UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"OPTIMIZACIÓN DEL SERVICIO DE RED CON EL RESPALDO DEL ENLACE A INTERNET WAN Y LA SEGURIDAD PERIMETRAL PARA LA EMPRESA SONEPAR SEDE LIMA"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

CIRIACO SUSANIBAR, NICOLH ANTONY

ASESOR:

CASTRO PULCHA, BERNARDO ELÍAS

Villa el Salvador

2021

DEDICATORIA

Dedico este trabajo de suficiencia a mi madre Maximina quien constantemente me brinda su apoyo para poder llegar hasta estas instancias de mis objetivos, ya que ella siempre ha estado presente en todo momento.

A mi tío Pedro que siempre ha formado parte muy importante en mi vida pues me guía como un padre a base de valores para lograr mis metas.

AGRADECIMIENTO

Agradezco a Dios y a mi familia por brindarme en todo momento su apoyo incondicional.

A mis amigos y compañeros de labores que contribuyeron en mis conocimientos.

A mi casa de estudios superiores la UNTELS por prepararme en la etapa universitaria y darme la oportunidad de empezar como profesional y poder así continuar creciendo.

Al Ing. Bernardo Castro Pulcha por orientarme con su experiencia el cual es de suma importancia para el desarrollo del presente proyecto.

ÍNDICE

LISTADO DE FIGURAS:

LISTADO DE TABLAS

RESUMEN

El presente trabajo de suficiencia profesional se basa mediante la experiencia obtenida en la empresa de razón social Grupo Dalisa, el cual consiste principalmente en la optimización del servicio de seguridad para redes e internet de los clientes corporativos, por ello se pudo observar que las instituciones del rubro comercial necesitan un constante servicio de internet sobre todo para mantener las actividades virtuales como es el caso de la presente institución empresarial SONEPAR PERU SAC sede de Lima.

Esta empresa no contaba con un respaldo a internet constante y presentaba incertidumbre con respecto al servicio WAN. En adición a esto, se observó que la presente empresa no contaba con un eficiente sistema de protección LAN afectando a la seguridad de sus servidores y equipos informáticos.

Por ello como soluciones principales se optó primero por incorporar el equipo balanceador mediante otro proveedor ISP con un servicio de ancho de banda diferente como respaldo del único enlace que existía. Como segunda solución se añadió un equipo firewall de seguridad perimetral de mayor eficiencia para la protección de los servidores y navegación de los usuarios de la empresa. Todo esto a través de tres procesos principales: Diseño, Implementación y operatividad como se muestra en el punto 3.2 de modelo de solución propuesto.

Lo que logramos después de la implementación del servicio fueron resultados favorables para el cliente, como muestro en el punto 3.3 de resultados, con un internet dedicado estable se evitó perdidas en las ventas virtuales mediante el funcionamiento de la página de ventas del cliente SONEPAR y con los equipos internos como servidores, protegidos de amenazas y ataques externas se logra una mayor producción de las actividades. Así como también una ganancia para la empresa Grupo Dalisa por el servicio de ingeniería contratado.

INTRODUCCIÓN

De acuerdo a la ley peruana 04237/2018-CR que promueve la seguridad de la información a través del internet, se está convirtiendo en una necesidad y obligación en las instituciones de diversa índole para poder seguir brindando un mejor servicio y seguridad para sus usuarios o clientes, de acuerdo a sus actividades correspondientes.

Una de estas instituciones que necesitaba una optimización de sus servicios de internet y seguridad y así mantenerse al margen de la ley ya establecida, fue SONEPAR PERU, empresa transnacional de origen francés dedicado a la venta y distribución de materiales eléctricos, estableció contacto con la empresa Grupo Dalisa a través de América Móvil para el desarrollo del nuevo servicio requerido.

El propósito del estudio fue brindar soluciones integrados mediante la optimización de una conexión segura tanto para la RED WAN y LAN mediante dos equipos principales: un balanceador para el enlace principal y su respaldo, así como un firewall, dedicado a la seguridad perimetral respectivamente, ambos equipos de la marca FORTINET reconocida a nivel mundial, para que el servicio de internet se mantenga constante y seguro en la entidad comercial SONEPAR sede de Lima.

Esto permitió una mayor protección y estabilidad de conexión para las áreas que utilizan el medio virtual. Con el fin de aumentar la calidad del servicio a los usuarios de la institución y la administración del control administrativo que la componen, hemos desarrollado un diseño y estructuras lógicas de red que tienen en cuenta los equipos de seguridad, los conmutadores, el ancho de banda y cada equipo.

CAPÍTULO I. ASPECTOS GENERALES

1.1 Contexto

La empresa GRUPO DALISA SAC se dedica a la implementación y optimización en seguridad administrada de red, elaborados para alrededor de 300 clientes de los cuales 250 son corporativos, sin exoneración a otros sectores como comercio, educación o entretenimiento; lo realiza mediante instalaciones de equipos de seguridad para redes, facilitados por diferentes proveedores internacionales de excelente reputación y garantía en el rubro y a través del personal capacitado de la empresa, estos preconfiguran los equipos dedicados dependiendo de cada cliente de acuerdo a sus necesidades.

