencia casi en tiempo real con miles de reglas de prevención de intrusiones para detectar y bloquear amenazas conocidas y sospechosas antes de que lleguen a sus dispositivos. Integrado de forma nativa en todo Fortinet Security Fabric, el servicio FortiGuard IPS ofrece rendimiento y eficiencia de IPS líder en la industria mientras crea una respuesta de red coordinada en toda su infraestructura más amplia de Fortinet. Fortinet (2023).

IPS Fortiguard con NGFT ofrece lo siguiente:

- Aplicación de parches virtuales basada en red para aplicaciones comerciales con parches difíciles o imposibles. Esto garantiza que las vulnerabilidades se protejan sin interrumpir las operaciones.
- Para ofrecer el mejor precio y rendimiento de IPS de la industria, el procesador de contenido FortiGuard, diseñado especialmente por Fortinet (CP9) en FortiGate, aceleró las capacidades de IPS FortiGuard.
- IPS se ha ampliado con funciones adicionales, como la inspección de SSL (incluido TLS 1.3) para identificar malware oculto, ransomware y otros ataques que se propagan a través de HTTPS.

- Novedades en el IPS dedicado: actualizaciones de extremo a extremo para la gestión del IPS dedicado, destinadas a finanzas y otras implementaciones reguladas, permiten la migración de hardware independiente a NGFW mientras se mantienen las operaciones y las prácticas de cumplimiento.

2.3 Definición de términos básicos

Backbone: En ingles significa columna vertebral, también llamado red troncal es aquella que conecta gran cantidad de enrutadores entre si, Esto puede conectar sedes de organizaciones, edificios gubernamentales, universidades, etc. Pero también ir mucho más allá y poder conectar países o incluso continentes. Genez (2020)

EBGP: El protocolo de enrutamiento BGP externo (EBGP) se utiliza para intercambiar información entre sistemas o redes autónomos en Internet. Este protocolo es utilizado para optimizar la ruta hacia destinos exteriores garantizando que los paquetes se entreguen de forma eficiente de un sistema autónomo a otro. OrhanErgun (2023)

IBGP: El protocolo de puerta de enlace de frontera interna (IBGP) permite que los enrutadores dentro del mismo sistema autónomo intercambien información de rutas, de esta forma elegirán la mejor manera de enrutar el tráfico internamente garantizando que los enrutadores internos tengan la misma vista de la topología de la red y puedan tomar decisiones de enrutamiento óptimas. OrhanErgun (2023)

MPLS: MPLS es simplemente un mecanismo para cambiar de tráfico. Los dispositivos MPLS solo miran las etiquetas en lugar de la cabecera de capa 3, lo que los hace independientes de los protocolos de capa 3. Se examina la etiqueta de un paquete de entrada y se compara con la base de datos de etiquetas. Se le asigna una nueva etiqueta al paquete basándose en los datos de la tabla para que sea enviado fuera de la interfaz adecuada. Ariganello & Barrientos (2010)

NGFW: NGFW por sus siglas en inglés significa Firewall de nueva generación, a diferencia de un firewall estándar que tiene la misma funcionalidad de crear políticas para bloquear tráfico potencialmente peligroso, los firewalls de nueva generación realizan inspección de tráfico más específico y pueden detectar amenazas por filtrado de paquete. Fortinet (2023).

Overbooking 1:1: Se utiliza overbooking en telecomunicaciones para aprovechar el máximo del ancho de banda, por ejemplo, Cuando un usuario "navega", no utiliza constantemente el canal porque una vez cargado el sitio, el enlace queda sin uso. Este tiempo sin uso puede ser utilizado por otro cliente para racionalizar el overbooking, en un servicio dedicado no existe racionalización entre clientes. Aliaga (2019)

Ping: El comando ping o traceroute es un método común utilizado para resolver problemas de acceso entre hosts o equipos de comunicaciones, envía una serie de mensajes eco del protocolo ICMP (Internet Control Message Protocol) a una dirección y luego espera una respuesta.

Esta prueba es exitosa si el mensaje de eco llega al destino y el destino puede obtener una respuesta de eco de regreso al origen dentro de un tiempo predeterminado llamado tiempo de espera agotado. Cisco (2023).

Ransomware: ESET (2023). En su blog define como tipo de software malicioso que se utiliza para la extorsión. El malware bloquea la pantalla o cifra la información del disco cuando un dispositivo es atacado con éxito, y se solicita un rescate a la víctima con los detalles para efectuar el pago.

Los creadores de ransomware emplean varias estrategias:

- El codificador de disco ransomware cifra todo el disco e impide que el usuario acceda al sistema operativo.
- El bloqueador de pantalla bloquea el acceso a la pantalla del dispositivo.
- El ransomware criptográfico cifra los datos del disco duro de la víctima.
- El bloqueador de PIN ataca los dispositivos Android y cambia los códigos de acceso para que los usuarios sean eliminados.

Sistemas Autónomo: Un Sistema Autónomo (AS) es un conjunto de redes de direcciones IP administradas por uno o más operadores de red con una política de ruteo única. Cada Sistema Autónomo tiene un número asociado que se utiliza como identificador cuando se comparte información de ruteo externo. Los sistemas autónomos comparten información de ruteo utilizando protocolos de ruteo externos como BGP. Lacnic (2023).

Traza: El comando traceroute se usa para identificar las rutas que realmente toman los paquetes cuando viajan a su destino. El dispositivo, como un enrutador o una PC, envía una secuencia de datagramas del Protocolo de datagrama de usuario (UDP) a una dirección de puerto no válida en el host remoto.

Se envían tres datagramas, cada uno de los cuales tiene un valor de campo de tiempo de vida (TTL) establecido. Tan pronto como llegue al primer router en la trayectoria, el datagrama entra en "tiempo de espera" con un valor TTL de 1. El router responde con un mensaje de tiempo excedido (TEM) ICMP que indica que el datagrama ha caducado. Cisco (2023).

VDOM: Fortigate (2023). Un FortiGate se divide en dos o más unidades virtuales que funcionan de forma independiente mediante el uso de dominios virtuales (VDOM). Los VDOM pueden proporcionar políticas de seguridad independientes y configuraciones de enrutamiento y servicios VPN completamente separadas para cada red conectada en modo NAT.

En el modo multi VDOM, se pueden crear y administrar múltiples VDOM como unidades independientes. La mayoría de las unidades FortiGate admiten 10 VDOM de forma predeterminada, y muchos modelos permiten la compra de una clave de licencia para aumentar el número máximo. Pueden existir ciertas excepciones.

CAPÍTULO III: DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y análisis del problema

En este capítulo se describe las problemáticas y solución del proyecto.

3.1.1 Definición del problema

La entidad bancaria con su proveedor actual no cuenta con redundancia de enlace tanto para su servicio de internet como la interconexión de agencias, por lo cual estas agencias no presentan confiabilidad en la continuidad de sus servicios, una avería en el medio físico como es la fibra óptica o una falla en los equipos de comunicaciones causaría la indisponibilidad en las agencias remotas paralizando las operaciones lo cual involucra pérdidas económicas a gran escala.

Por otro lado, la entidad bancaria no cuenta con un firewall para hacer frente a amenazas de tipo ransonware (software malicioso), robo de credenciales y otro tipo de ataques que provienen de la web. Por lo tanto, son susceptibles a cualquier tipo de amenaza. De acuerdo con el último informe de ciberataques de tipo ransomware 2023.

Arroja un crecimiento en ataques de ransomware a nivel mundial de casi el 40%, El mayor aumento de ataques de ransomware lo experimentaron las entidades del sector cultural, de entretenimiento y recreativo, con una tasa de crecimiento superior al 430 %. (Zscalers, 2023)

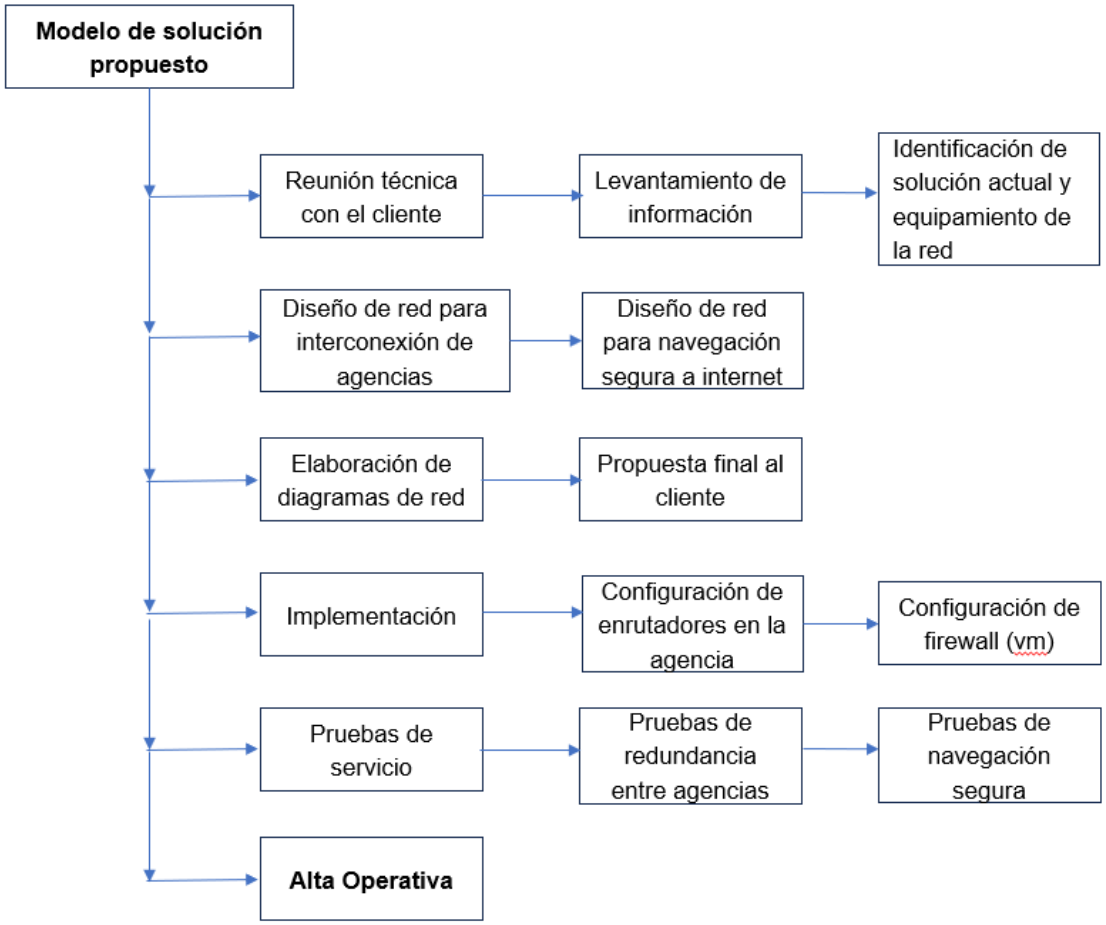
3.2 Modelo de solución propuesto:

Durante mis estudios de pregrado en la UNTELS, me he inclinado con orientación al campo de las telecomunicaciones, iniciando por comunicaciones móviles durante mis prácticas preprofesionales y posterior a ello, pase al área de redes IP, los cursos que moldearon mis competencias y habilidades desde la fecha fueron Arquitectura del computador y Arquitectura de redes y protocolos. La solución propuesta para este proyecto se basó mediante el siguiente diagrama de actividades.

El siguiente diagrama mostrado en la Figura 9, se detalla las fases del proyecto conformado por el levantamiento de información, diseño, implementación de configuración y pruebas de redundancia.

Figura 9

Diagrama de proceso de solución para la entidad bancaria.



Nota. Elaboración propia.

A continuación, en la Tabla 3, se presenta el cronograma con las actividades de acuerdo con el modelo de solución propuesto, realizadas para la entidad bancaria.

Tabla 3

Cronograma de ejecución para el proyecto.

Fecha	Actividad para desarrollar	Personal a cargo
7/08/2023	Se sostuvo una reunión técnica con el cliente	TST - Entidad bancaria
8/08/2023	Levantamiento de información en las agencias.	TST - técnico contratista
10/08/2023	Propuesta de diseño con alta redundancia	TST
11/08/2023	Elaboración de diagrama de red	TST
14/08/2023	Instalación de 4 enrutadores en la agencia principal	Técnico contratista
14/08/2023	Instalación de un enrutador en las 3 agencias remotas	Técnico contratista
16/08/2023	Configuración de los 4 enrutadores empleando los protocolos BGP y VRRP	TST
18/08/2023	Configuración de la VDOM o cortafuegos virtual	TST
21/08/2023	Configuración de los 3 enrutadores en las agencias remotas mediante el protocolo BGP hacia la agencia principal	TST
25/08/2023	Pruebas de redundancia tanto para el servicio de Internet como enlace de datos, se simulará la caída de ambos enlaces principales	TST - Entidad bancaria
26/08/2023	Pruebas de filtrado de a destinos maliciosos	TST - Entidad bancaria
30/09/2023	Alta Operativa	PMO - TST

Nota. Las actividades que corresponden a TST fueron desarrolladas por mi persona. Elaboración propia.

3.2.1 Diseño

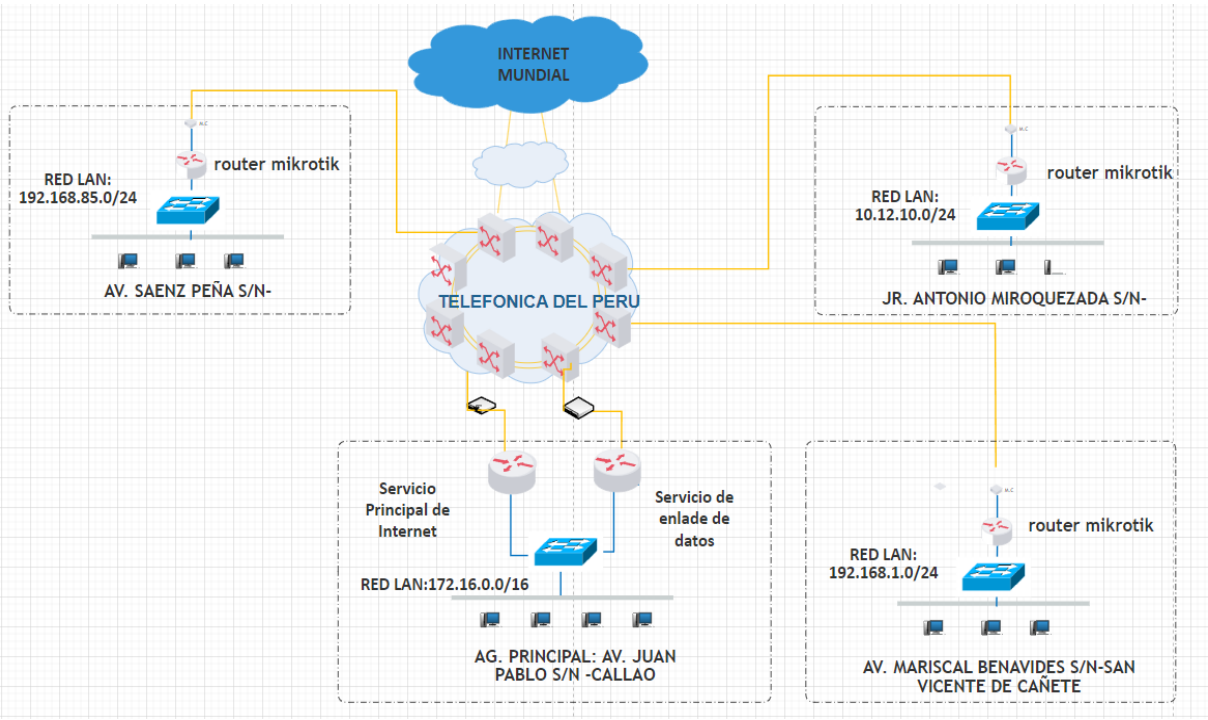
Previo al diseño de la solución final y topología de red, se realizó un kickoff (reunión de inicio de proyecto) con el cliente para el levantamiento de información técnica, respecto al equipamiento y parámetros lógicos instalados por su actual proveedor. La entidad bancaria cuenta con un conmutador propio en capa 2 gestionable en su agencia principal, así como en sus 3 agencias remotas.

TDP (Telefónica del Perú) implementó dos enlaces dedicados conectados a dos enrutadores de marca cisco uno para el servicio de Internet y otro para el enlace de datos en la agencia principal, ambos enrutadores se interconectan con el conmutador del cliente. En las agencias remotas TDP implementó un solo enrutador con un solo enlace dedicado, este enrutador se interconecta al conmutador del cliente.

En la Figura 10, se representa el diagrama de red de la entidad bancaria con su proveedor actual TDP, podemos notar que no existe redundancia a nivel físico como lógico para interconexión de agencias y navegación a internet.