Mi labor fue participar desde el diseño hasta su implementación, operación y mantenimiento, específicamente realizando las validaciones de la optimización mediante el funcionamiento y conectividad de los equipos en conjunto con el técnico de implementación y finalmente llevándolo a producción y así lograr que la mejora del servicio se establezca, verificando la conectividad a internet después de haber culminado la instalación de los equipos y corroborar las diferentes funcionalidades de los servicios ofrecidos tales como políticas y filtros de seguridad para evitar cualquier inconveniente en las actividades, incluyendo actualizaciones de los equipos como mantenimiento cada cierto periodo.

1.2 Delimitación temporal y espacial del trabajo

1.2.1 Temporal

El periodo en el que se optimizo el proyecto fue de setiembre a octubre del 2019 a dedicación exclusiva; desde el diseño de red e implementación considerando la topología, software y hardware respectivamente. Continuándose con su operación y mantenimiento hasta la culminación del contrato en diciembre del 2022.

1.2.2 Espacial

El proyecto se optimizo para la empresa comercial SONEPAR con dirección Av. República de Panamá 3517, sede principal ubicado en el distrito de San Isidro, Lima-Perú.

1.3 Objetivos

1.3.1 Objetivo General:

Optimizar el servicio de red mediante el respaldo del enlace a internet Wan y la seguridad perimetral para la empresa SONEPAR sede de Lima.

1.3.2 Objetivos Específicos:

- Brindar seguridad para la red de la comercializadora SONEPAR mediante los filtros del equipo perimetral firewall.

- Implementar la conectividad a internet con un enlace de respaldo que garantice la disponibilidad del servicio mediante el equipo de respaldo Fortiwan.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

Para desarrollar mi proyecto de suficiencia profesional he considerado conclusiones importantes relacionadas a mi trabajo de los siguientes temas en seguridad perimetral y respaldo de internet aplicados en el Perú y el exterior.

2.1.1 Antecedentes Internacionales

Benavides, E. y Olaya, D. (2018), en su trabajo de postgrado titulado: “Diseño de un plan de contingencia para un enlace crítico del banco financorp**”** Universidad Piloto De Colombia, Bogotá., es un proyecto de respaldo para enlaces de internet del banco Colombiano, tanto para el principal como el secundario utilizando un mecanismo virtual configurado llamado HSRP, el cual consta de que los enrutadores ejecuten el protocolo mencionado y trabajen en equipo como un solo enrutador virtual y así llegar al flujo del cien por ciento de servicio de internet para el banco. El cual aporta a nuestro trabajo de suficiencia con la demostración que se logra para un respaldo de internet orientado a una sede corporativa.

Pilacuán, E. (2015), en su trabajo de tesis titulado: “Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cia. Ltda. Con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001” Universidad De Las Fuerzas Armadas en Ecuador, Sangolquí., en los sectores en los que la seguridad de la información debe mantener constantemente los principios de disponibilidad, confidencialidad e integridad, la norma ISO 27001 se está utilizando para elaborar políticas de seguridad de la información basadas en la norma. Una de las conclusiones del presente proyecto que aporta a mi trabajo de suficiencia es la implementación de políticas de seguridad perimetral para empresas medianas y pequeñas mediante un firewall de software libre llamado ClearOS.

2.1.2 Antecedentes Nacionales:

Ramos, J. (2017), en su trabajo de suficiencia profesional titulado: "Implementación del protocolo getvpn para optimizar el proceso de seguridad mediante la encriptación de tráfico en una entidad financiera" UNTELS, Lima., tiene por finalidad proporcionar una solución para el despliegue del protocolo IPSec debido a la dificultad de hacer un túnel para la ubicación de cada empresa, por lo que para resolver dicha problemática se implementó el protocolo GETVPN. El aporte a mi trabajo es permitirme tener una visión del funcionamiento de una VPN ya que es un parámetro fundamental para la seguridad perimetral.

Lizana, J. (2016), en su trabajo de suficiencia profesional titulado: "Diseño de una red de datos para sede principal y remotas del sat con seguridad perimetral y bandwidth manager con alta disponibilidad en su sede principal" UNTELS, Lima., muestra cómo construir una solución integrada basada en la alta disponibilidad, la gestión del ancho de banda y la conexión con ubicaciones distantes en la sede del SAT (Sistema de Administración Tributaria), al tiempo que permite la comunicación con las oficinas centrales del sistema. Una de las conclusiones que aporta a mi trabajo es con respecto al manejo de los equipos empleados para la seguridad perimetral tanto para la red LAN y WAN según la necesidad de la empresa corporativa.

Guevara, R. y López, W. (2016), en su trabajo de tesis titulado: "Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática" USP, Chiclayo, desarrolla una alternativa de sistema para mejorar la seguridad perimetral, este sistema hace uso de complejos algoritmos para el cifrado y descifrado de los paquetes de información que se transfieren dentro de la entidad de estudio con el fin de garantizar la privacidad de la información personal de los usuarios. Por lo que la conclusión principal aporta a mi trabajo sobre la mejora de la seguridad de la red identificando los puntos vulnerables a mejorar en la topología.

Valenzuela, J. (2012), en su trabajo de tesis titulado: “Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña” PUCP, Lima., la solución que se presenta aquí es una solución de seguridad perimetral que se adapta a las necesidades de la red informática de una pequeña empresa. También se muestra una simulación del concepto sugerido en un entorno de prueba controlado. Este trabajo tiene como conclusión dar las politicas y configuraciones de seguridad perimetral como aporte a mi trabajo de suficiencia.