Figura 10

Diagrama de red de la entidad bancaria con el proveedor TDP



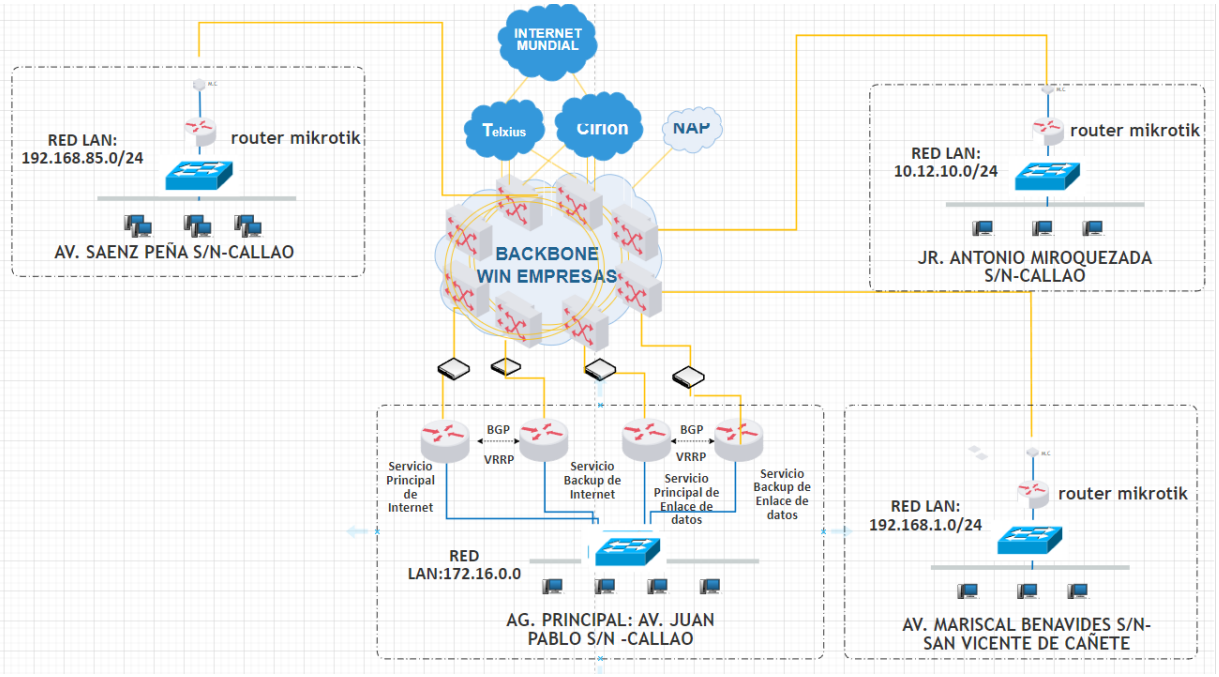
Nota. Elaboración propia

3.2.1.1 Diseño de Enlace de datos.

En la Figura 11. Presento la propuesta de diseño de red final, la agencia principal contará con cuatro enlaces dedicados por fibra óptica, dos enlaces para el servicio de internet seguro y dos enlaces para el servicio de enlace de datos, las agencias remotas tendrán un enlace dedicado de fibra óptica que interconectara hacia los enrutadores de la agencia principal, se establecerá el protocolo dinámico BGP entre el enrutador de las agencias remotas y los dos enrutadores de interconexión de datos de la agencia principal.

Figura 11

Diagrama de red WAN para enlace de datos, propuesta final por Win empresas

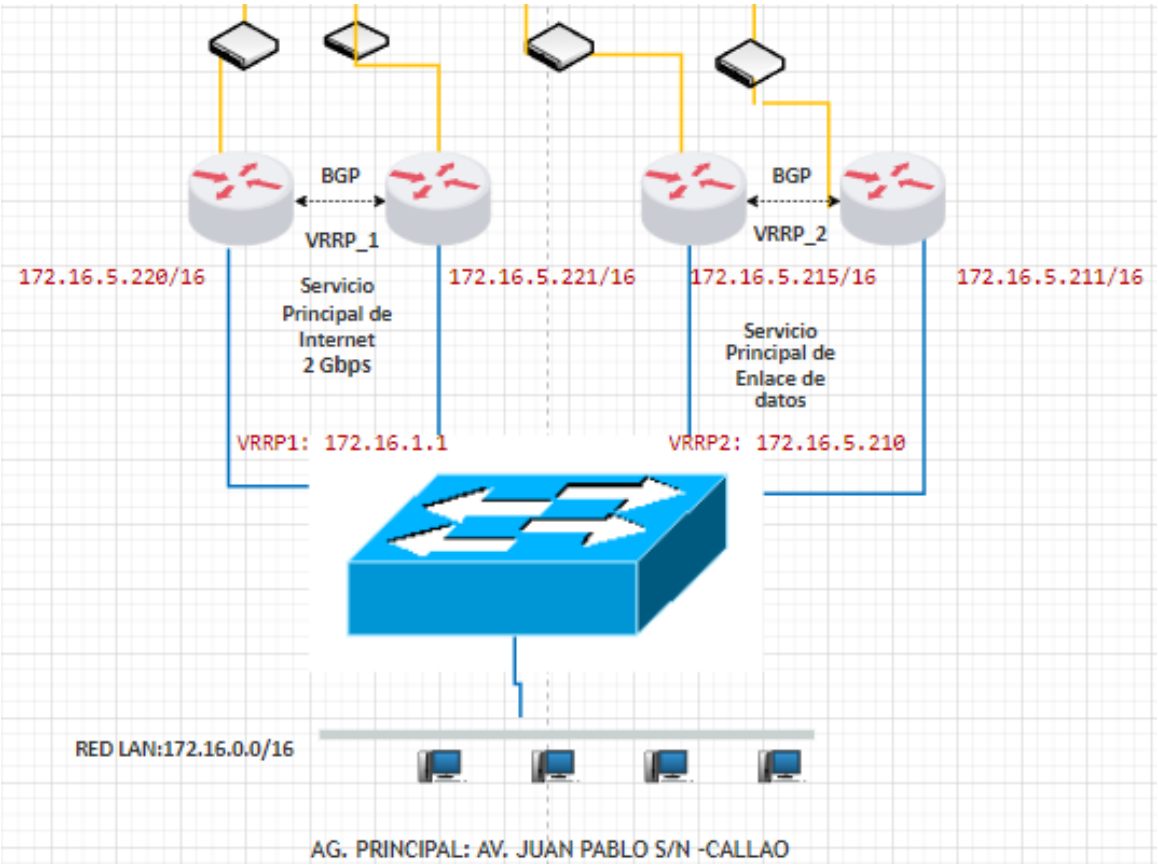


Nota. Diagrama de red para interconexión de agencias, solución final que será implementado por Win empresas. Elaboración propia

En la Figura 12, presento el diagrama de red LAN para la agencia principal, se configurarán 2 grupos de VRRP para ambos servicios, los host y servidores internos de la agencia principal tendrán como Gateway la IP virtual del VRRP_2 de enlace de datos, con esto aseguraremos conectividad a nivel LAN con alta redundancia hacia las agencias remotas y navegación a internet.

Figura 12

Diagrama de red LAN, propuesta final por Win empresas.

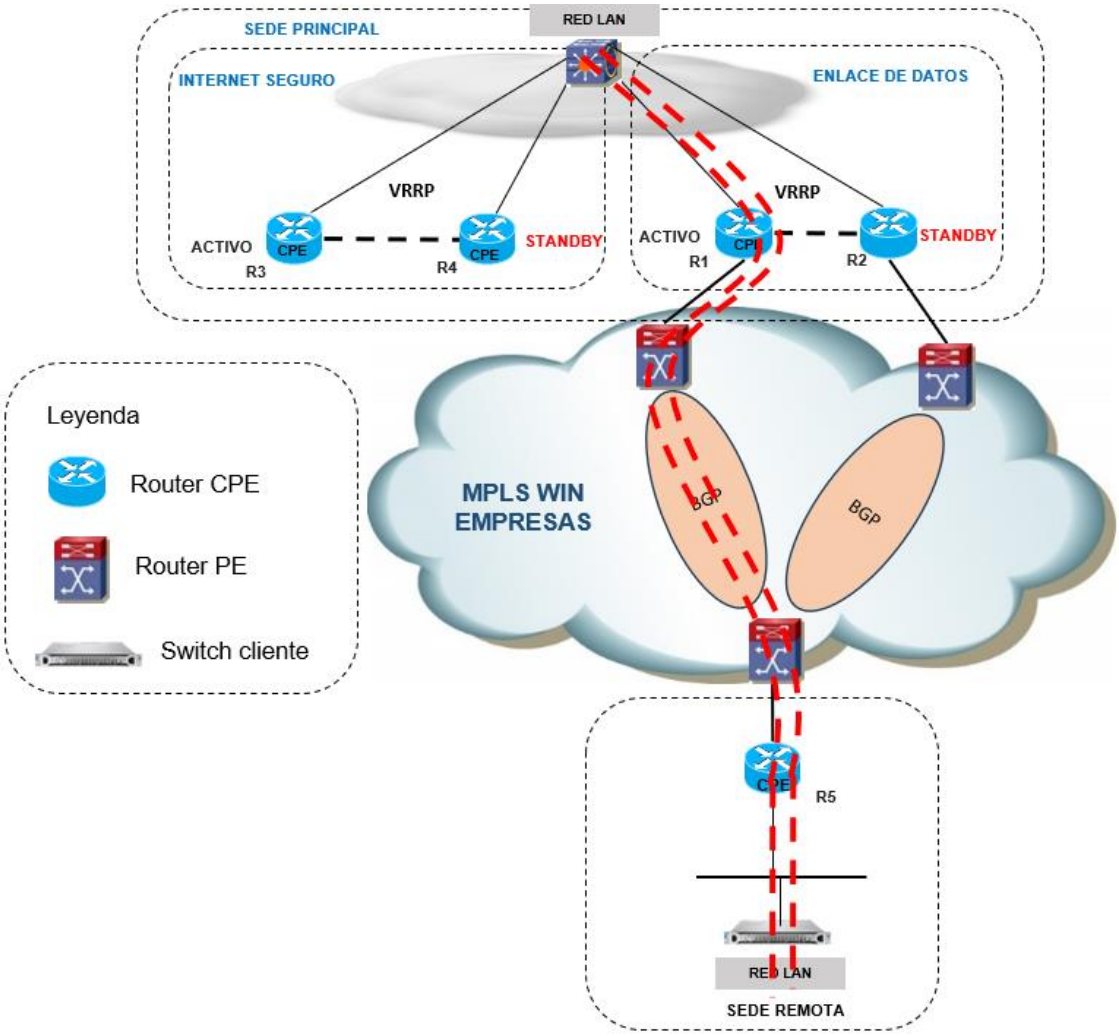


Nota. Elaboración propia.

En el siguiente diagrama representado en la Figura 13, explico la ruta por la cual el tráfico de datos sigue desde la red LAN de las agencias remotas hasta la red LAN de la agencia principal, se establece 2 rutas por enrutamiento dinámico BGP desde el enrutador de la agencia remota hasta la agencia principal, para este caso considerando que ambos enlaces están activos el tráfico tomará el camino de la izquierda por tener mayor prioridad a nivel de preferencia de rutas. En la agencia principal se configura el protocolo VRRP entre los enrutadores R1 Y R2, de esta forma R1 estará en estado "*Activo"* y R2 "*Standby".*

Figura 13

Tráfico de red para el servicio de enlace de datos - enlace principal activo.

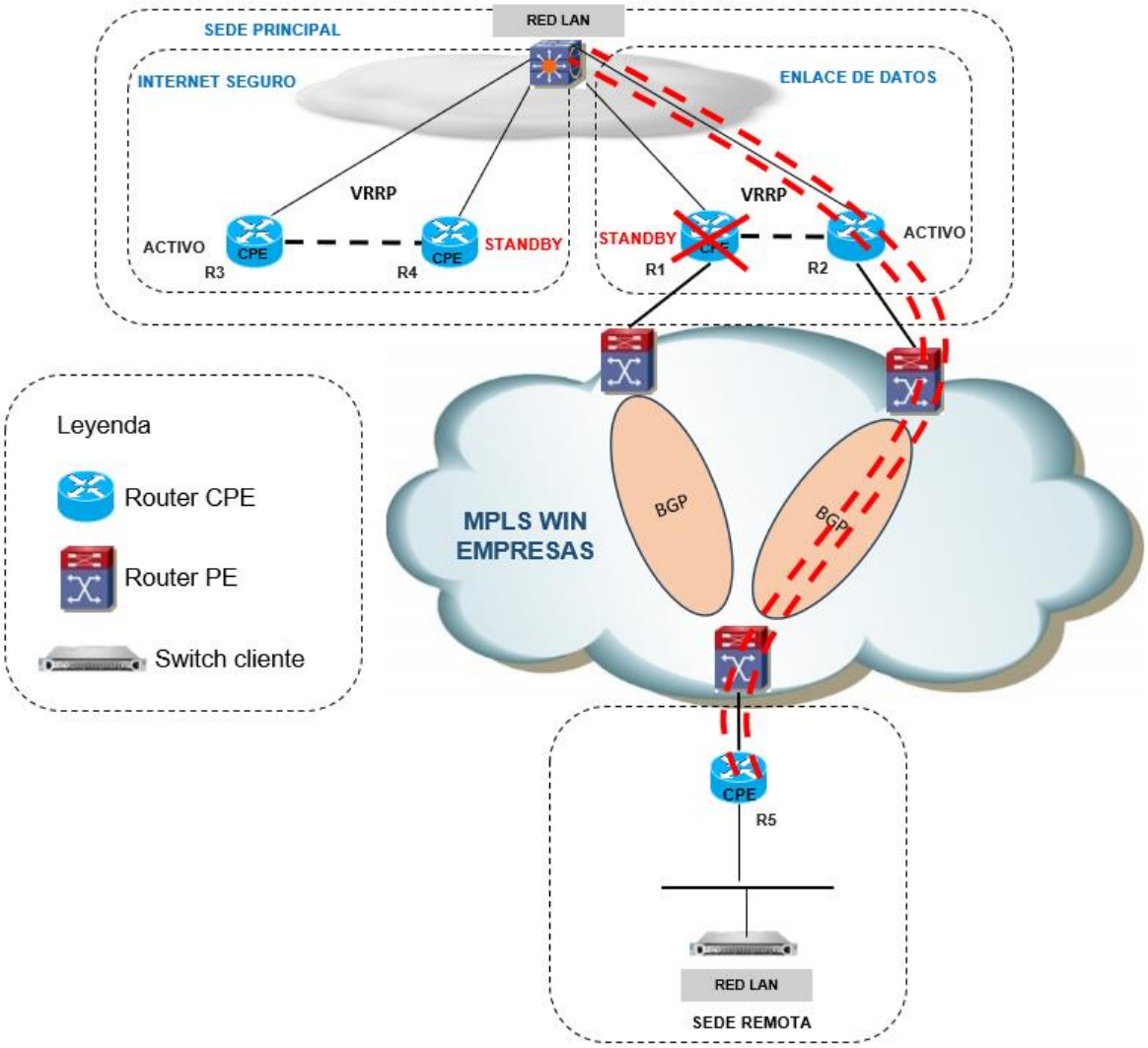


Nota. Elaboración propia.

A continuación bajo el escenario de una caída en el enlace principal mostrado en la Figura 14, el tráfico de datos conmuta automáticamente por la segunda ruta, en la agencia principal el R1 pasará de activo a standby y R2 tomará el rol de activo.

Figura 14

Tráfico de red para el servicio de enlace de datos - enlace principal caído.



Nota. Elaboración propia.

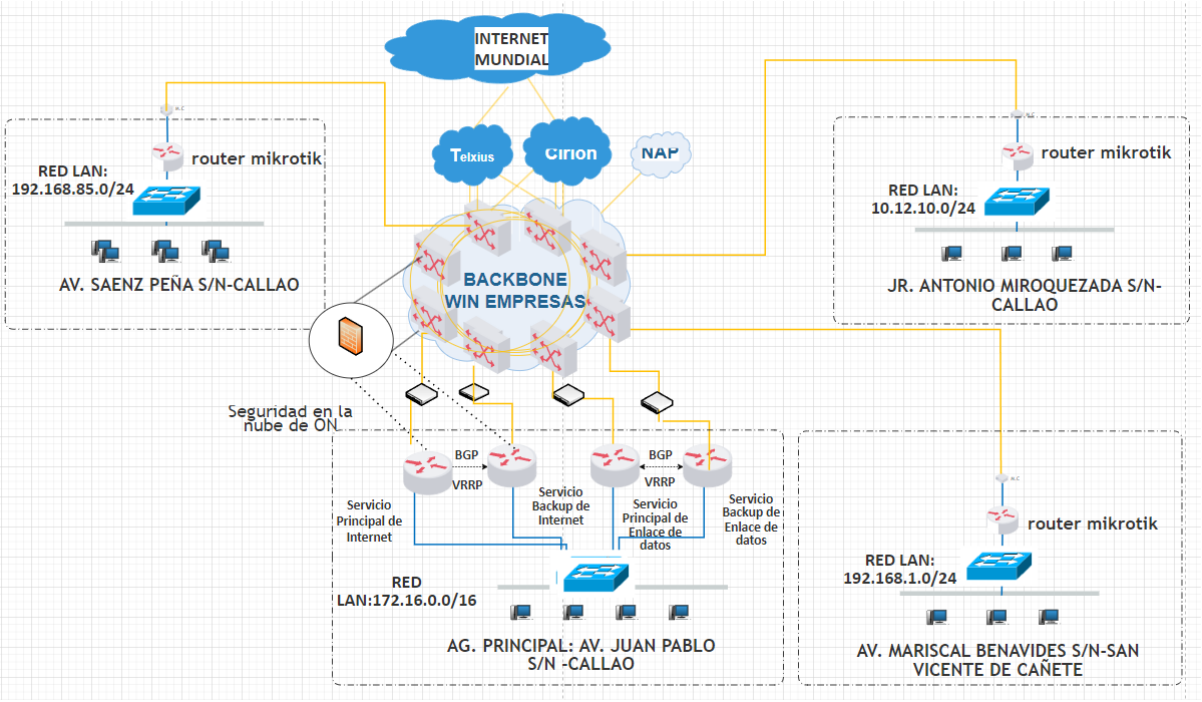
3.2.1.2 Diseño de Internet Seguro

Para esta solución se creará un entorno virtual VDOM en el firewall Fortinet alojado en la red backbone de Win Empresas, este firewall tendrá conectividad a los dos enrutadores dedicados para internet seguro en la agencia principal por enrutamiento dinámico BGP, de esta manera tendremos alta disponibilidad para la navegación de internet.

En la Figura 15, se representa el diagrama con los elementos para esta solución, Las agencias remotas para poder navegar a internet tendrán un esquema de navegación centralizado, el paquete llegará por el servicio de enlace de datos a la agencia principal luego de eso este paquete será enviado hacia los enrutadores de internet seguro, posterior a ello, viajará al firewall y por último a los proveedores internacionales como Telxius o Cirion.