Ramírez, A. (2011), en su trabajo 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” Universidad Nacional de Ingeniería, Lima., nos desarrolla una optimización en el uso de internet para un campus universitario mediante un diseño de solución segura y administrativa en la red WAN, como objetivo la satisfacción de las necesidades para con los clientes tanto en la calidad de velocidad del internet por ancho de banda y protección del servicio de la información. Aporte que brinda a mi trabajo, una perspectiva para beneficiar a los usuarios con un internet constante y de calidad obtenido mediante el respaldo.

2.2 Bases Teóricas

2.2.1 Seguridad de Red:

“La seguridad de red se refiere a las tecnologías, procesos y políticas utilizadas para defender cualquier red, tráfico de red y activos accesibles por red frente a ciberataques, acceso no autorizado y pérdida de datos.

La seguridad de red debe proteger en los diversos límites de la red y también dentro de la red, con un enfoque de capas. Las vulnerabilidades existen en todos lados, desde dispositivos y rutas de datos a aplicaciones y usuarios. Debido a que las organizaciones encuentran tantas posibles amenazas, también hay cientos de herramientas de administración de seguridad de red que tienen como objetivo abordar las amenazas individuales o aprovechar o ayudar con otras necesidades de infraestructura de misión crítica, como un cumplimiento continuo”. (Fortinet, 2021).

De acuerdo a la figura 1, se muestra una topología clásica de la seguridad de red.

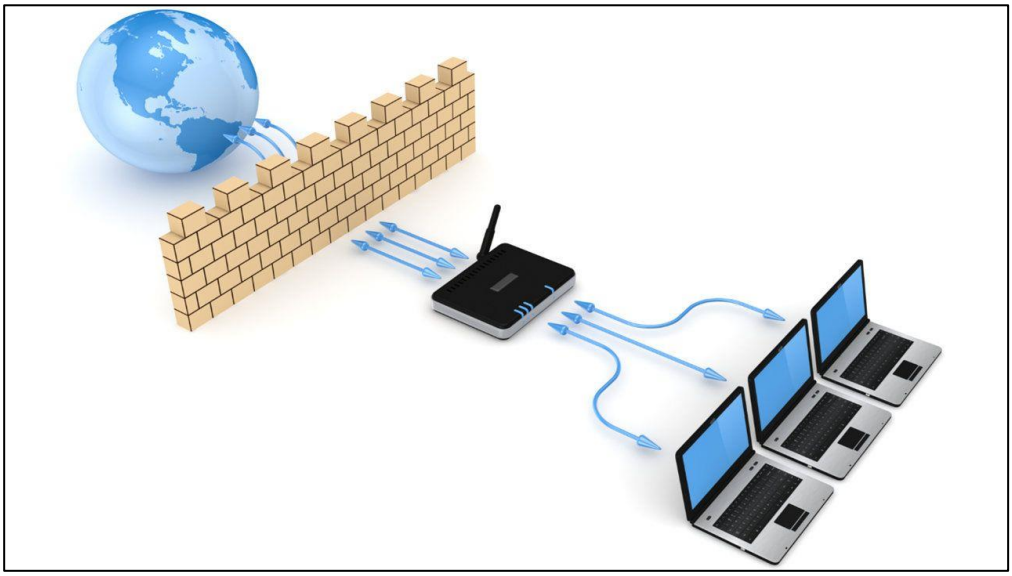


Figura 1: Representación básica de una seguridad de red.

Fuente: https://www.muycomputer.com/2015/05/29/herramientas-hacking-redes/

2.2.1.1 Beneficios de la seguridad de red

Son varias las ventajas que una empresa puede obtener al aplicar la gestión de la seguridad de la red. (ISO Tools, 2021):

- La disponibilidad de una red mucho más estable, así como un menor número de interrupciones en el negocio, se traducirá en un aumento de la productividad.
- La seguridad de la red es un tema frecuente en muchas normativas, por lo que es importante mantener también el cumplimiento de las mismas.
- Reducción del peligro de acciones legales como resultado de las medidas de la empresa para asegurar los datos de los clientes, que demuestran la debida atención y cuidado de la empresa.
- Mejora de la reputación de la empresa como resultado de los esfuerzos realizados para asegurar los datos de los clientes, que demuestran la dedicación de la empresa a mantener estrictos controles de seguridad.

2.2.1.2 Normativa estándar de la seguridad de red: ISO/IEC 27033

“Norma dedicada a la seguridad en redes, consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante Gateway, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes”. (ISO, 2005).

Objetivos de la normativa:

- Proporciona orientación sobre cómo identificar e investigar los problemas de seguridad de la red, así como la idea de las necesidades de seguridad de la red con respecto a ese análisis, de cara al futuro.
- Ofrece un panorama completo de los controles que ayudan a implementar los diseños técnicos de la red, la seguridad, los controles técnicos relacionados y los controles no técnicos.
- Dentro de este documento se ofrecen directrices para lograr arquitecturas tecnológicas y riesgos de seguridad de red de alta calidad, factores de

controles relacionados con los escenarios de red, diseño y escenarios de red típicos en las secciones de "tecnología".

- En un enfoque muy básico, este documento describe las dificultades relacionadas con las medidas de seguridad de las operaciones de red, incluida la instalación de dichos controles, así como la supervisión y evaluación de su eficacia.

2.2.2 Seguridad Perimetral:

“Son herramientas y técnicas de protección informática que tienen como propósito establecer una línea de defensa relacionada con la red interna y toda la prolongación que forma parte del entorno bajo el que se encuentra la tecnología de la información de una empresa.

La seguridad perimetral establece medidas de protección que prevengan de ataques externos a la vez que identifica la actividad natural y esperada dentro de la propia red y filtra, protege y aísla actividad desconocida o fraudulenta”. (Avansis, 2021).

Según la figura 2, se observa la topología más común para la seguridad perimetral.

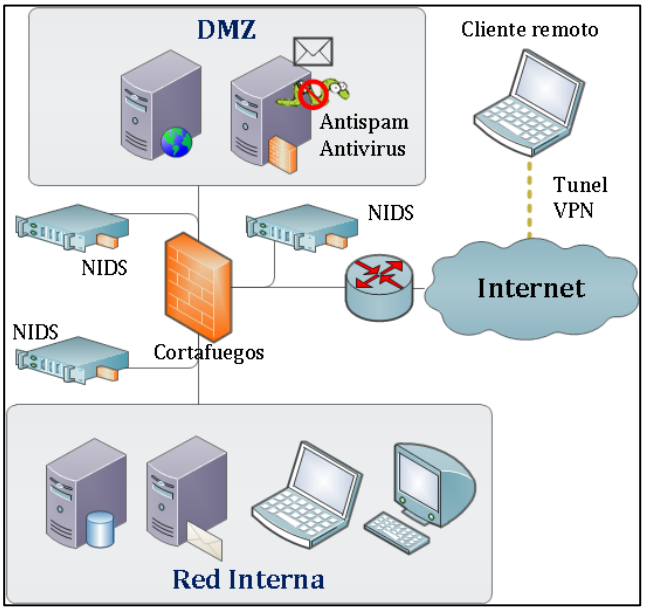


Figura 2: Representación de una seguridad perimetral corporativa.

Fuente: https://www.avansis.es/ciberseguridad/que-es-seguridad-perimetral/?cn-reloaded=1

2.2.2.1 Elementos de la seguridad perimetral

2.2.2.1.1 Router Frontera

El router frontera es el enrutador que se instala en la parte más externa de la red corporativa, se encarga de comprobaciones de seguridad en el tráfico de salida y entrada de la red, una especie de policía de tráfico entrante y saliente. Estos equipos están diseñados para soportar muchas conexiones en las grandes organizaciones u operadores, en una instalación doméstica este papel lo hace un router convencional, que es el que se encarga de proporcionar también acceso a Internet. De acuerdo a la figura 3, los protocolos con los que trabajan los enrutadores frontera son los EGP (Exterior Gateway Protocol), siendo el más extendido el BGP (Border Gateway Protocol).

Estos protocolos son necesarios para poder encaminar la información en Internet. (Birt, 2020)

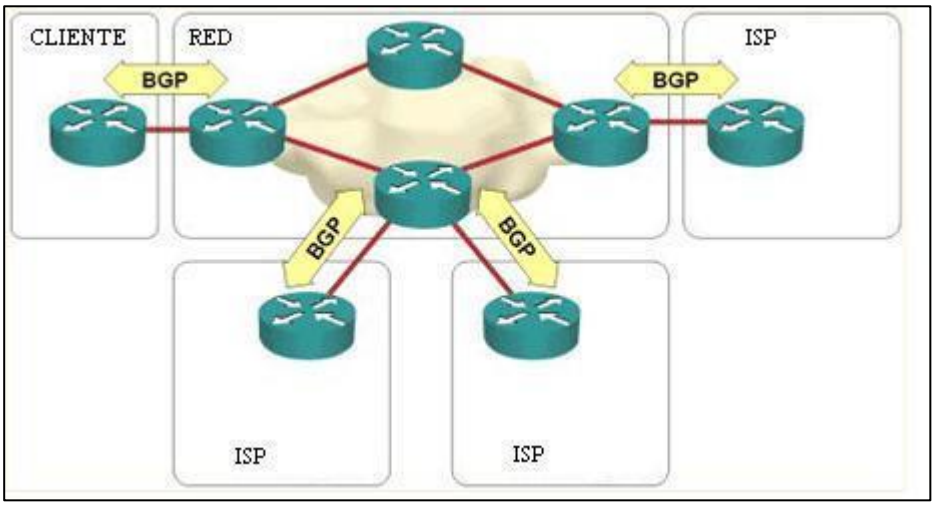


Figura 3: Representación del protocolo BGP para el entramado de internet.

Fuente: https://ikastaroak.birt.eus/edu/argitalpen/backupa/

2.2.2.1.2 Redes Privadas Virtuales – VPN

“Una Red Privada Virtual (VPN) es una tecnología que permite establecer una conexión similar a la de una red LAN sobre una red pública como Internet. Para conseguir esto utiliza mecanismos de encapsulación o tunelización y a veces encriptación”. (Fortinet, 2020).

De acuerdo a la figura 4, se muestra un diseño convencional de la red privada virtual para la seguridad perimetral.

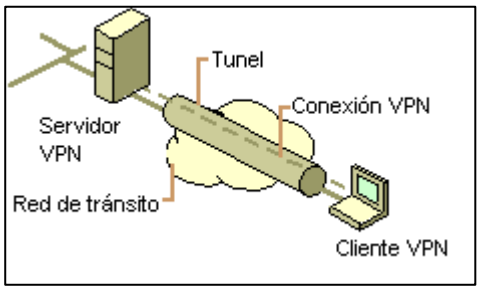


Figura 4: Representación clásica de una VPN.