Figura 15

Diagrama de red WAN para Internet Seguro, propuesta final.



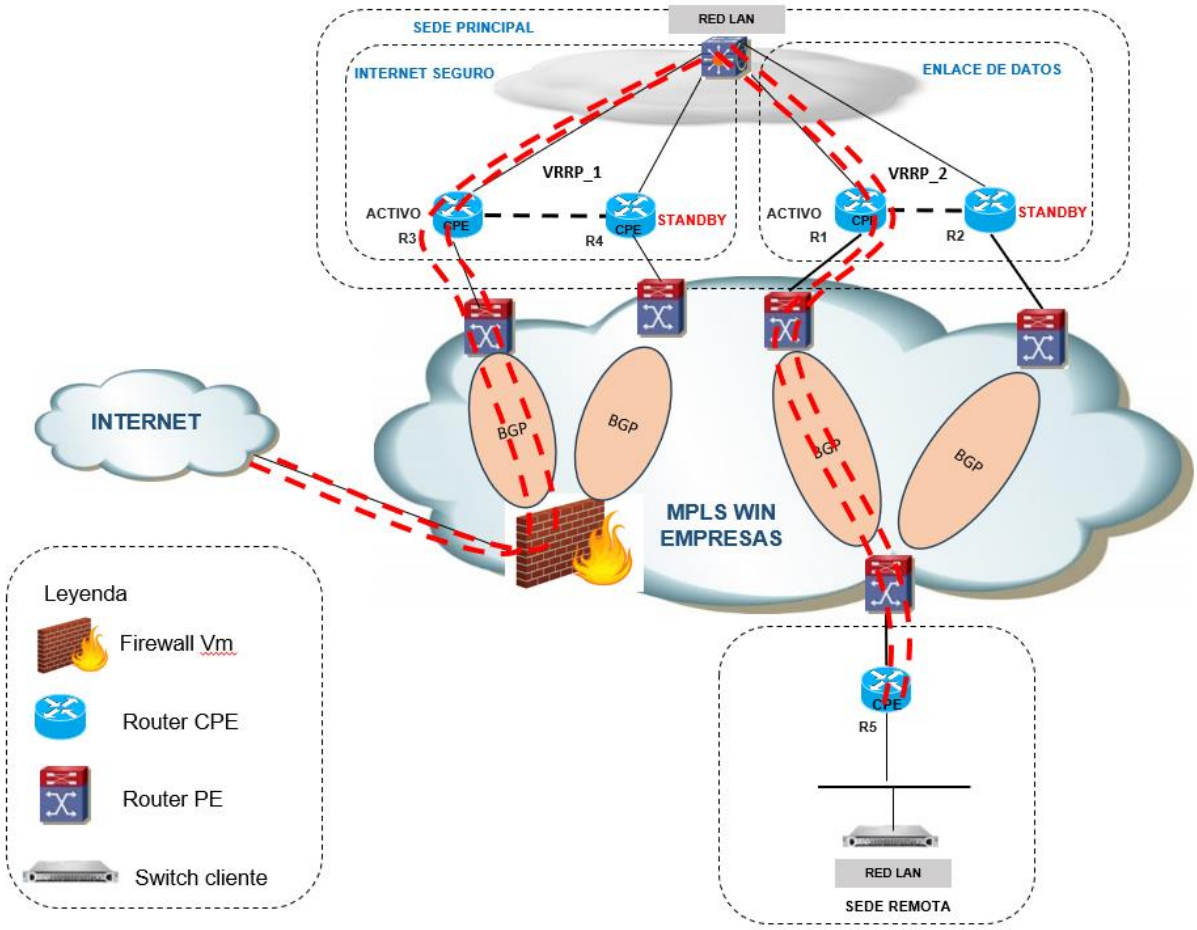
Nota. Elaboración propia.

En el siguiente diagrama de la Figura 16, muestro la ruta que toma el tráfico de datos desde el Conmutador cliente en la agencia principal hacia Internet, en las Figura 12 y 13 ya se explicó como el tráfico viaja desde la agencia remota hasta el Conmutador cliente en la agencia principal.

Ambos enrutadores R3 u R4 de Internet seguro se interconectan por BGP al firewall en la backbone, se definió la ruta izquierda como preferente, entonces bajo este escenario donde ambas rutas están activas, el tráfico tomará el camino de la izquierda siendo R3 el enrutador activo.

Figura 16

Tráfico de red para el servicio de Internet Seguro - enlace principal activo.

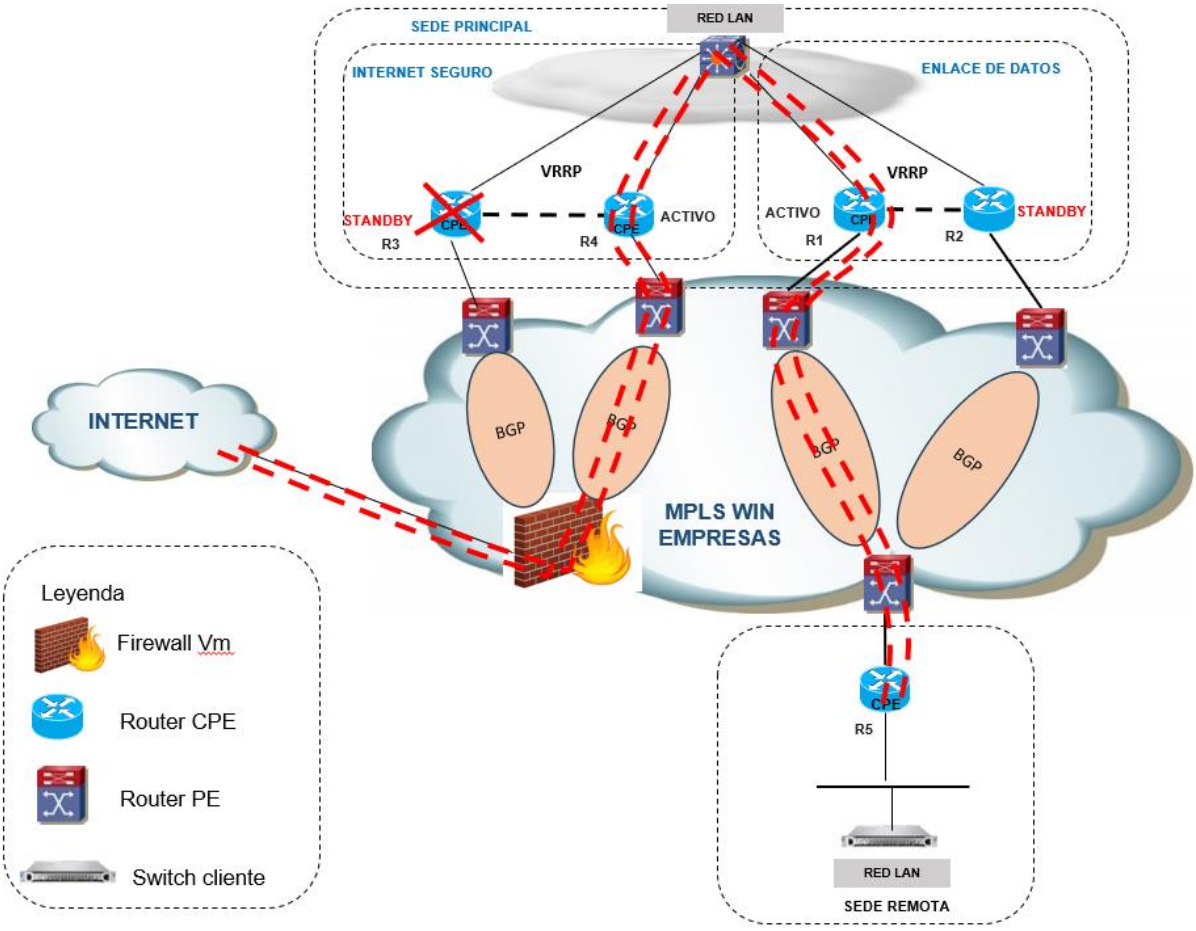


Nota. Elaboración propia.

Bajo la casuística del escenario de una caida en el enlace principal del servicio de Internet Seguro mostrado en la Figura 17, el tráfico de datos conmuta automáticamente por la segunda ruta, en la agencia principal el R3 pasará de activo a standby y R4 tomará el rol de activo.

Figura 17

Tráfico de red para el servicio de Internet Seguro - enlace principal caído



Nota. Elaboración Propia.

3.2.2 Implementación de servicios

3.2.2.1 Implementación de servicio: Enlace de datos

Posterior a la entrega de los diagramas de solución final al cliente, se procedió con la instalación de 4 enrutadores en la agencia principal y 3 enrutadores en cada agencia remota, en la Tabla 4, se detallan las características como marca y modelo los equipos instalados por cada agencia.

Tabla 4

Tabla de características de los enrutadores implementados.

Agencia	Rol	Servicio	Marca	Modelo
Av. Juan Pablo	Principal	Internet Seguro	Mikrotk	CCR2004-16G-2S+
Av. Juan Pablo	Respaldo	Internet Seguro	Mikrotk	CCR2004-16G-2S+
Av. Juan Pablo	Principal	Enlace de datos	Mikrotk	CCR2004-16G-2S+
Av. Juan Pablo	Respaldo	Enlace de datos	Mikrotk	CCR2004-16G-2S+
Av. Sáenz Peña	Principal	Enlace de datos	Mikrotk	RB3011UiAS
Jr. Antonio Miró Quesada	Principal	Enlace de datos	Mikrotk	RB3011UiAS
Av. Mariscal Benavides	Principal	Enlace de datos	Mikrotk	RB3011UiAS

Nota. Elaboración propia.

En la Tabla 5, especificamos los segmentos a configurar para cada agencia, se definió un segmento en máscara 28 para futuras implementaciones de hasta al menos 14 agencias, asimismo, se define los sistemas autónomos para las agencias principales y remotos.

Tabla 5

Tabla de segmentación a nivel WAN para enlace de datos.

Agencia	Segmento de red WAN	Sistema autónomo
AG. PRINCIPAL: AV. JUAN PABLO S/N -CALLAO - Principal	172.20.13.81/28	65501
AG. PRINCIPAL: AV. JUAN PABLO S/N -CALLAO - Backup	172.20.13.82/28	65501
JR. ANTONIO MIROQUEZADA S/N-CALLAO	172.20.13.84/28	65002
AV. SAENZ PEÑA S/N-CALLAO	172.20.13.85/28	65002
AV. MARISCAL BENAVIDES S/N-SAN VICENTE DE CAÑETE	172.20.13.86/28	65002

Nota. Elaboración propia.

A. Implementación de configuración BGP: Enrutador principal contra agencias remotas

En la Figura 18, se muestra la configuración de enrutamiento dinámico BGP entre el enrutador principal de la agencia principal con las 3 agencias remotas, en la Tabla 5 se definen los segmentos para esta configuración.

- local.address / Corresponde a la IP WAN del enrutador principal.
- remote.address / Corresponde a la IP WAN de agencias remotas.
- name / Descripción que corresponde al nombre de la sede remota.
- hold-time=6s y *keepalive=2s / Estos parámetros de intervalo de actividad y el tiempo de espera se configura con los mismos valores.
- output.default-originate=always / Esta configuración indica que anunciaremos una ruta por defecto a nuestras agencias remotas.

Figura 18

Configuración de BGP entre el enrutador principal y las 3 agencias remotas

```
/routing bgp connection
add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.81 .role=ebgp name="Saenz Pe\F1a" nexthop-choice=default output.default-originate=always
remote.address=172.20.13.85/32 .as=65002 router-id=\
    172.20.13.81 routing-table=main templates=temp1 use-bfd=no
add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.81 .role=ebgp name="Mariscal Benavides" nexthop-choice=default output.default-originate=always
remote.address=172.20.13.86/32 .as=65002 router-id=\
    172.20.13.81 routing-table=main templates=temp1 use-bfd=no
add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.81 .role=ebgp name=Antonio_Miroquezada nexthop-choice=default output.default-originate=always
remote.address=172.20.13.84/32 .as=65002 router-id=\
    172.20.13.81 routing-table=main templates=temp1 use-bfd=no
```

Nota. Tomado de RouterOS – Winbox

Se realizó la configuración de netwatch para escanear el estado de enlace a nivel WAN, definiendo el siguiente script mostrado en la Figura 19, el host de monitoreo es 10.40.140.105 si en intervalo de 10 segundos no se tiene respuesta de este host la VRRP_2 actuará bajando la prioridad de 200 a 100, ósea el enrutador cambiará de estado de activo a standby.

Figura 19

Configuración de netwatch entre el enrutador principal y la red backbone

```
/tool netwatch
add disabled=no down-script="interface vrrp set vrrp2 priority=100" host=10.40.140.105 http-codes=""
interval=10s test-script="" timeout=10ms type=simple up-script="interface vrrp set vrrp2 priority=200"
```

Nota. Tomado de RouterOS – Winbox

B. Implementación de configuración BGP: Enrutador backup contra agencias remotas

En la Figura 20, se puede verificar la configuración BGP entre el enrutador backup de la agencia principal contra las agencias remotas, a diferencia de la Figura 18 el único cambio realizado en la configuración es el *local.address, ya que al ser otro enrutador le corresponde una IP WAN diferente.

La configuración de netwatch solo se realiza en el enrutador principal.

Figura 20

Configuración de BGP entre el enrutador backup y las 3 agencias remotas

```
/routing bgp connection

add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.82 .role=ebgp name="SAENZ PE\D1A_1060" nexthop-choice=default \
    output.default-originate=always remote.address=172.20.13.85/32 .as=65002 router-id=172.20.13.82
routing-table=main templates=temp1
add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.82 .role=ebgp name="SEDE CA\D1ETE" nexthop-choice=default \
    output.default-originate=always remote.address=172.20.13.86/32 .as=65002 router-id=172.20.13.82
routing-table=main templates=temp1
add address-families=ip as=65001 disabled=no hold-time=6s keepalive-time=2s local.address=
172.20.13.82 .role=ebgp name="SEDE MIROQUEZADA" nexthop-choice=default \
    output.default-originate=always remote.address=172.20.13.84/32 .as=65002 router-id=172.20.13.82
routing-table=main templates=temp1
```

Nota. Tomado de RouterOS – Winbox

C. Implementación de configuración BGP: Agencias remota contra Agencia principal

El escenario de configuración BGP entre las agencias remotas y los dos enrutadores de la agencia principal son las mismas, las agencias remotas tienen 2 direcciones remotas con las cuales se establecerá la sesión BGP, en la Figura 21 muestro la configuración BGP.

- remote-address=172.20.13.81 y *remote-address=172.20.13.82, los parámetros hold-time y keepalive se mantienen de acuerdo con los pares configurados.

Figura 21

Configuración de BGP entre el enrutador remoto y la agencia principal.

```
/routing bgp peer
add hold-time=6s in-filter=PRIN instance=BGP-L2L keepalive-time=2s max-prefix-restart-time=infinity name=PRIN-L2L
remote-address=\ 172.20.13.81 remote-as=65001
add hold-time=6s in-filter=BK instance=BGP-L2L keepalive-time=2s max-prefix-restart-time=infinity name=BK-L2L
remote-address=\ 172.20.13.82 remote-as=65001
```

Nota. Tomado de RouterOS – Winbox

Como se muestra en la Figura 22, se configurará un filtro en BGP llamado “Weight” en los enrutadores de las agencias remotas para definir el camino de acuerdo con el diseño presentado, considerar que a mayor valor de peso mayor la preferencia de ruta por lo tanto de acuerdo con la Figura 13. R1 será definido como enrutador principal.

Dentro de la Figura 22, también mostramos el comando *routing bgp network / este comando indica que red estamos anunciando, los enrutadores de las agencias remotas deben recibir una ruta por defecto de los enrutadores de la agencia principal y anunciar el segmento LAN que corresponde a cada agencia.

Figura 22

Configuración de Weihgt entre el enrutador remoto y la agencia principal.

```
/routing filter
add bgp-weight=200 chain=PRIN set-bgp-weight=200
add bgp-weight=100 chain=BK set-bgp-weight=100

/routing bgp network
add network=192.168.85.0/24 synchronize=no
```

Nota. Tomado de RouterOS – Winbox

En la Tabla 6, se define los segmentos LAN de cada agencia y el Gateway o puerta de enlace.

Tabla 6

Tabla de segmentación a nivel LAN para enlace de datos.

AGENCIA	SEGMENTO DE RED LAN	GATEWAY
AG. PRINCIPAL: AV. JUAN PABLO S/N -CALLAO	172.16.0.0/16	172.16.0.1
AV. MARISCAL BENAVIDES S/N-SAN VICENTE DE CAÑETE	192.168.1.0/24	192.168.1.1
JR. ANTONIO MIROQUEZADA S/N-CALLAO	10.12.10.0/24	10.12.10.1
AV. SAENZ PEÑA S/N-CALLAO	192.168.85.0/24	192.168.85.1

Nota. Elaboración propia.

D. Implementación de configuración: Enrutamiento estático en la agencia principal.

En la agencia principal contamos con 2 enrutadores para el servicio de internet seguro y dos enrutadores para el servicio de enlace de datos, hasta el momento ya contamos con comunicación de las agencias remotas con los enrutadores del servicio de enlace de datos, pero para que las sedes remotas puedan navegar a internet los enrutadores del servicio de internet seguro deben conocer las rutas de las agencias remotas para ello configuraremos enrutamiento estático.

De acuerdo con la Figura 11. Existen dos grupos de VRRP:

- VRRP_1: Entre los enrutadores del servicio Internet Seguro
- VRRP_2 entre los enrutadores del servicio enlace de datos.

Crearemos una ruta por defecto en los enrutadores de enlace de datos con siguiente salto la IP flotante de la VRRP_1, en la Figura 23, se muestra que aprenderemos las ruta por defecto desde la IP 172.16.1.1.

Figura 23

Configuración de ruta estática entre el enrutador de enlace de datos con el enrutador de internet seguro

```
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=172.16.1.1 routing-table=main suppress-hw-offload=no
```

Nota. Tomado de RouterOS – Winbox

Por último, para que el tráfico tenga el correcto retorno configuraremos enrutamiento estático en los enrutadores de internet seguro y aprenderemos los segmentos LAN de las agencias remotas a través de las IP flotante VRRP_2 del enrutador de enlace de datos, considerar que este enrutamiento se tiene que replicar en los enrutadores backup.

Como se muestra en la Figura 24, se crearon 3 rutas estáticas de las 3 agencias remotas aprendiendo sus segmentos LAN a través de la IP flotante VRRP_2.

Figura 24

Configuración de ruta estática entre el enrutador de internet seguro con el enrutador de enlace de datos

```
/ip route

add comment="Sede: Saenz Pe\F1a 1060" disabled=no distance=1 dst-address=192.168.85.0/24 gateway=172.16.5.215 pref-src="" routing-table=main scope=\
    30 suppress-hw-offload=no target-scope=10
add comment="Sede: Ca\F1ete" disabled=no distance=1 dst-address=192.168.1.0/24 gateway=172.16.5.215 pref-src="" routing-table=main scope=30 \
    suppress-hw-offload=no target-scope=10
add comment="Sede: Miroquezada" disabled=no distance=1 dst-address=10.12.10.0/24 gateway=172.16.5.215 pref-src=0.0.0.0 routing-table=main scope=30 \
    suppress-hw-offload=no target-scope=10
```

Nota. Tomado de RouterOS – Winbox

3.2.2.2 Implementación de servicio: Internet Seguro

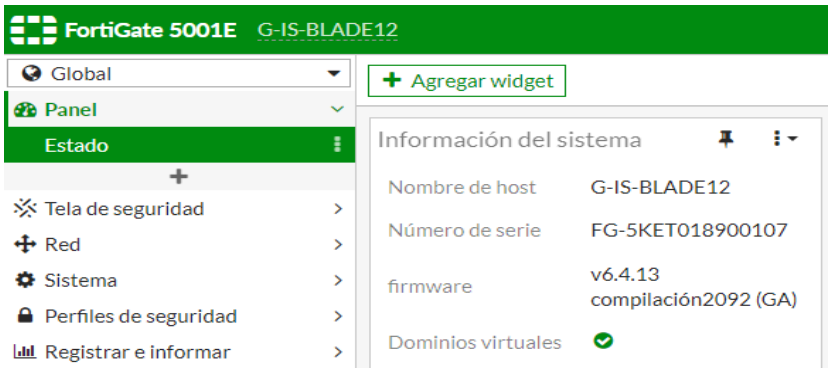
a) Creación de VDOM.

En WIN EMPRESAS contamos con el servicio de seguridad en la nube con multi vendors, para este proyecto crearemos una VDOM en un equipo FORTIGATE alojado en la backbone, sobre este firewall o cortafuegos crearemos reglas de navegación para las agencias, adicional a ello, estableceremos dos sesiones BGP hacia los enrutadores de internet seguro en la agencia principal, con esto lograremos doble redundancia.

En la Figura 25, se muestra las características como número de serie y versión de firmare del equipo firewall donde configuraremos la VDOM.

Figura 25

Panel del Fortigate 5001E



Nota. Tomado del Sistema Operativo FortiOS.

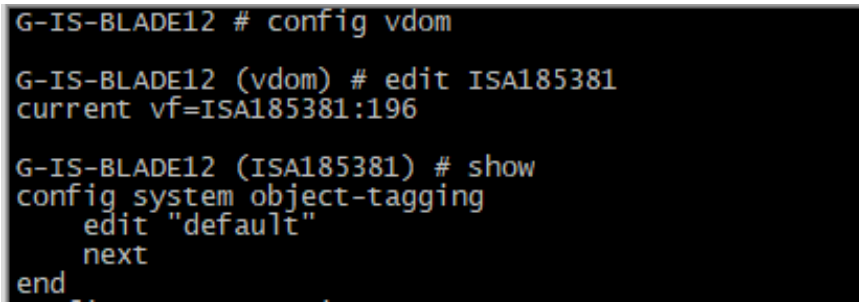
b) Configuración de sistema.

La VDOM será creada sobre el BLADE 12(Cuchilla o chasis) tendrá la descripción del número de circuito a la cual pertenece el servicio, para este caso **ISA185381.**

En la Figura 26, se muestra la configuración para la creación de VDOM ISA185381, en la configuración global digitamos el comando “config vdom” para entrar al modo “vdom” posterior a ello digitamos el comando “edit + el nombre del circuito” con ello ya se creó el entorno virtual “VDOM ISA185381” con parámetros básicos sin ningún tipo de acción.

Figura 26

Configuración de VDOM y sistema.



Nota. Tomado del sistema Operativo FortiOS.

c) Configuración de Interfaces

Se configurará segmentos sobre 2 interfaces físicas y una interfaz Loopback. Las conexiones tendrán los roles WAN y LAN sobre Vlans, el rol WAN es un segmento de paso entre el Fortinet y el enrutador de borde para la salida internacional, el rol LAN es un segmento de paso entre el Fortinet y el enrutador de la backbone que a través de la red MPLS por de Win empresas tendrá conexión con los enrutadores de internet seguro en la agencia principal, a continuación, detallo los segmentos en la siguiente Tabla 7.

La interfaz virtual Loopback aloja las IP PUBLICAS asignados a la entidad bancaria, me limitare a indicar el segmento por seguridad.

Tabla 7

Direccionamiento IP en la VDOM.

FIREWALL	VLAN	ROL
10.44.120.6/30	3245	WAN
10.44.170.5/30	2245	LAN
10.35.46.89/30	2245	LAN
x.x.x.x/30	-	Loopback

Nota. Elaboración Propia.

En la Figura 27, se muestra la configuración de la interfaz LAN y WAN del firewall, sobre la interfaz LAN se configurarán 2 segmentos IP una principal y otra secundaria debido a que la VDOM apunta a dos enrutadores en la agencia principal, véase la Tabla 7. Posterior a ello en la misma interfaz se configura la vlan 2245 que a través de la MPLS se trasportara hasta los enrutadores en la agencia principal.

La configuración de la Interfaz WAN muestra el segmento de paso definido entre el firewall y enrutador perimetral con la vlan 3245, este segmento de paso se crea con la finalidad de navegar a internet, sobre este segmento crearemos una ruta estática aprendiendo una ruta por defecto a través del siguiente salto que vendría a ser la IP 10.44.120.5.

Figura 27

Configuración de interfaz WAN y LAN en la VDOM.

```
G-IS-BLADE12 (interface) # edit LAN-ISA185381

G-IS-BLADE12 (LAN-ISA185381) # show
config system interface
    edit "LAN-ISA185381"
        set vdom "ISA185381"
        set ip 10.44.170.5 255.255.255.252
        set allowaccess ping
        set alias "ISA-LAN"
        set device-identification enable
        set role lan
        set snmp-index 309
        set secondary-IP enable
        set interface "port3"
        set vlanid 2245
        config secondaryip
            edit 1
                set ip 10.35.46.89 255.255.255.252
                set allowaccess ping
            next
        end
    next
end
G-IS-BLADE12 (LAN-ISA185381) # end

G-IS-BLADE12 (ISA185381) # conf system interface

G-IS-BLADE12 (interface) # edit WAN-ISA185381

G-IS-BLADE12 (WAN-ISA185381) # show
config system interface
    edit "WAN-ISA185381"
        set vdom "ISA185381"
        set ip 10.44.120.6 255.255.255.252
        set allowaccess ping https
        set alias "ISA-WAN"
        set device-identification enable
        set role wan
        set snmp-index 308
        set interface "port3"
        set vlanid 3245
    next
end
```

Nota. Tomado del sistema Operativo FortiOS.

d) Enrutamiento dinámico en el Firewall.

Estableceremos 2 sesiones BGP entre el firewall y los enrutadores del servicio de internet seguro que se alojan en la agencia principal de la entidad bancaria.

Como primer paso crearemos mapa de rutas, esta herramienta nos servirá para manipular los segmentos que anunciamos y recibiremos. En la Figura 28, muestro la configuración. Anunciaremos una ruta por defecto bajo el mapa “DEFAULT_OUT” y recibiremos los segmentos de las agencias bajo el mapa “red_cliente_pri” y “red_cliente_bk”.

Figura 28

Configuración de mapa de rutas en el firewall.

```
G-IS-BLADE12 (ISA185381) # show router route-map
config router route-map
    edit "DEFAULT_OUT"
        config rule
            edit 1
                set match-ip-address "DEFAULT"
                unset set-ip-nexthop
                unset set-ip6-nexthop
                unset set-ip6-nexthop-local
                unset set-originator-id
            next
        end
    next
    edit "red_cliente_princ"
        config rule
            edit 1
                set match-ip-address "redes_cliente"
                unset set-ip-nexthop
                unset set-ip6-nexthop
                unset set-ip6-nexthop-local
                unset set-originator-id
            next
        end
    next
    edit "red_cliente_bk"
        config rule
            edit 1
                set match-ip-address "redes_cliente"
                set set-aspath "65130" "2"
                unset set-ip-nexthop
                unset set-ip6-nexthop
                unset set-ip6-nexthop-local
                unset set-originator-id
            next
        end
    next
end
```

Nota. Tomado de Operativo FortiOS

Como segundo paso. crearemos prefix list o muy parecido a lista de accesos, esta herramienta nos permite filtrar actualización de rutas entre vecinos.

En la Figura 29, mostramos la crearemos dos perfiles de prefix_list, una llamada “DEFAULT” que será una ruta por defecto que anunciaremos a los enrutadores de la agencia principal, el perfil “redes_cliente” serán las únicas rutas que permitiremos recibir de los enrutadores, estas redes clientes pertenecen a los segmentos LAN de la agencia principal y las agencias remotas.

Figura 29

Configuración lista de prefijos en el firewall.

```
G-IS-BLADE12 (ISA185381) # show router prefix-list
config router prefix-list
    edit "DEFAULT"
        config rule
            edit 1
                set prefix 0.0.0.0 0.0.0.0
                unset ge
                unset le
            next
        end
    next
    edit "redes_cliente"
        config rule
            edit 1
                set prefix 192.168.0.0 255.255.0.0
                unset ge
                unset le
            next
            edit 2
                set prefix 172.16.0.0 255.255.0.0
                unset ge
                unset le
            next
            edit 3
                set prefix 10.10.1.0 255.255.255.0
                unset ge
                unset le
            next
            edit 4
                set prefix 192.168.85.0 255.255.255.0
                unset ge
                unset le
            next
            edit 5
                set prefix 192.168.1.0 255.255.255.0
                unset ge
                unset le
            next
            edit 6
                set prefix 10.12.10.0 255.255.255.0
                unset ge
                unset le
            next
        end
    next
end
```

Nota. Tomado del sistema Operativo FortiOS.

Como tercer paso, configuraremos el protocolo BGP, para ello definiremos el AS local y remoto, AS (Sistema Autónomo).

- AS Local Firewall: 65120.
- AS Remoto enrutador principal y backup: 65130.

Luego definimos los vecinos, estos segmentos corresponden al segmento de paso LAN entre el firewall y enrutador principal y respaldo de internet seguro en la agencia principal, en la Tabla 8, se define los segmentos.

Tabla 8

Segmento de paso entre el firewall y los enrutadores de la agencia principal

FIREWALL	AGENCIA PRINCIPAL
10.44.170.5/30	10.44.170.6/30 - PRINCIPAL
10.35.46.89/30	10.35.46.90/30 - BACKUP

Nota. Elaboración propia.

14 En la Figura 30, se muestra la configuración BGP entre el Firewall y los enrutadores de la agencia principal, dentro de la configuración global de BGP se define el AS local, luego se configura los vecinos o neighbor dentro de estas se definen el AS remoto y el mapa de rutas in y out,

- ✓ set route-map-in / rutas recibidas de la agencia principal.
- ✓ set route-map-out / rutas anunciadas a la agencia principal.

Figura 30

Configuración BGP entre el firewall y la agencia principal y backup

```
G-IS-BLADE12 (ISA185381) # conf router bgp

G-IS-BLADE12 (bgp) # show
config router bgp
    set as 65120
    config neighbor
        edit "10.44.170.6"                    ROUTER PRINCIPAL
            set capability-default-originate enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65130
            set route-map-in "red_cliente_princ"
            set route-map-out "DEFAULT_OUT"
        next
        edit "10.35.46.90"                    ROUTER RESPALDO
            set capability-default-originate enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65130
            set route-map-in "red_cliente_bk"
            set route-map-out "DEFAULT_OUT"
        next
    end
    config network
        edit 1
            set prefix 172.16.0.0 255.255.0.0
        next
        edit 2
            set prefix 10.10.1.0 255.255.255.0
        next
        edit 3
            set prefix 192.168.1.0 255.255.255.0
        next
        edit 4
            set prefix 10.12.10.0 255.255.255.0
        next
    end
```

Nota. Tomado del sistema Operativo FortiOS

e) Enrutamiento dinámico en los enrutadores de la agencia principal y el firewall

En la Figura 31, se muestra la siguiente configuración. El sistema Autónomo local es 65130, estableceremos la sesión BGP con el Sistema Autónomo 65120 (Firewall), desactivaremos el comando *output.default-originate debido a que este enrutador no anunciara una ruta por defecto hacia el firewall lo que anunciara serán los segmentos LAN de las agencias, en la configuración de *Network=RED_LAN / se encuentran los segmentos configurados que anunciaremos al firewall para que estas redes puedan tener navegación.

Figura 31

Configuración BGP entre el enrutador principal y el firewall.

```
/routing bgp connection
add address-families=ip as=65130 disabled=no hold-time=6s keepalive-time=2s local.address=10.44.170.6 \
    .role=ebgp name=BGP-ISA-PRI nexthop-choice=default output.default-originate=never .network=RED_LAN \
    remote.address=10.44.170.5/32 .as=65120 router-id=10.44.170.6 routing-table=main templates=temp1

/ip firewall address-list
add address=172.16.0.0/16 list=RED_LAN
add address=10.10.1.0/24 list=RED_LAN
add address=192.168.85.0/24 list=RED_LAN
add address=10.17.1.0/24 list=RED_LAN
add address=192.168.1.0/24 list=RED_LAN
add address=10.12.10.0/24 list=RED_LAN
```

Nota. Tomado de RouterOS – Winbox

Se realizó la configuración de netwatch para escanear el estado de enlace a nivel WAN, definiendo el siguiente script mostrado en la Figura 32, el host de monitoreo es 10.44.170.5 si en intervalo de 10 segundos no se tiene respuesta de este host la VRRP_1 actuará bajando la prioridad de 200 a 50, ósea el enrutador cambiará de estado de activo a standby y realizará la conmutación de enlace por el backup.

Figura 32

Configuración de netwatch entre el enrutador principal y la red backbone

```
/tool netwatch
add disabled=no down-script="interface vrrp set vrrp1 priority=50" host=10.44.170.5
http-codes="" interval=\
    10s test-script="" timeout=10ms type=simple up-script="interface vrrp set vrrp1
priority=200"
```

Nota. Tomado de RouterOS – Winbox

f) Configuración de BGP entre el enrutador backup y el firewall.

Estableceremos una sesión BGP entre el enrutador backup con el firewall, en la Figura 33, podemos notar la configuración del peer remoto, el AS remoto y las redes LAN que anunciaremos.

Figura 33

Configuración BGP entre el enrutador backup y el firewall.

```
/routing bgp connection
add address-families=ip as=65130 disabled=no hold-time=6s keepalive-time=2s
local.address=10.35.46.90 .role=ebgp name=BGP-ISA-BK nexthop-choice=default
output.default-originate=never .network=RED_LAN \
    remote.address=10.35.46.89/32 .as=65120 router-id=10.35.46.90 routing-table=main
templates=temp1

/ip firewall address-list
add address=172.16.0.0/16 list=RED_LAN
add address=192.168.0.0/16 list=RED_LAN
add address=192.168.1.0/24 list=RED_LAN
add address=10.12.10.0/24 list=RED_LAN
add address=10.17.1.0/24 list=RED_LAN
add address=10.10.1.0/24 list=RED_LAN
```

Nota. Tomado de RouterOS – Winbox

Una vez finalizado la configuración de alta redundancia entre las agencias de la entidad bancaria con el firewall procederemos en el siguiente capitulo a configurar la navegación segura.