Fuente: https://ikastaroak.birt.eus/edu/argitalpen/backupa/

2.2.2.1.3 Zona Desmilitarizada

La zona desmilitarizada de una red, también denominada DMZ**,** es una zona de seguridad en la que los equipos tienen una relación de comunicación bidireccional con la red WAN pero no con la red LAN. Es decir, un equipo situado en la WAN podrá conectarse con un equipo de la zona DMZ y viceversa, pero un equipo de la zona DMZ no podrá conectarse hacia un equipo de la red LAN.

Las zonas DMZ se emplean para situar los dispositivos que proporcionan servicios públicos como alojamientos de páginas Web (servidores Web), servidores de correo o servidores DNS. En la zona DMZ se dejan los equipos que se quiere tener expuestos a la red. (Birt, 2020).

Según la figura 5, se observa el diseño para una zona desmilitarizada y su ubicación dentro la seguridad perimetral.

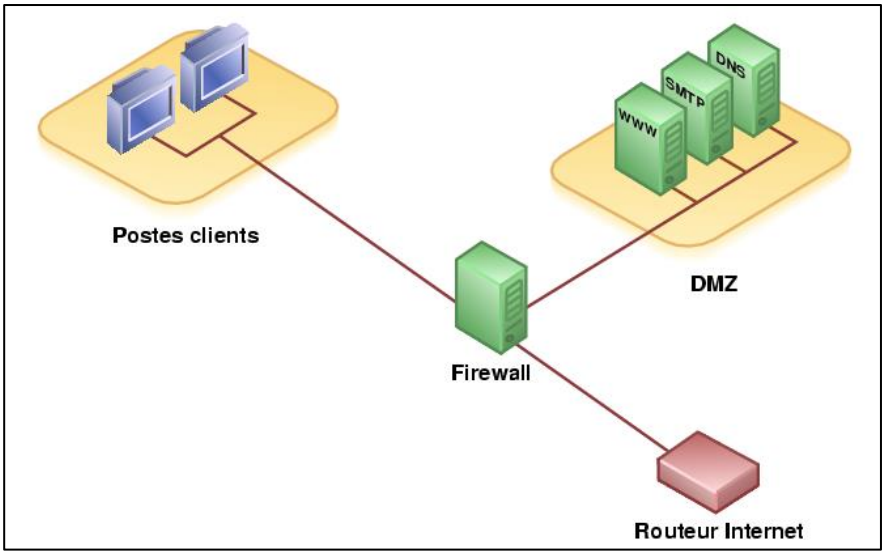


Figura 5: Representación de una DMZ.

Fuente: https://ikastaroak.birt.eus/edu/argitalpen/backupa

2.2.2.2 Firewall

En el ámbito de la ciberseguridad, un cortafuegos es una especie de instrumento que se utiliza para filtrar el tráfico en una red. Los cortafuegos, como se conocen en inglés, son dispositivos que pueden utilizarse para aislar los nodos de la red de las fuentes de tráfico externas, de las fuentes de tráfico internas o incluso de determinadas aplicaciones. Los tipos de cortafuegos disponibles incluyen los basados en software, los basados en hardware y los basados en la nube, y cada tipo ofrece distintas ventajas e inconvenientes.

La función principal de un cortafuegos es impedir que pasen las solicitudes de tráfico y los paquetes de datos maliciosos, permitiendo al mismo tiempo que pase el tráfico genuino.

“Los firewalls protegen una red de ordenadores contra el compromiso, la denegación de servicio y otros ataques de piratas informáticos que intentan entrometerse en la red desde el exterior. Un firewall debe estar conectado a un mínimo de dos interfaces de red, una que se supone que está protegida (su red interna) y otra que está expuesta a ataques (generalmente Internet). Un firewall también puede considerarse como una puerta de enlace implementada entre las dos redes”. (Protecciondatos-lopd, 2021)

Metodologías que aplican los firewalls:

- ✓ **Filtrado de paquetes**

"Es en un enrutamiento básico capaz de actuar sobre las unidades de datos de protocolo de nivel de red tcp/ip. Examina las cabeceras de cada paquete que circula a través del cortafuegos en cada dirección, filtrando los paquetes en función de las direcciones ip origen o destino y de los números de puertos". (Areitio, 2008, p.332)

- ✓ **Servicio de proxy**

"Es la puerta de enlace de la aplicación ya que controla el tráfico a nivel de la aplicación. A pesar de examinar los paquetes sin procesar, filtra los datos sobre la base de los campos de encabezado, el tamaño del mensaje y el contenido también. El servicio proxy es parte del firewall, el firewall de paquetes por sí solo no sería factible porque no puede diferenciar entre números de puerto". (Living, 2021)

- ✓ **Inspección con estado**

"Es el método más moderno de escaneo de firewall, La inspección de estado, o filtrado dinámico de paquetes, es una tecnología de firewall que controla todas las conexiones activas y usa esta información para decidir que paquetes autoriza a seguir su camino. la inspección de estado analiza los paquetes a nivel de aplicación. Al registrar información como la dirección IP y los puertos afectados, la filtración de paquetes dinámica puede implementar una postura mucho más segura que una simple herramienta de filtrado estático". (Techtarget, 2021)

Tipos de firewall

Hay varios tipos distintos de firewall que pueden clasificarse en función de su estructura general y su modo de funcionamiento, y a continuación se analizan las características de cada tipo.