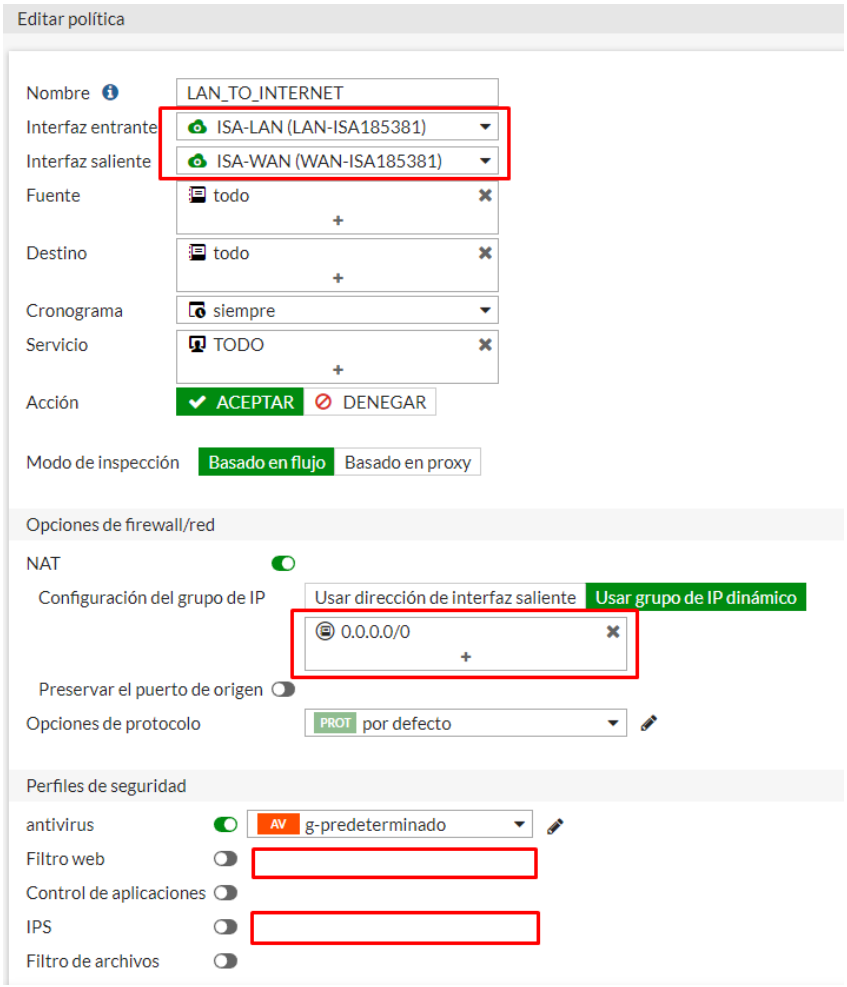
g) Configuración de NAT y Política de navegación

Se realiza el nateo para traducción de IP, para este caso traduciremos el segmento LAN de la entidad bancaria con la primera IP PUBLICA disponible. Para poder tener salida a internet desde las agencias es indispensable crear la política de navegación, sin esta no podrían navegar, la lógica de configuración es siempre de LAN a WAN.

En la Figura 34, creamos la política con interfaz origen LAN e interfaz salida WAN, como política inicial tanto el origen o fuente como el destino permitiremos todo, en el apartado de NAT usamos el grupo de IP dinámico y seleccionamos la IP publica con la que natearemos la red LAN, de momento no crearemos sobre esta política filtros web ni IPS (prevención de intrusiones).

Figura 34

Política básica para navegación



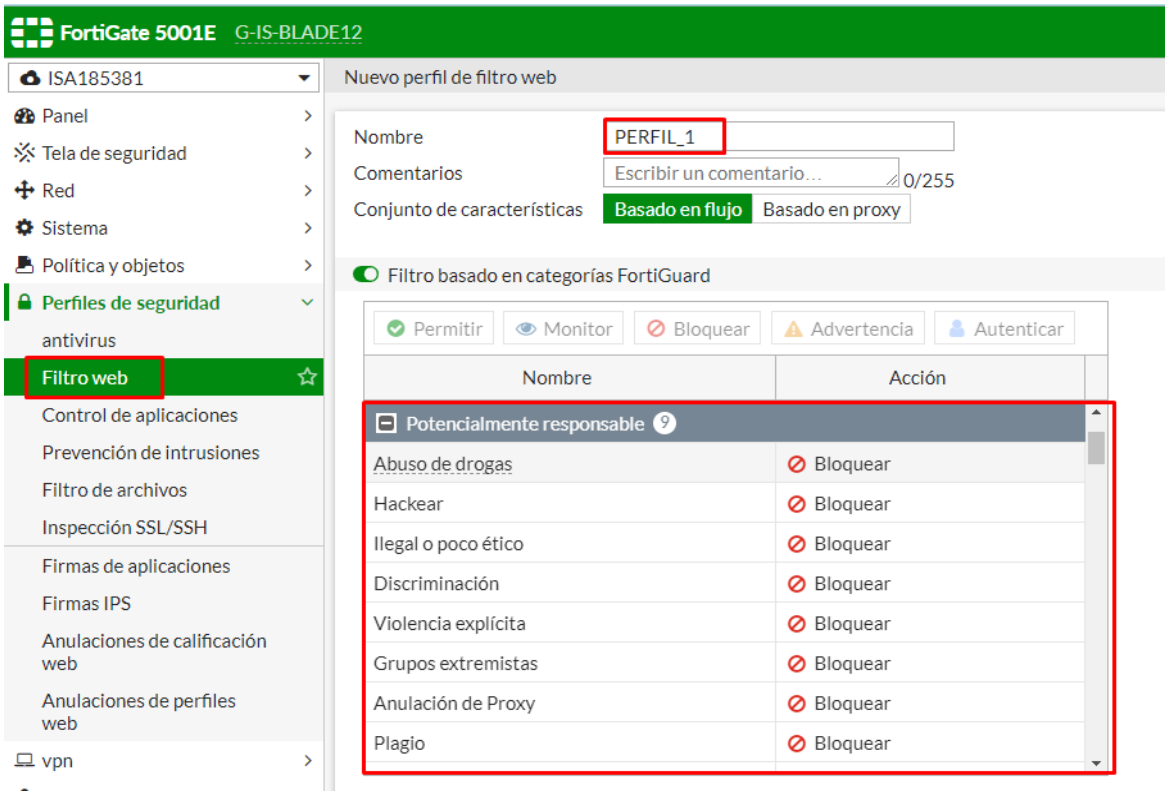
Nota. Tomado del sistema Operativo FortiOS

h) Creación de perfil para filtros web.

En la Figura 35, configuraremos un perfil “PERFIL_1” con los filtros web bloqueando destinos y categorías con riesgo medio y alto, en el Anexo 5 muestro una tabla de categorías en la cual por buenas prácticas se estará bloqueando y permitiendo.

Figura 35

Configuración de perfil para filtro web.



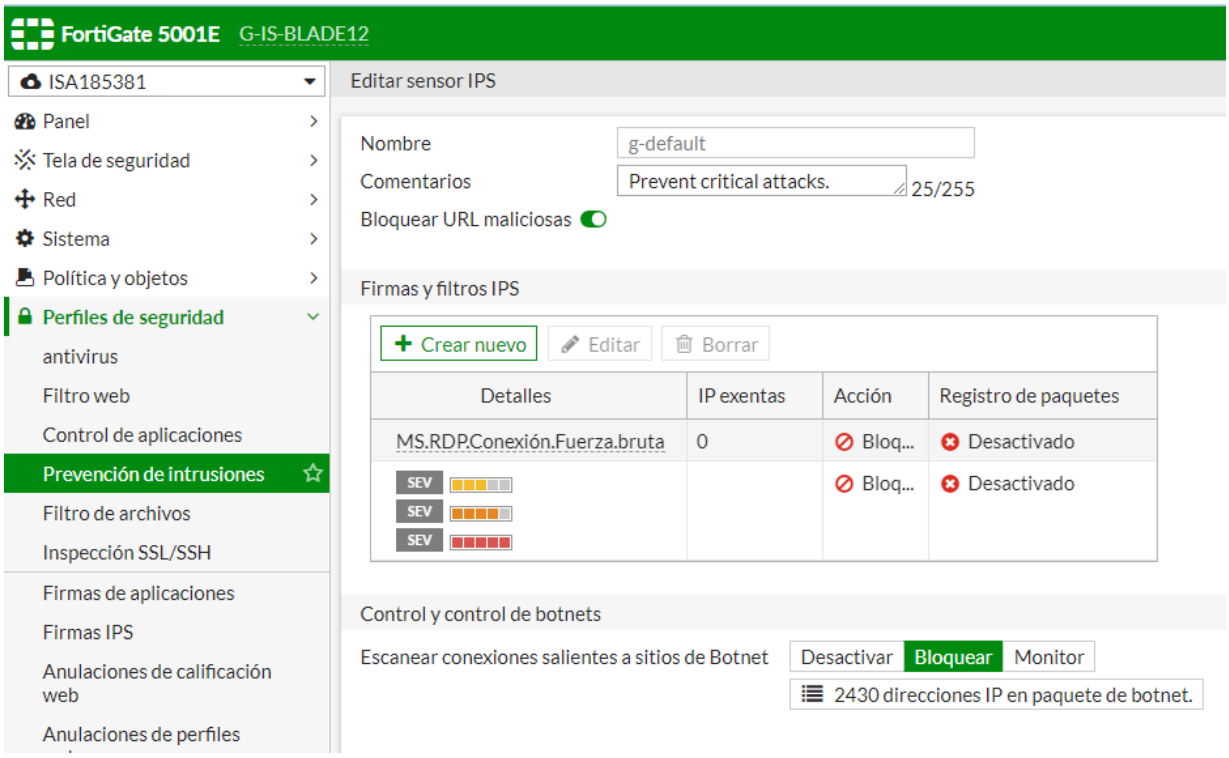
Nota. Tomado del sistema Operativo FortiOS.

i) Creación de perfil IPS

Bajo este perfil creado como se muestras en la Figura 36, bloquearemos todo destino SEVERO categorizado como medio y grave, Fortinet realiza una inspección con sus ingenieros de ciberseguridad y van actualizando esta base de datos, adicional con este perfil estamos bloqueando 2430 IP PUBLICAS categorizadas como botnets.

Figura 36

Perfil de creación de intrusiones IPS, en Fortinet.



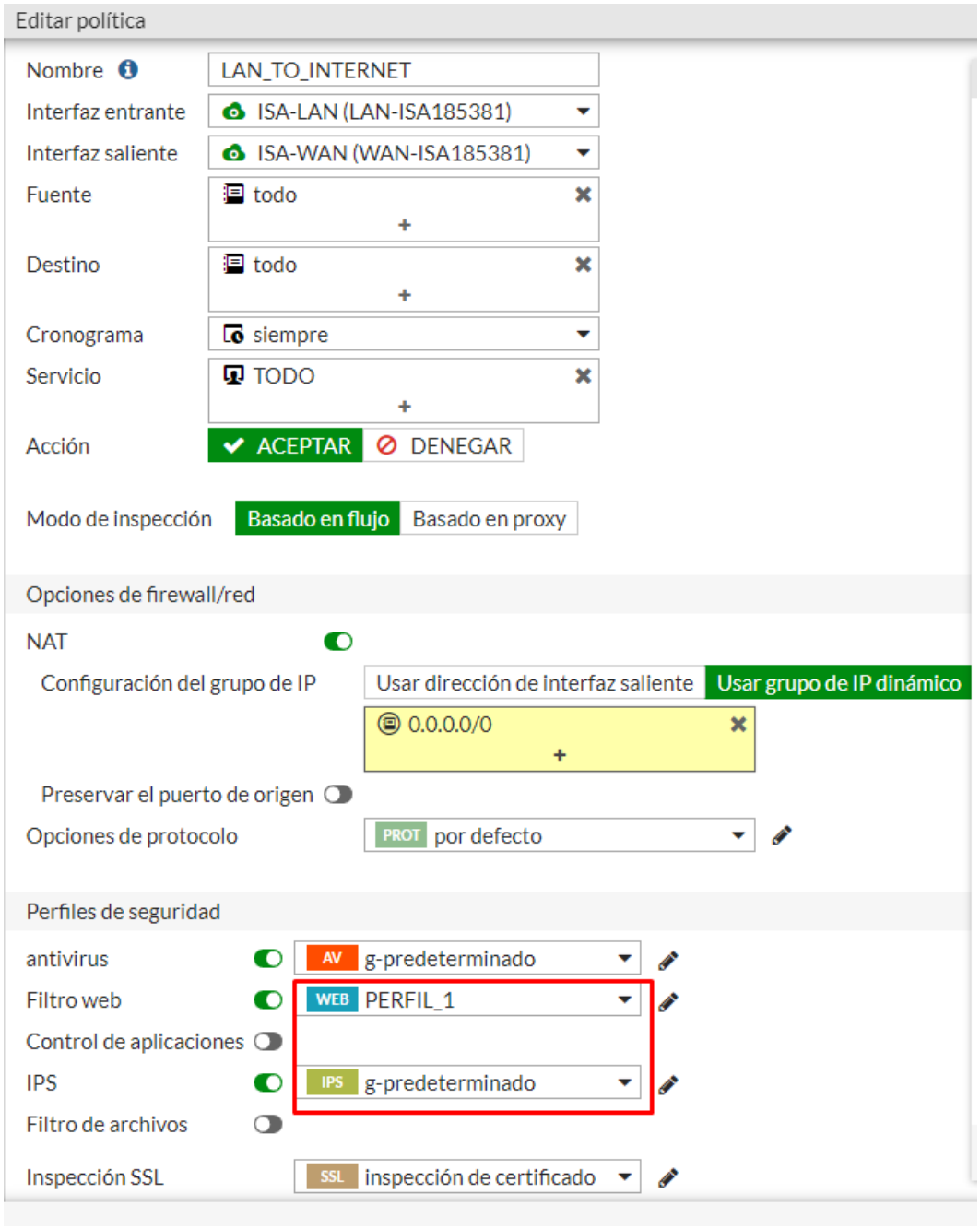
Nota. Tomado del sistema Operativo FortiOS.

j) Configuración de política de navegación final.

Como último proceso de configuración, En la Figura 37, definiremos una política de navegación final de LAN a WAN, agregando los perfiles de filtros web, IPS y antivirus, con esta política la agencia principal y remota podrán navegar a internet.

Figura 37

Política de Navegación con perfiles de seguridad.



Nota. Tomado del sistema Operativo FortiOS

3.3 Resultados

Se detalla los resultados obtenidos luego de concluir con la implementación y configuración para los servicios de enlace de datos e Internet seguro.

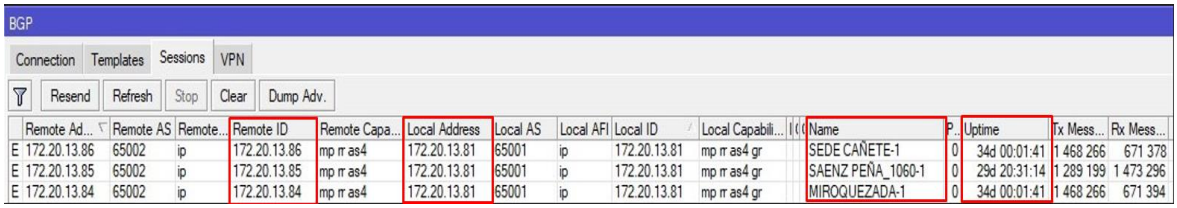
3.3.1 Resultados para el servicio en enlace de datos

a. Como primer punto se valida el establecimiento de sesión BGP entre el enrutador principal y las agencias remotas.

En la Figura 38, se muestra el establecimiento de sesión BGP (local address) con las 3 agencias remotas (remote ID), y el tiempo en la cual se encuentra activo el enlace (uptime)

Figura 38

Estado de sesión BGP entre el enrutador principal y las 3 agencias remotas.



Nota. Tomado de RouterOS – Winbox.

b. Realizaremos una prueba ICMP en una de las agencias remotas para verificar el camino que toma en llegar hasta el conmutador del cliente alojado en la agencia principal.

En la Figura 39, hicimos una prueba ping desde la agencia Antonio Miróquezada con segmento LAN 10.12.10.0/24 hacia la agencia principal con segmento LAN 172.16.0.0/16 y podemos notar que de los 4 paquetes enviados se recibieron 4 sin ninguna perdida y el tiempo de respuesta es menor al orden de los decimales, adicional a ello, se realizó una traza para verificar los saltos o ruta, notamos que realiza 2 saltos:

- ✓ 172.20.13.81 / Esta IP corresponde a la IP WAN del enrutador principal en la agencia principal.
- ✓ 172.16.1.28 / Este es el host a la cual se realizó la prueba, completando la traza.

Con esta prueba validamos que la conectividad entre sedes toma el camino por el R1 enrutador principal según el diseño mostrado en la Figura 14.

Figura 39

Prueba ICMP desde la red LAN de la agencia Miróquezada a un host en la agencia principal- Antes del corte.

```
[adminoptical@CID185385] > tool traceroute 172.16.1.28 src-address=10.12.10.1
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST
 1 172.20.13.81                      0%    3   0.2ms     0.2     0.2     0.2
 2 172.16.1.28                       0%    3   0.4ms     0.4     0.4     0.5

[adminoptical@CID185385] > ping 172.16.1.28 src-address=10.12.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.16.1.28                                56  62 0ms
    1 172.16.1.28                                56  62 0ms
    2 172.16.1.28                                56  62 0ms
    3 172.16.1.28                                56  62 0ms
    sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

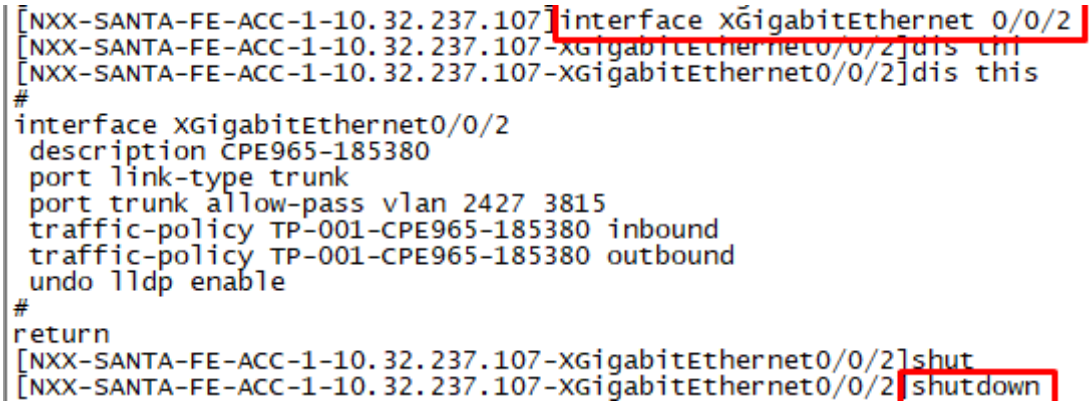
Nota. Ping y traza como origen 10.12.10.1 con destino 172.16.1.28. Tomado de RouterOS – Winbox

c. Validar la conmutación automática de los servicios simulando caída del enlace principal a nivel WAN.

Para realizar esta prueba es necesario simular una avería en R1, en la Figura 40, muestro el proceso para apagar la interfaz que conecta R1 al enrutador en la backbone.

Figura 40

Prueba apagando la interfaz del enrutador de la backbone que interconecta al enrutador R1 de la agencia principal



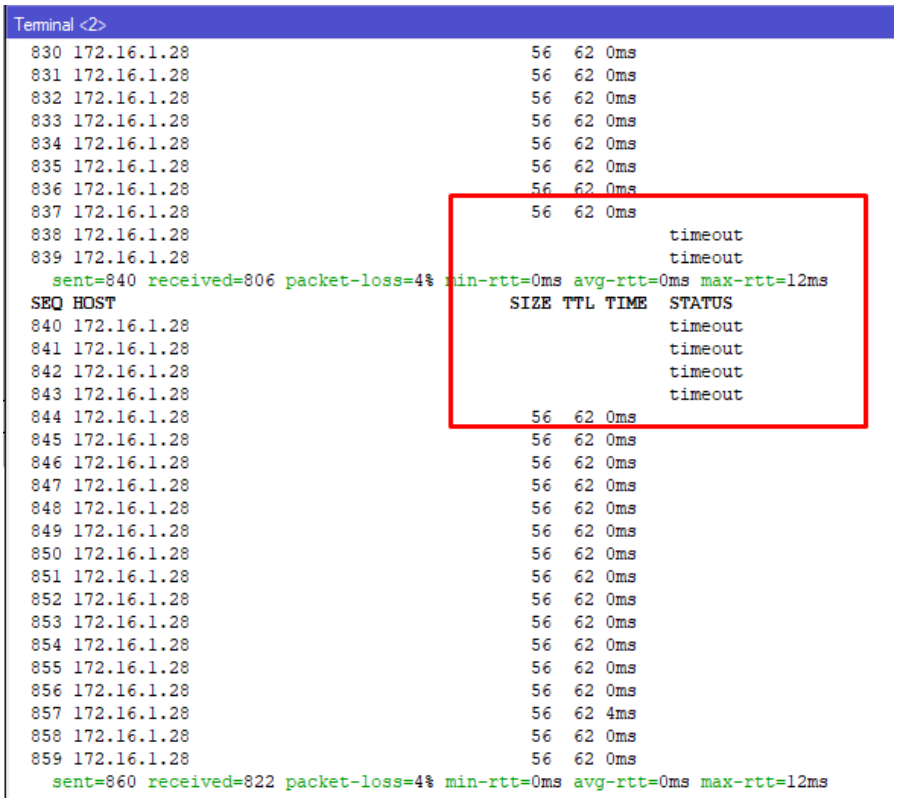
Nota. Tomado de SecureCRT

A continuación, paralelo a apagar la interfaz se realizó un ping y traza constante como origen 10.12.10.1 y destino 172.16.1.28 para monitorear el estado de enlace.

Como se verifica en la Figura 41, se perdieron 6 paquetes en el proceso de conmutación de enlace, lo cual es óptimo para este escenario, en la Figura 42 verificamos la traza que el salto al host destino lo realiza por el R2 enrutador secundario.

Figura 41

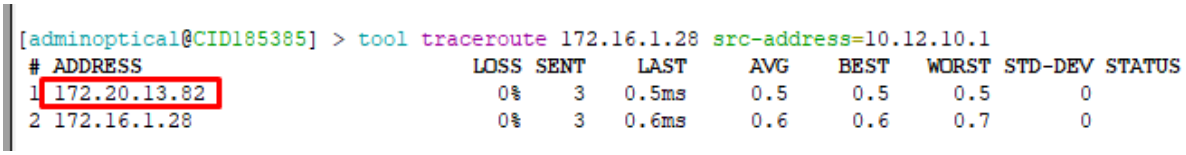
Ping desde la red LAN de la agencia Miróquezada a un host en la agencia principal - Durante el corte



Nota. Tomado de RouterOS – Winbox

Figura 42

Traza desde la red LAN de la agencia Miróquezada a un host en la agencia principal - Durante el corte



Nota. Tomado de RouterOS – Winbox

Con ello demostramos confiabilidad y alta redundancia en el servicio de interconexión de agencias, si la ruta principal se interrumpe automáticamente conmuta por la ruta backup.

3.3.2 Resultados para el servicio en Internet Seguro

- Como primer punto validamos el establecimiento de sesión BGP entre el firewall y los enrutadores de la agencia principal.

En la Figura 43, validamos el establecimiento de sesión BGP entre el firewall y los 2 enrutadores de la agencia principal.

Figura 43

Estado de sesión BGP entre el firewall y los enrutadores en la agencia principal.

```
G-IS-BLADE12 (ISA185381) $ get router info bgp summary
VRF 0 BGP router identifier 45.231.82.131, local AS number 65120
BGP table version is 15
11 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.35.46.90 4      65130 1838547 1839029       14    0    0 01w3d00h        4
10.44.170.6 4      65130 1962153 1962774       14    0    0 01w3d00h        5

Total number of neighbors 2
```

Fuente: Tomado del sistema Operativo FortiOS

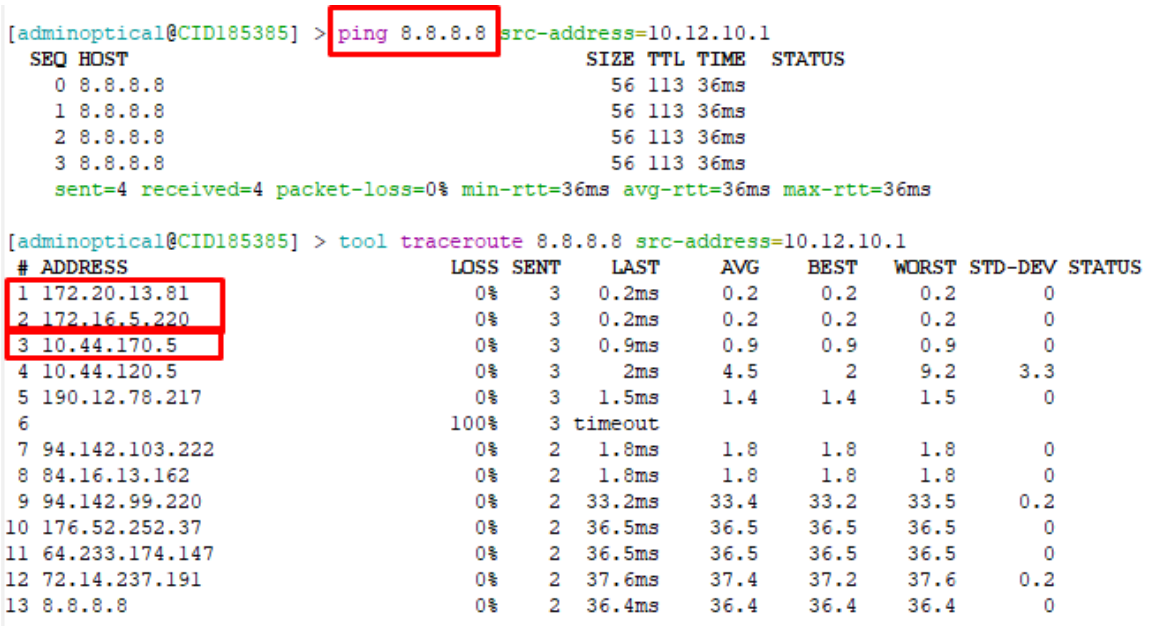
- Realizaremos una prueba ICMP en una de las agencias remotas para verificar el camino que toma para navegación a internet.

En la Figura 44, se realizó una prueba ping y traza desde la agencia Antonio Miróquezada con segmento LAN 10.12.10.0/24 hacia las DNS de Google. Se verifica navegación exitosa por la prueba Ping.

En la traza realizada podemos verificar que la ruta que toma es R1 y R3 es decir el enrutador principal del servicio de enlace de datos y el enrutador principal del servicio de internet seguro. De acuerdo con el diseño propuesto en la Figura 16. La consulta está siguiendo la ruta principal de ambos servicios.

Figura 44

Prueba ICMP desde la red LAN de la agencia Miróquezada hacia las DNS de Google - Antes del corte



```
[adminoptical@CID185385] > ping 8.8.8.8 src-address=10.12.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56 113 36ms
    1 8.8.8.8                                    56 113 36ms
    2 8.8.8.8                                    56 113 36ms
    3 8.8.8.8                                    56 113 36ms
    sent=4 received=4 packet-loss=0% min-rtt=36ms avg-rtt=36ms max-rtt=36ms

[adminoptical@CID185385] > tool traceroute 8.8.8.8 src-address=10.12.10.1
 # ADDRESS                                LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 172.20.13.81                            0%    3   0.2ms     0.2     0.2     0.2       0
 2 172.16.5.220                            0%    3   0.2ms     0.2     0.2     0.2       0
 3 10.44.170.5                             0%    3   0.9ms     0.9     0.9     0.9       0
 4 10.44.120.5                             0%    3     2ms     4.5       2     9.2     3.3
 5 190.12.78.217                           0%    3   1.5ms     1.4     1.4     1.5       0
 6                                        100%    3 timeout
 7 94.142.103.222                          0%    2   1.8ms     1.8     1.8     1.8       0
 8 84.16.13.162                            0%    2   1.8ms     1.8     1.8     1.8       0
 9 94.142.99.220                           0%    2  33.2ms    33.4    33.2    33.5     0.2
10 176.52.252.37                           0%    2  36.5ms    36.5    36.5    36.5       0
11 64.233.174.147                          0%    2  36.5ms    36.5    36.5    36.5       0
12 72.14.237.191                           0%    2  37.6ms    37.4    37.2    37.6     0.2
13 8.8.8.8                                 0%    2  36.4ms    36.4    36.4    36.4       0
```

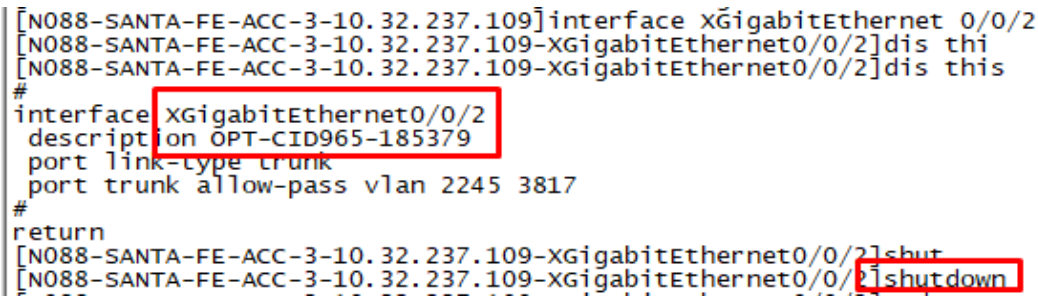
Nota. Tomado de RouterOS – Winbox

- Validar la conmutación automática de los servicios simulando caída del enlace principal a nivel WAN.

Para realizar esta prueba es necesario simular una avería en R3, en la Figura 45, muestro el proceso para apagar la interfaz que conecta R3 al enrutador en la backbone.

Figura 45

Prueba apagando la interfaz del enrutador de la backbone que interconecta al enrutador R3 de la agencia principal



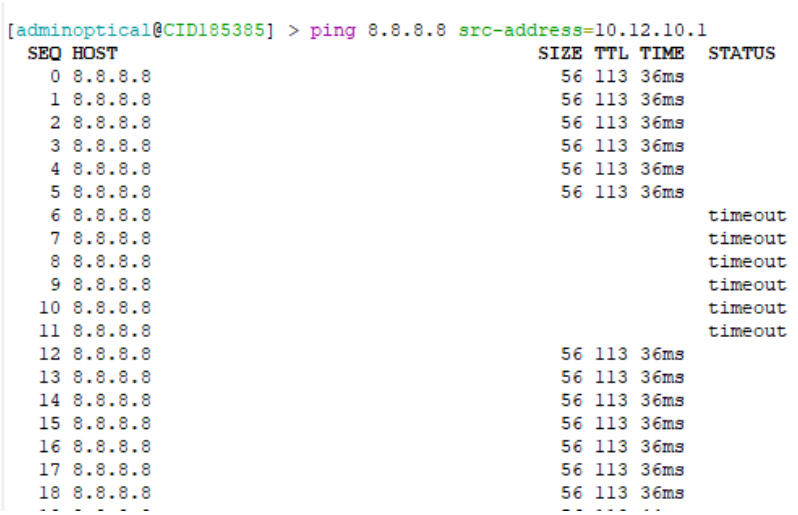
```
[N088-SANTA-FE-ACC-3-10.32.237.109]interface XGigabitEthernet 0/0/2
[N088-SANTA-FE-ACC-3-10.32.237.109-XGigabitEthernet0/0/2]dis thi
[N088-SANTA-FE-ACC-3-10.32.237.109-XGigabitEthernet0/0/2]dis this
#
interface XGigabitEthernet0/0/2
 description OPT-CID965-185379
 port link-type trunk
 port trunk allow-pass vlan 2245 3817
#
return
[N088-SANTA-FE-ACC-3-10.32.237.109-XGigabitEthernet0/0/2]shut
[N088-SANTA-FE-ACC-3-10.32.237.109-XGigabitEthernet0/0/2]shutdown
```

Nota. Tomado de SecureCRT

Se realizó ping y traza constante como origen 10.12.10.1 y destino las DNS de Google. Como se verifica en la Figura 46 se perdieron 6 paquetes en el proceso de conmutación de enlace, lo cual es óptimo para este escenario, en la Figura 47, verificamos la traza que el salto al host destino lo realiza por el R4 enrutador secundario.

Figura 46

Ping desde la red LAN de la agencia Miróquezada a las DNS de Google – durante el corte

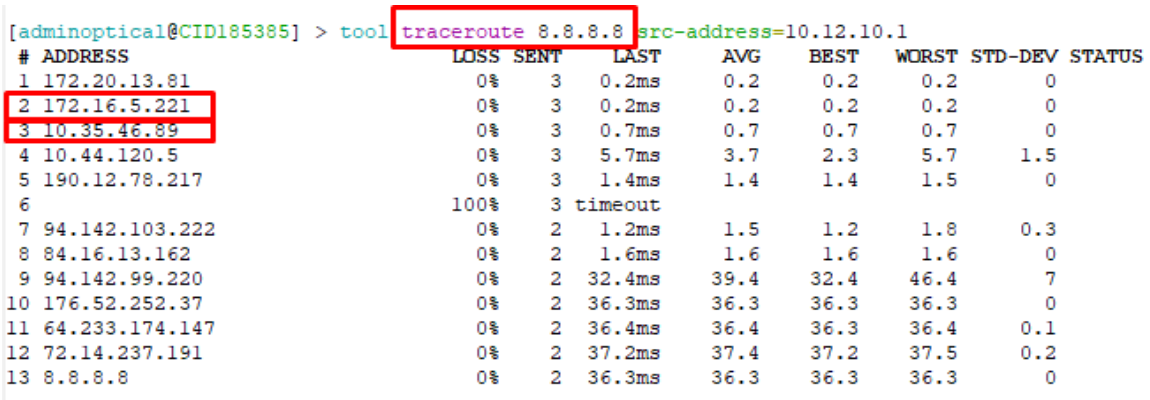


```
[adminoptical@CID185385] > ping 8.8.8.8 src-address=10.12.10.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56 113 36ms
    1 8.8.8.8                                    56 113 36ms
    2 8.8.8.8                                    56 113 36ms
    3 8.8.8.8                                    56 113 36ms
    4 8.8.8.8                                    56 113 36ms
    5 8.8.8.8                                    56 113 36ms
    6 8.8.8.8                                               timeout
    7 8.8.8.8                                               timeout
    8 8.8.8.8                                               timeout
    9 8.8.8.8                                               timeout
   10 8.8.8.8                                               timeout
   11 8.8.8.8                                               timeout
   12 8.8.8.8                                    56 113 36ms
   13 8.8.8.8                                    56 113 36ms
   14 8.8.8.8                                    56 113 36ms
   15 8.8.8.8                                    56 113 36ms
   16 8.8.8.8                                    56 113 36ms
   17 8.8.8.8                                    56 113 36ms
   18 8.8.8.8                                    56 113 36ms
```

Nota. Tomado de RouterOS – Winbox

Figura 47

Traza desde la red LAN de la agencia Miróquezada a las DNS de Google – durante el corte