Según método de operación:

- **Firewall de filtrado de paquetes**

“Es el tipo de arquitectura de firewall más básico y más antiguo, los firewalls de filtrado de paquetes básicamente crean un punto de control en un enrutador o conmutador de tráfico. El firewall realiza una simple verificación de los paquetes de datos que ingresan a través del enrutador, inspeccionando información como el destino y la dirección IP de origen, el tipo de paquete, el número de puerto y otra información a nivel de superficie sin abrir el paquete para inspeccionar su contenido”. (Protecciondatos-lopd,2021)

Como muestra la figura 6, se descarta si el paquete de información no pasa la inspección.

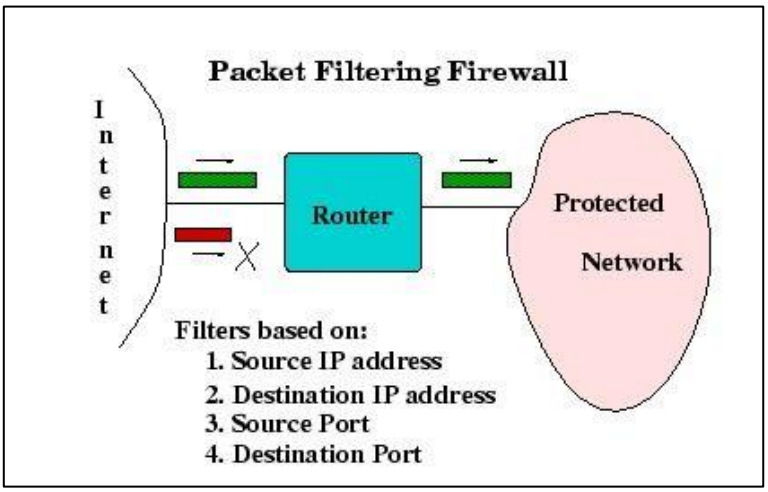


Figura 6: Esquema de un filtrado de paquetes

Fuente: https://www.cloudcenterandalucia.es

“En un cortafuegos de filtrado de paquetes los accesos desde la red interna al exterior que no están bloqueados son directos, por lo que esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad.

El principal problema es que no disponen de un sistema de monitorización sofisticado, por lo que muchas veces el administrador no puede determinar si el router está siendo atacado o si su seguridad ha sido comprometida". (Ibiblio, s.f.)

- **Firewall de inspección con estado**

"Los firewalls de inspección de paquetes con estado funcionan según el mismo principio general de filtrado de paquetes, pero pueden realizar un seguimiento al tráfico a nivel granular." (Vega, 2021, p.84)

Según nos muestra la figura 7, el tráfico que pasa a través de un cortafuegos de estado suele estar especificado por las direcciones IP de origen y destino, los puertos que se utilizan y la cantidad de tráfico de red existente.

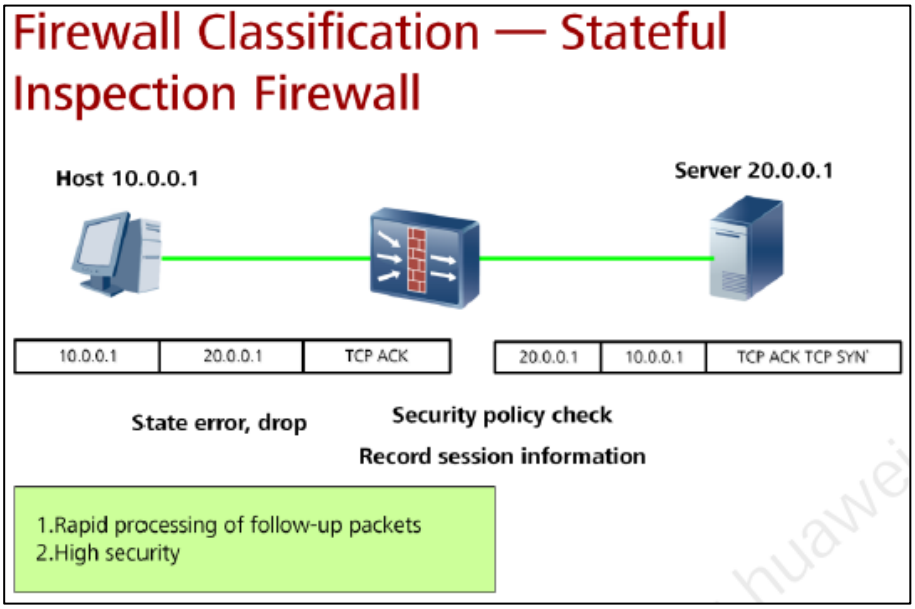


Figura 7: Diagrama básico de una inspección de estado en un firewall

Fuente: https://forum.huawei.com/enterprise/es/que-son-los-firewall-por-inspeccion-de-estado

- **Firewall Proxy**

“Estos firewalls son similares al firewall de inspección con estado en que analiza tanto el paquete como el protocolo de enlace TCP. Sin embargo, los firewalls proxy también pueden realizar inspecciones de paquetes de capa profunda, verificando el contenido real del paquete de información para verificar que no contiene malware”. (protecciondatos-lopd, 2021)

El firewall proxy no permite que el tráfico se conecte directamente a la red, sino que crea una conexión con el origen del tráfico e inspecciona los paquetes de datos entrantes. Según la figura 8:

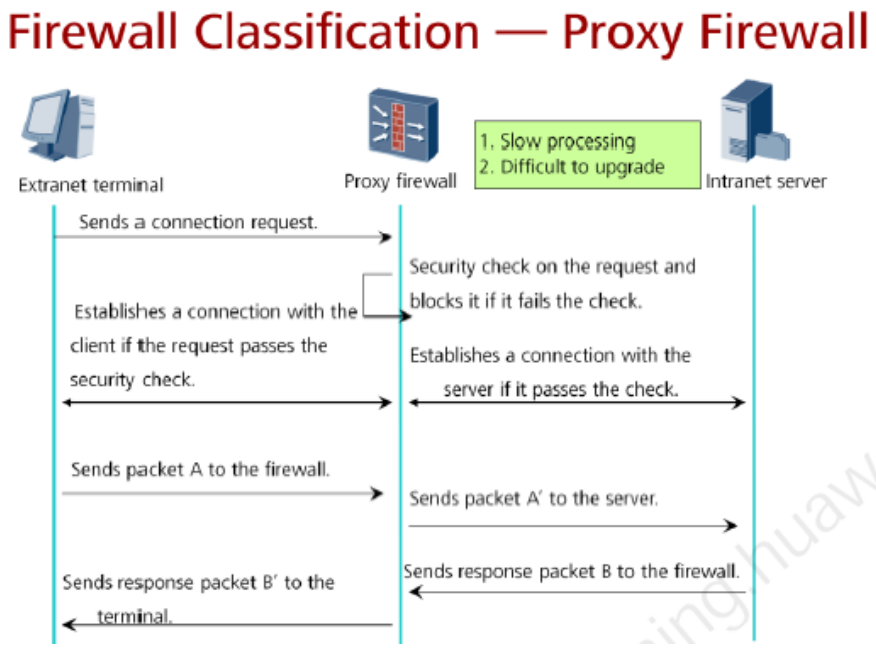


Figura 8: Esquema de un firewall proxy

Fuente: https://forum.huawei.com/enterprise/es/

Sin embargo, la desventaja de este tipo de protección es que a veces puede interferir con datos entrantes no amenazantes, reduciendo el funcionamiento del sistema. (Kaspersky, 2021)

Según estructura:

- **Cortafuegos de Software**

Un firewall de software, como su nombre indica, es una solución basada en software que puede desplegarse como un dispositivo virtual o en máquinas individuales de su red para protegerlas de las vulnerabilidades. Tiene la capacidad de controlar el comportamiento asociado a ciertas aplicaciones. (geekflare,2021)

Esto permite que las personas introduzcan datos en un software mientras se evita que los datos se introduzcan en otro. Los cortafuegos de software también pueden filtrar los datos que se reciben, así como responder a las solicitudes que se realizan de forma remota. El inconveniente más importante de los cortafuegos de software corporativos es que deben instalarse, actualizarse y administrarse en cada ordenador de la organización. (islabit, 2021)

De acuerdo a la figura 9, se muestra un diagrama aplicado para un firewall de software.

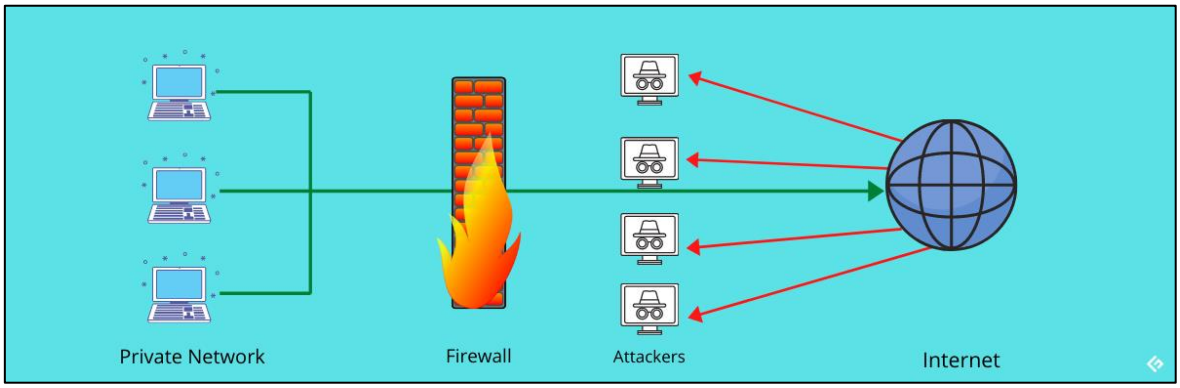


Figura 9: Diagrama de un firewall de software.

Fuente: https://geekflare.com/es/hardware-vs-software-cloud-firewall/

- **Cortafuegos de Hardware**

“Los cortafuegos por hardware o firewalls de red, son dispositivos electrónicos externos que se colocan entre la computadora o red y el modem que da acceso a Internet, y su objetivo es controlar las comunicaciones y conexiones con el exterior, tanto entrantes como salientes. Los firewalls por hardware proporcionan una línea de defensa adicional contra ataques procedentes del exterior, por ser dispositivos separados con su propio sistema operativo”. (guiaspracticas,2021)

Según muestra la figura 10, la configuración se realiza mediante una interfaz web, a la que se accede a través del mismo navegador que el usuario utiliza al conectarse a Internet. Este tipo de dispositivo ya se coloca en los routers de acceso a Internet, garantizando la seguridad de los ordenadores que se conectan a ellos.