```
[adminoptical@CID185385] > tool traceroute 8.8.8.8 src-address=10.12.10.1
 # ADDRESS                                LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 172.20.13.81                             0%    3     0.2ms     0.2     0.2     0.2       0
 2 172.16.5.221                             0%    3     0.2ms     0.2     0.2     0.2       0
 3 10.35.46.89                              0%    3     0.7ms     0.7     0.7     0.7       0
 4 10.44.120.5                              0%    3     5.7ms     3.7     2.3     5.7     1.5
 5 190.12.78.217                            0%    3     1.4ms     1.4     1.4     1.5       0
 6                                        100%    3 timeout
 7 94.142.103.222                           0%    2     1.2ms     1.5     1.2     1.8     0.3
 8 84.16.13.162                             0%    2     1.6ms     1.6     1.6     1.6       0
 9 94.142.99.220                            0%    2    32.4ms    39.4    32.4    46.4       7
10 176.52.252.37                            0%    2    36.3ms    36.3    36.3    36.3       0
11 64.233.174.147                           0%    2    36.4ms    36.4    36.3    36.4     0.1
12 72.14.237.191                            0%    2    37.2ms    37.4    37.2    37.5     0.2
13 8.8.8.8                                  0%    2    36.3ms    36.3    36.3    36.3       0
```

Nota. Tomado de RouterOS – Winbox

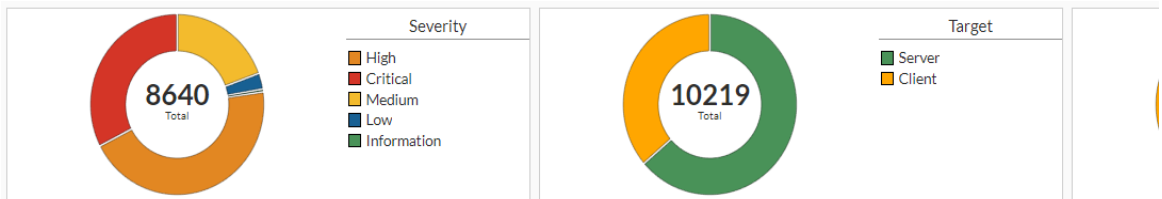
De acuerdo con el diseño de internet seguro este escenario se verifica en la Figura 17. Con esta prueba se demostró alta redundancia para la navegación desde las agencias de la entidad bancaria.

- Validar la limitación hacia destinos maliciosos a través del internet seguro.

La entidad bancaria cuenta con protección IPS (Sistema de prevención de intrusiones), en la Figura 48, podemos verificar que la entidad cuenta con 8640 registros de ataques bloqueados en el campo IPS Signature y acción, calificados por tipo de gravedad “severity”

Figura 48

Servicio de sistema de prevención de intrusiones



Create New | Edit | Delete | Search

Name	Severity	Tar...	OS	Action	CVE-ID
IPS Signature 8640					
Opera.Configuration.Overwrite		Client	All	Block	
NUUO.Network.Video.Recorder.Remote.Command.Execution		Server	Linux	Block	CVE-2019-9653
Libvpx.vp8.encoding.Heap.Buffer.Overflow		Client	All	Block	CVE-2023-5217
3Com.Intelligent.Management.Center.Information.Disclosure		Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux	Block	
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux	Block	
D-Link.D-View.JWT.Static.Key.Authentication.Bypass		Server	Linux	Block	CVE-2023-5074
Libwebp.BuildHuffmanTable.Heap.Buffer.Overflow		Server Client	All	Block	CVE-2023-4863 CVE-2023-41064
Wordpress.File.Manager.Pro.Plugin.CSRF		Server	All	Block	CVE-2023-4827
F5.BIG-IP.TMUI.AJP.Smuggling.Authentication.Bypass		Server	Linux	Block	CVE-2023-46747
Apache.ActiveMQ.CVE-2023-46604.Code.Execution		Server	All	Block	CVE-2023-46604
A32S.Botnet		Server Client	All	Block	
AAEH.Botnet		Server	All	Block	
AARC.Botnet		Client	All	Block	
ABBS.Audio.Media.Player.LST.Buffer.Overflow		Server Client	Windows	Block	

Fuente: Tomado del sistema Operativo FortiOS

En la Figura 49, nos muestra que la entidad bancaria tuvo 3 intentos de ataque en los últimos 50 minutos desde las IP publicas 91.92.243.203, 68.183.234.223, 31.220.96.219, la acción fue “dropped” o eliminada por el Firewall.

Figura 49

Servicio de sistema de prevención de intrusiones

Date/Time		Severity	Source	P...	U...	Action	C...	Attack Name
29 minutes ago			91.92.243.203	6		dropped		Mirai.Botnet
40 minutes ago			68.183.234.223	6		dropped		WordPress.xmlrpc.php.system.multicall.Amplification.Attack
46 minutes ago			31.220.96.219	6		dropped		AndroxGh0st.Malware

Fuente: Tomado del sistema Operativo FortiOS

En la Figura 50, se muestra logs o eventos de navegación con acción “passthrough” o permitido, siendo estos destinos seguros de acuerdo con la política configurada.

Figura 50

Logs de los filtros Web Acción permitido.

Policy ID: 26 OR NOT Add Filter

Date/Time	Action	URL
5 minutes ago	passthrough	https://edge.microsoft.com/
7 minutes ago	passthrough	https://candclist.gdatasecurity.de/
7 minutes ago	passthrough	https://edge.microsoft.com/
11 minutes ago	passthrough	https://candclist.gdatasecurity.de/
11 minutes ago	passthrough	https://candclist.gdatasecurity.de/
17 minutes ago	passthrough	https://settings-win.data.microsoft.com/
17 minutes ago	passthrough	https://settings-win.data.microsoft.com/
17 minutes ago	passthrough	https://settings-win.data.microsoft.com/
17 minutes ago	passthrough	https://candclist.gdatasecurity.de/
22 minutes ago	passthrough	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallow...
23 minutes ago	passthrough	https://candclist.gdatasecurity.de/
23 minutes ago	passthrough	https://v10.events.data.microsoft.com/
48 minutes ago	passthrough	https://settings-win.data.microsoft.com/
48 minutes ago	passthrough	https://candclist.gdatasecurity.de/
52 minutes ago	passthrough	https://candclist.gdatasecurity.de/
52 minutes ago	passthrough	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinruless...
52 minutes ago	passthrough	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx/h0Ztl+...
53 minutes ago	passthrough	https://v10.events.data.microsoft.com/
53 minutes ago	passthrough	https://candclist.gdatasecurity.de/
54 minutes ago	passthrough	https://data-edge.smartscreen.microsoft.com/
54 minutes ago	passthrough	https://candclist.gdatasecurity.de/
54 minutes ago	passthrough	https://ping-edge.smartscreen.microsoft.com/

Nota. Tomado del sistema Operativo FortiOS.

En la Figura 51, se muestran los logs o eventos de navegación con acción “block” o bloqueado, siendo estos destinos categorizados como riesgo medio o alto de acuerdo con la política generada para navegación.

Figura 51

Logs de los filtros Web acción bloqueado.

Date/Time		Destination	Action
2 minutes ago		190.196.215.59 (mirror.orbyta.com)	block
2 minutes ago		200.25.7.49 (edgeuno-bog2.mm.fcix.net)	block
2 minutes ago		201.159.221.67 (mirror.cedia.org.ec)	block
2 minutes ago		201.159.221.67 (mirror.cedia.org.ec)	block
2 minutes ago		200.129.163.17 (mirror.ufam.edu.br)	block
2 minutes ago		200.136.207.1 (mirror.ufscar.br)	block
2 minutes ago		200.75.160.21 (mirror.megalink.com)	block
2 minutes ago		200.9.157.182 (mirrors.eze.sysarmy.com)	block
2 minutes ago		163.178.174.25 (mirrors.ucr.ac.cr)	block
2 minutes ago		190.196.215.59 (mirror.orbyta.com)	block
2 minutes ago		200.25.7.49 (edgeuno-bog2.mm.fcix.net)	block
2 minutes ago		201.159.221.67 (mirror.cedia.org.ec)	block
2 minutes ago		201.159.221.67 (mirror.cedia.org.ec)	block
2 minutes ago		200.129.163.17 (mirror.ufam.edu.br)	block
2 minutes ago		200.136.207.1 (mirror.ufscar.br)	block

Nota. Tomado del sistema Operativo FortiOS.

CONCLUSIONES

- Se diseñó una red de alta disponibilidad con enrutamiento dinámico para la interconexión de agencias y navegación a internet, donde un enlace es declarado principal y el otro redundante. Los enlaces logran mantener activo los servicios ante alguna falla a nivel físico o lógico, mejorando así la confiabilidad y disponibilidad de los servicios frente al anterior proveedor TDP.

- En cuanto a la implementación de configuración de los equipos de red para interconectar las agencias y el firewall, se logró a través de los protocolos BGP y VRRP establecer comunicación entre agencias y conmutación de enlaces de forma dinámica.

- Se realizó la configuración de políticas en el firewall, permitiendo la navegación a internet únicamente de los segmentos LAN de las agencias. Las pruebas realizadas fueron a través ICMP a las DNS de Google siendo estas exitosas.

- Se realizó con éxito las pruebas de redundancia de red, determinando que cuando el enlace principal sufre una avería, el enlace secundario tiene la capacidad de asumir el rol principal, el tiempo de convergencia es mínimo, durante la conmutación de enlace se perdieron 6 paquetes luego de ello restableció la conectividad entre agencias y la navegación a internet.

- Se ha logrado mediante políticas de navegación que incluyen configuraciones como filtros web e IPS, limitar destinos con riesgo medio y alto, así como bloquear todo tipo de ataques que afecten los host y servicios publicados desde los servidores de la entidad bancaria.

RECOMENDACIONES

- Recomiendo para futuras investigaciones aplicar balanceo de carga a través de atributos de BGP, con ello se podría optimizar el ancho de banda y la calidad de servicio.

- Recomiendo para futuras investigaciones e implementaciones revisar la solución SDN o SDWAN, con esta solución las empresas podrían tener alta redundancia con seguridad de red con un solo equipo perimetral, ahorrando CAPEX.

- Para soluciones de alta redundancia con diferentes proveedores de servicio se recomienda configurar iBGP u OSPF en lugar de VRRP o HSRP.

- Se recomienda mantener actualizado el firmware a las versiones recomendadas por el fabricante en los firewalls, cabe resaltar que estas actualizaciones corrigen graves brechas de seguridad y bugs críticos.

- Recomiendo utilizar este diseño y solución para pequeñas, medianas y grandes empresas.

REFERENCIAS BIBLIOGRÁFICAS

Aliaga Arce, J. O. Diseño de una red GPON, para el Municipio de Achacachi del Departamento de La Paz (Doctoral dissertation).

Ciriaco Susanibar, N. A. (2021). Optimización Del Servicio De Red Con El Respaldo Del Enlace A Internet Wan Y La Seguridad Perimetral Para La Empresa Sonepar Sede Lima (Doctoral dissertation, Universidad Nacional Tecnológica de Lima Sur).

Cisco. (2023, September 6). What is a lan? Local Area Network. Cisco. https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-

Cisco. (2023, August 15). What is a wan? wide-area network. Cisco. https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html?dtid=osscdc000283

Cisco. (2023, August 30). Enrutamiento de IP. Cisco. https://www.cisco.com/c/es_mx/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html

D. McPherson, IETF, RFC 4277, Experience with the BGP-4 Protocol 2006

Dordoigne, J., & Atelin, P. (2006). Redes informáticas. Editions ENI. Noviembre.

Ernesto Ariganello, & Enrique Barrientos Sevilla. (2010). Redes Cisco CCNP a Fondo (Alfaomega Grupo Editor, Ed.; Primera).

ESET (2023). ¿Qué es Ransonware? Recuperado de: https://www.eset.com/es/caracteristicas/ransomware/

Fortinet. (2023). Seguridad de red. Recuperado de https://www.fortinet.com/lat/products/next-generation-firewall

Fortinet. (2023). Servicio de filtrado web Fortiguard. Recuperado de https://www.fortinet.com/lat/support/support-services/fortiguard-security-subscriptions/web-filtering

Fortinet. (2023). Servicio de FortiGuard IPS. Recuperado de https://www.fortinet.com/lat/products/ips

Fortinet. (2023), Document Library, recuperado de https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/675558/fortiguard-filter

Gustavo Genez. (2020). Qué es backbone o red troncal y para qué se utiliza. 18 de diciembre de 2020

Guedrez, Dugeon, “Demonstration of Segment Routing with SDN Based Label Stack Optimization”, IEEE, 2017

Goitia, M. J. (2004). Protocolos de enrutamiento para la capa de red en arquitecturas de redes de datos. Argentina, Universidad Nacional de Nordeste, Departamento Informática.

IsoTools Excellence. (2021). Como administrar la seguridad de red según la norma ISO 27001. Recuperado de https://www.pmg-ssi.com/2016/07/como-administrar-la-seguridad-de-red-segun-la-norma-iso-27001/

ISO 27000. (2005). Serie27000. Recuperado De http://www.iso27000.es/iso27000.html

J.Moy, IETF, RFC 2328, OSPF versión 2, 1998

Lacnic (2023) Distribución de números de sistema autónomo (ASN). Recuperado de: https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomoas

Méndez, G. L. A., Muñoz, V. S., & Varney, P. S. (2010). Modelo de trabajo para el diseño e implementacion de redes en malla wifi como una solución para el acceso a banda ancha en áreas rurales. Revista GTI, 9(23), 59-73.

Mullo Pilamunga, X. E. (2019). Firewall para la seguridad de la red en los laboratorios de la Universidad Estatal de Bolívar.

Muñoz Martínez, A. (2019). Protocolo de enrutamiento dinámico BGP en redes de alta disponibilidad.

Olaya Toledo, D., & Benavides Guayacán, E. A. (2018). Diseño de un plan de contingencia para un enlace crítico del banco Financorp.

OrhanErgun (2023). ebgp-vs-ibgp. Recuperado de https://orhanergun.net/ebgp-vs-ibgp

Paredes Malpartida, L. H. (2021). Diseño de una red de proveedor de servicios de telecomunicaciones basado en Arquitectura SR-MPLS.

Rekhter, Li, Hares , IETF, RFC 4271, A Border Gateway Protocol 4 (BGP-4), 2006

Rodriguez Vigil, L. A. (2023). Optimización del sistema de interconexión, seguridad perimetral y de comunicación entre sedes de empresa minera con migración de tecnología MPLS a IP sobre enlaces dedicados de internet.

Ramírez Martínez, A. V. (2011). Diseño de la solución de seguridad y administración de tráfico WAN del enlace de Internet dedicado con alta disponibilidad para un campus universitario.

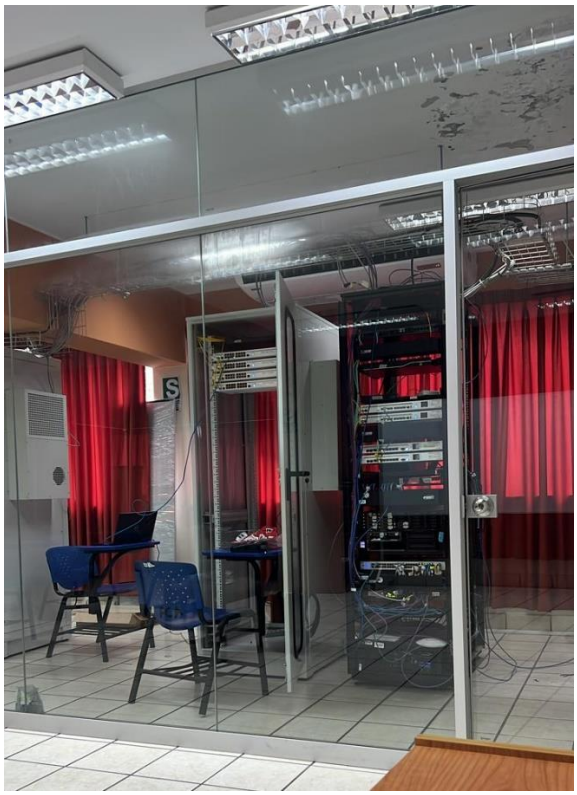
Perez Inca, J. N. (2023). Solución integral de networking y seguridad en alta disponibilidad en ZEGEL IPAE Año-2020.

Win empresas 2023. ¿Quiénes somos? Recuperado de: https://winempresas.pe/quienes-somos

Zscalers, 2023. Recuperado de: https://www.zscaler.es/press/zscalers-ransomware-report-2023-shows- global-ransomware-attack-growth-of-nearly-40-percent

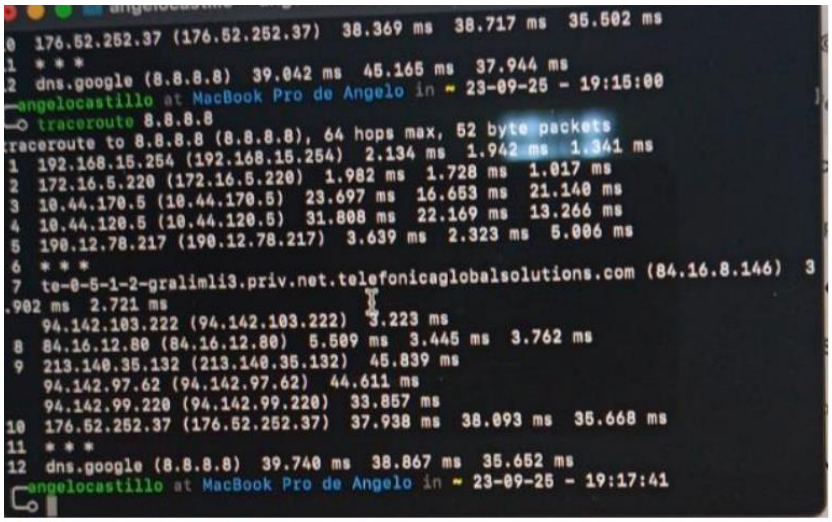
ANEXOS

ANEXO 1. Instalación de los 4 enrutadores Mikrotik CCR2004-16G-2S+ en la agencia principal.



ANEXO 2. Instalación del router Mikrotik RB3011 en una de las agencias remotas.

ANEXO 3. Traza a Google desde un servidor interno, se verifica que el salto es por el enrutador principal.

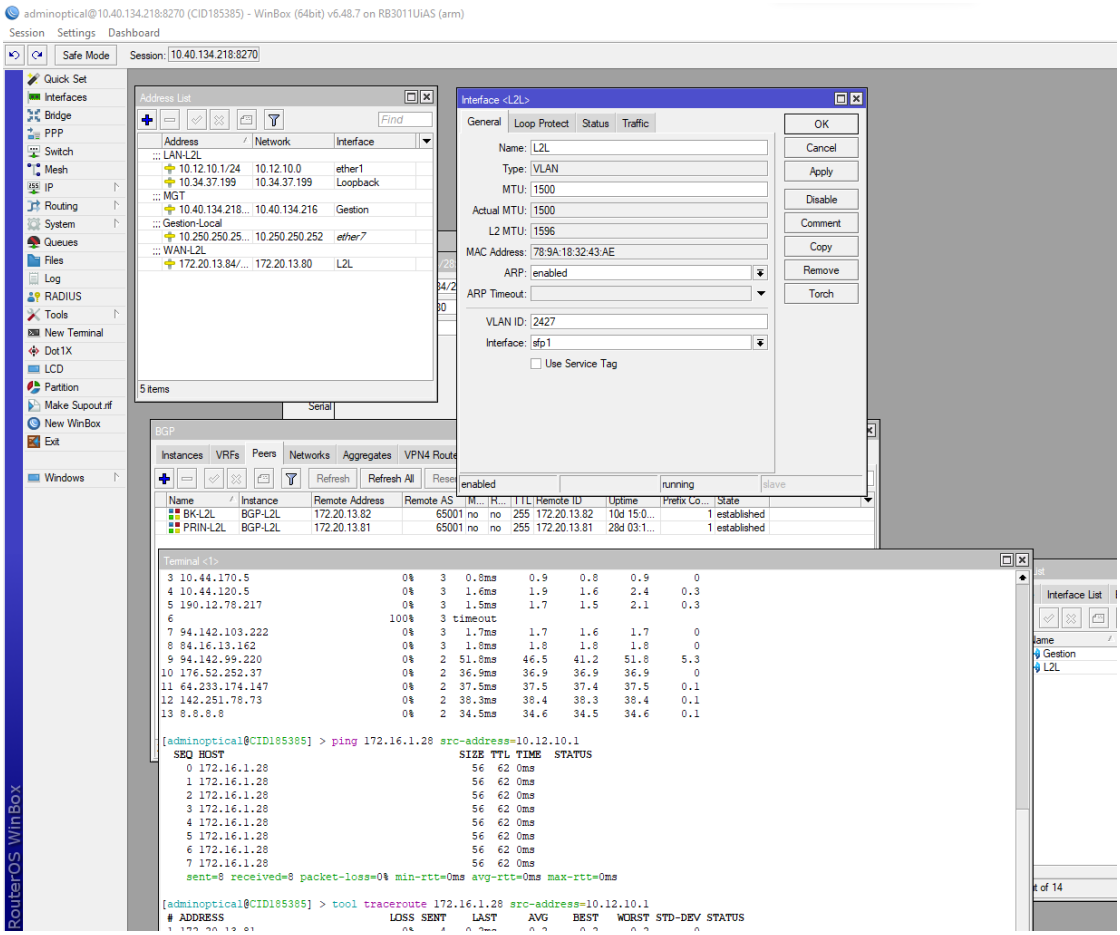


ANEXO 4. Traza a Google desde un servidor interno, se verifica que el salto es por el enrutador respaldo.

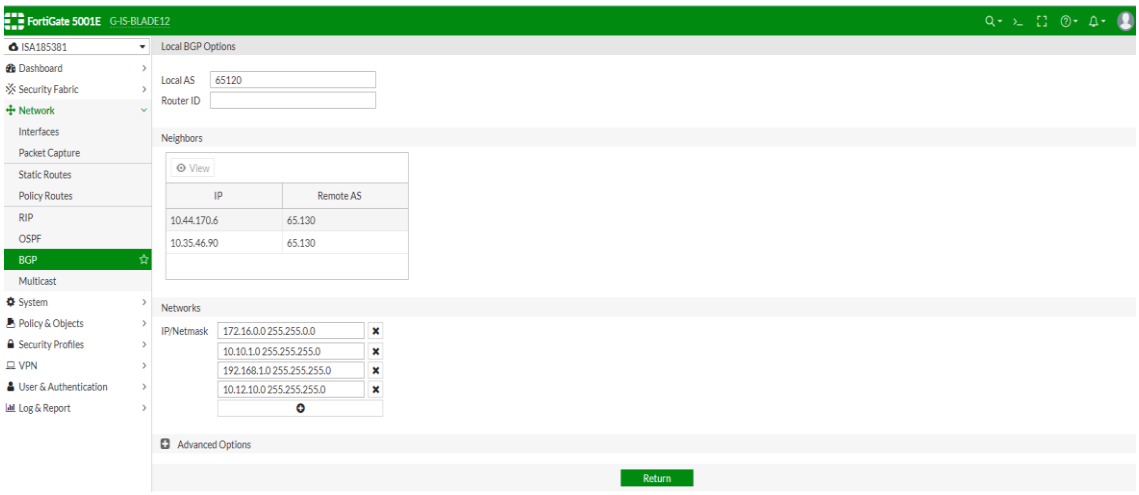
ANEXO 5. Categorías bloqueadas y permitidas por el Firewall o corta fuegos

categorías bloqueadas	**Categorías permitidas**
Potencialmente responsable	**Interés General - Negocios**
Violencia explícita	Finanzas y Banca
Discriminación	Motores de búsqueda y portales
Ilegal o poco ético	Organizaciones generales
Hackear	Negocio
Abuso de drogas	Seguridad de la Información y la Computación
Grupos extremistas	Organizaciones gubernamentales y legales
Anulación de Proxy	Tecnologías de la información
Plagio	Fuerzas Armadas
Abuso sexual infantil	Alojamiento web
Terrorismo	Sitios web seguros
Minería criptográfica	Aplicaciones basadas en web
Programa potencialmente no deseado	Organizaciones de caridad
Contenido para adultos/maduros	Acceso remoto
Creencias alternativas	analista de la red
Aborto	Reunión en línea
Otros materiales para adultos	Acortamiento de URL
Organizaciones de abogados	**Interés General - Personal**
Juego	Organizaciones políticas
Desnudez y riesgo	Noticias y medios
Pornografía	Medicamento
Tener una cita	Búsqueda de trabajo
Armas (Ventas)	Salud y Bienestar
Marijuana	Educación
Educación sexual	Arte y Cultura
Alcohol	Entretenimiento
Tabaco	Correo electrónico basado en web
Lencería y traje de baño	juegos
Juegos de caza deportiva y guerra	Corretaje y Comercio
Consumo de ancho de banda	Publicidad
Descargas de software y software gratuito	Referencia
Uso compartido y almacenamiento de archivos	Religión global
Transmisión de medios y descarga	Compras
Intercambio de archivos de igual a igual	Sociedad y estilos de vida
Radio y televisión por Internet	Deportes
Telefonía por Internet	Viajar
Riesgo de seguridad	Vehículos personales
Páginas web maliciosas	Contenido dinámico
Suplantación de identidad	Chat web
URL de spam	Mensajería instantánea
DNS Dinámico	Grupos de noticias y tableros de mensajes
Dominio recién observado	Postales digitales
Dominio recién registrado	Educación Infantil
	Bienes raíces
	Restaurante y Comedor
	Blogs y sitios web personales
	Servidores de contenido
	Aparcamiento de dominio
	Privacidad personal
	Subasta

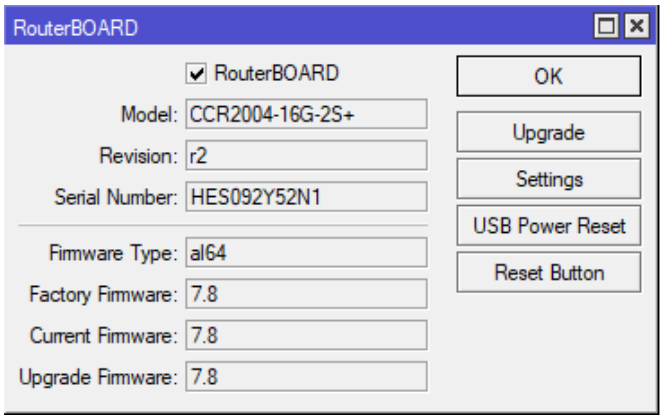
ANEXO 6. Interfaz gráfica de los equipos Mikrotik.



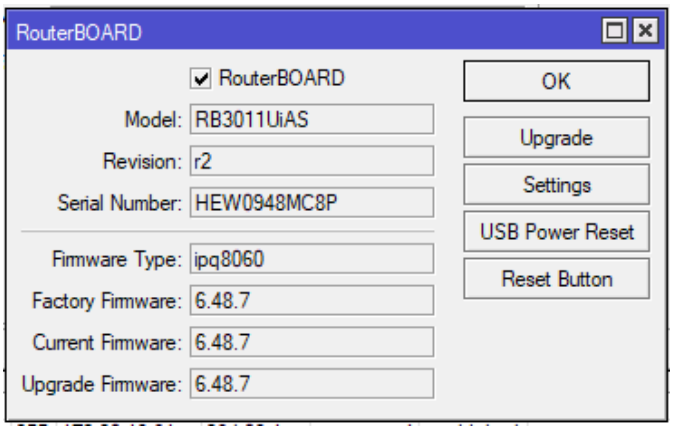
ANEXO 7. Interfaz gráfica del firewall Fortinet.



ANEXO 8. Versión de un equipo Mikrotik en la agencia principal.



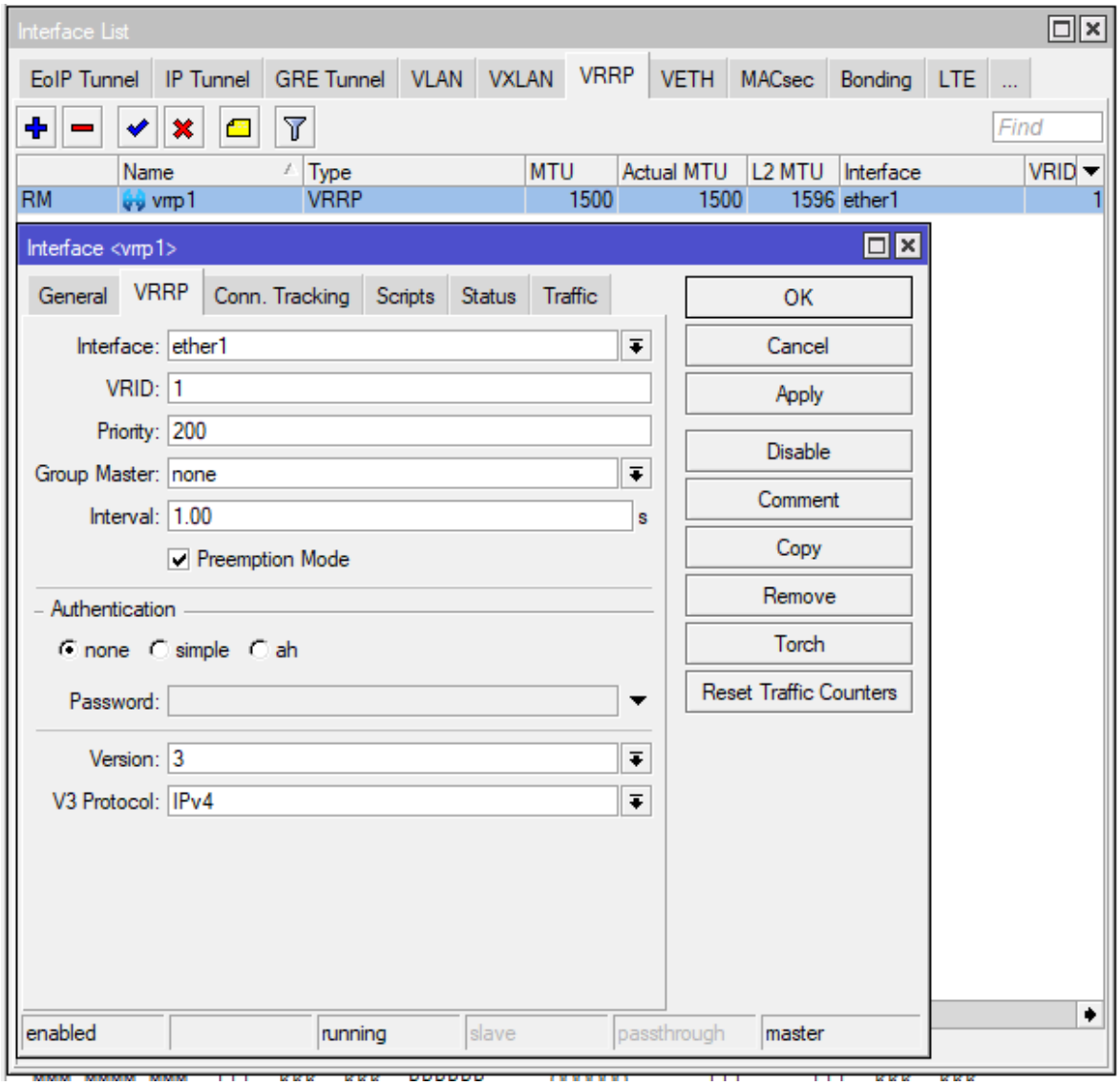
ANEXO 9. Versión de un equipo Mikrotik en la agencia remota.



ANEXO 10. Configuración VRRP (VRRP_1)

```
/interface vrrp
add interface=ether1 name=vrrp1 priority=200 vrid=1

/interface vrrp
add interface=ether1 name=vrrp1 vrid=1
```



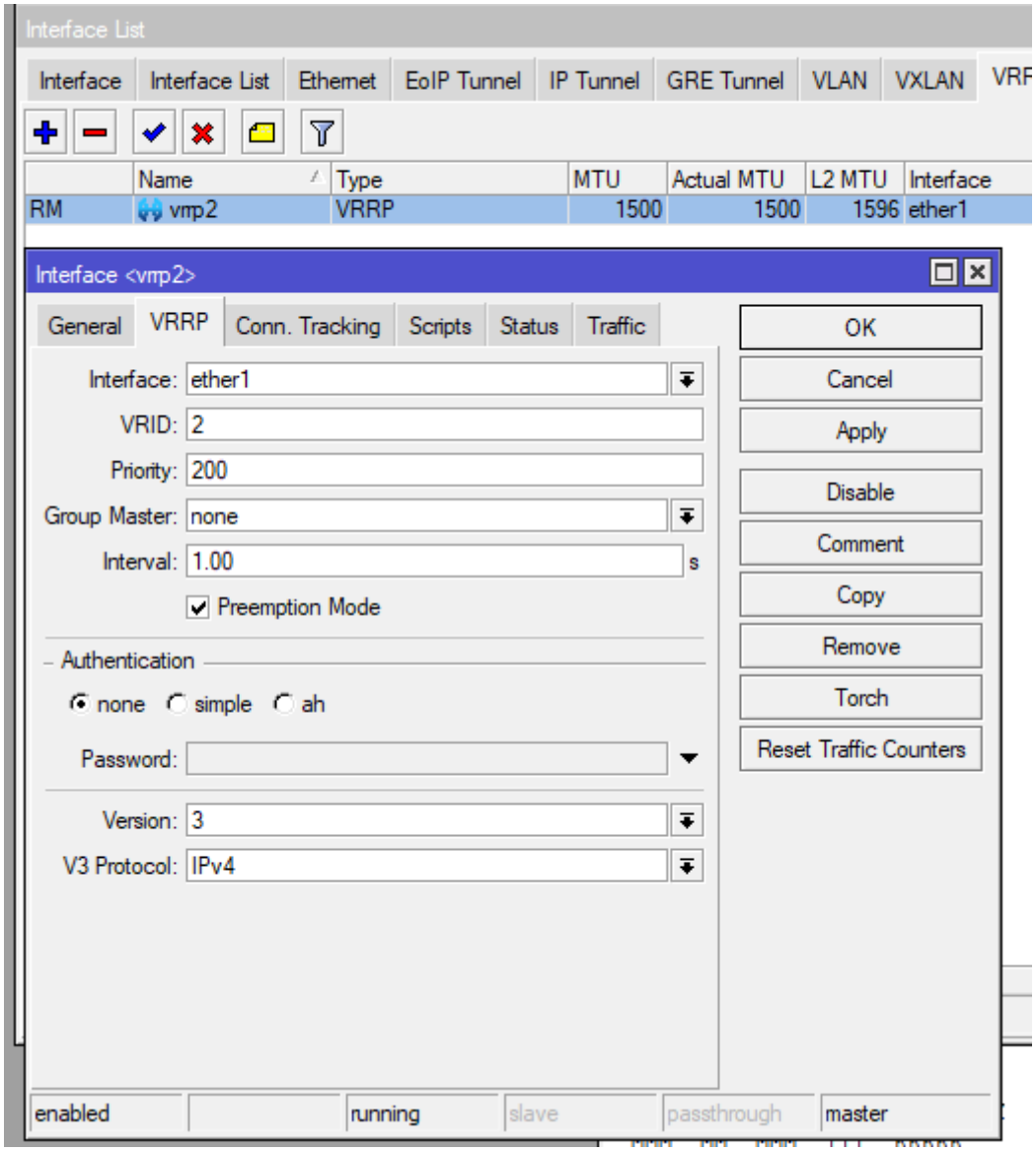
ANEXO 11. Configuración VRRP (VRRP_2)

Configuración VRRP enrutador Principal.

```
/interface vrrp
add interface=ether1 name=vrrp2 priority=200 vrid=2
```

Configuración VRRP enrutador redundante.

```
/interface vrrp
add interface=ether1 name=vrrp2 vrid=2
```



11% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 11% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.untels.edu.pe Internet	3%
2	tesis.pucp.edu.pe Internet	1%
3	fortinet.com Internet	<1%
4	cisco.com Internet	<1%
5	coursehero.com Internet	<1%
6	de.scribd.com Internet	<1%
7	repositorio.usanpedro.edu.pe Internet	<1%
8	parmenidesmc.wordpress.com Internet	<1%

9	mindomo.com Internet	<1%
10	pdfcoffee.com Internet	<1%
11	1library.co Internet	<1%
12	repositorio.ufsc.br Internet	<1%
13	whois.icann.org Internet	<1%
14	tesis.ipn.mx Internet	<1%
15	itdigitalsecurity.es Internet	<1%
16	Reyes, Gustavo. "The Effects of the Patient Self-Determination Act of 1... Publication	<1%
17	dspace.ups.edu.ec Internet	<1%
18	es.slideshare.net Internet	<1%
19	mindmeister.com Internet	<1%
20	cybertesis.unmsm.edu.pe Internet	<1%

21	fiberlux.pe Internet	<1%
22	repositorio.unicauca.edu.co:8080 Internet	<1%
23	docplayer.es Internet	<1%
24	hdl.handle.net Internet	<1%
25	repositorio.escuelamilitar.edu.pe Internet	<1%
26	repositorio.espe.edu.ec Internet	<1%