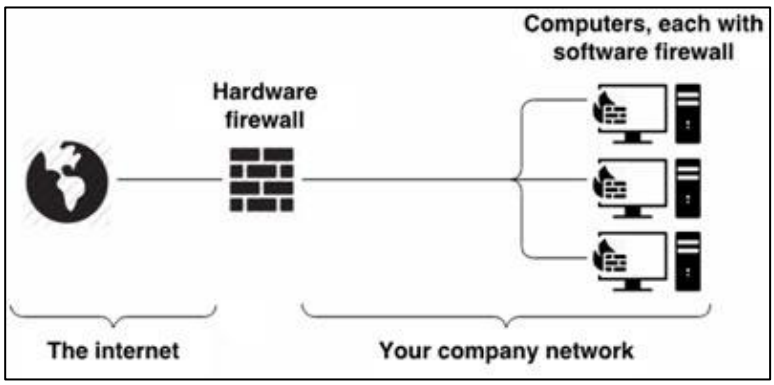


Figura 10: Diagrama de un firewall de hardware

Fuente: https://airoserver.com/blog/everything-about-firewall/

- **Cortafuegos en la nube**

Los firewalls de nube pública son dispositivos virtuales de seguridad de red implementados en la nube pública. Como regla general, los firewalls de nube pública suelen ofrecen capacidades similares a las de los firewalls de hardware. Sin embargo, en implementaciones de nube híbrida, los firewalls de nube pública ofrecen ventajas significativas en comparación con los dispositivos locales en cuanto a escalabilidad, disponibilidad y extensibilidad. A veces llamados “firewalls virtuales”, estos dispositivos se conocen como “firewalls de nube pública” cuando se usan en esos entornos. (paloaltonetworks, 2020).

Formados como una barrera virtual que rodea las plataformas en la nube, la infraestructura y los servicios de aplicaciones, los firewalls basados en la nube son cada vez más populares. Funcionan de la misma manera que los cortafuegos convencionales, ya que crean una barrera alrededor de la red interna de una organización. Los firewalls en la nube también pueden utilizarse para proteger la infraestructura y los datos locales. (cloudflare, 2021)

De acuerdo a la figura 11, se observa un esquema que refleja a un firewall cloud.

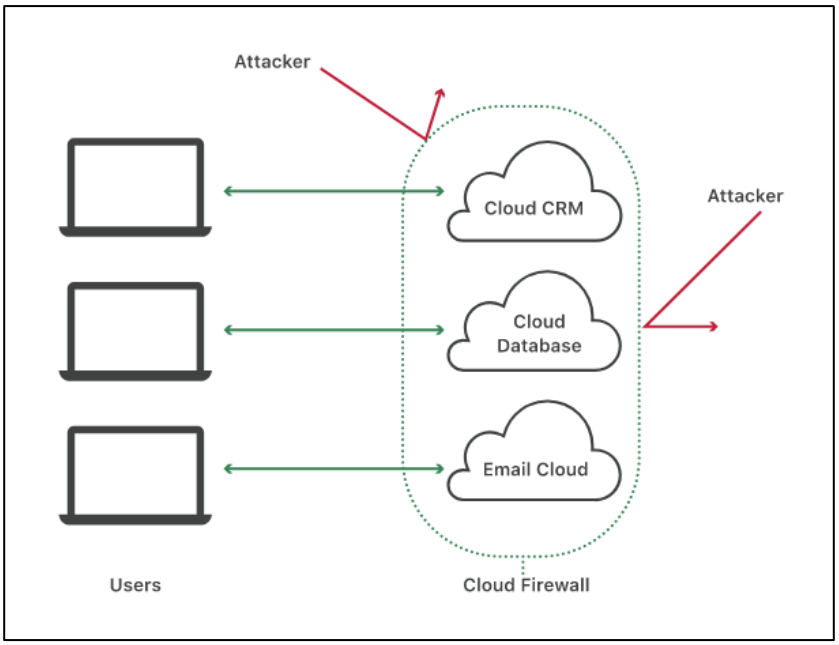


Figura 11: Representación de un firewall en la nube

Fuente: https://www.cloudflare.com/es-es/learning/cloud/what-is-a-cloud-firewall/

- **Cortafuegos de Próxima Generación (NGFW)**

“Son una versión más avanzada de los firewalls tradicionales ya mencionados. Al igual que los cortafuegos normales, el NGFW utiliza filtros de paquetes estáticos y dinámicos y soporte de VPN para asegurar que todas las conexiones entre la red, Internet y el firewall sean válidas y seguras. Ambos tipos traducen las direcciones de red y de puerto para mapear las IPs. La diferencia fundamental entre el

cortafuegos tradicional y los cortafuegos de próxima generación es la capacidad de para filtrar aplicaciones. Estos tienen un amplio control y visibilidad de las aplicaciones que se pueden identificar analizando y cotejando las firmas. Pueden utilizar listas blancas o un IPS basado en firmas para distinguir entre aplicaciones seguras y no deseadas, que luego se identifican mediante el descifrado de SSL. A diferencia de la mayoría de los cortafuegos tradicionales, el NGFW también incluye una ruta a través de la cual se recibirán las futuras actualizaciones.

Estos equipos bloquean contenido malicioso para que no entre en la red de la empresa, algo que los firewalls tradicionales nunca pudieron conseguir. Están mejor equipados para hacer frente a las amenazas persistentes avanzadas (APT). NGFW puede ser una opción de bajo costo para las empresas que buscan mejorar su seguridad básica, ya que pueden incorporar el trabajo de los antivirus y otras aplicaciones de seguridad en una sola solución. Las principales características de NGFW incluyen el conocimiento de las aplicaciones, servicios de inspección y un sistema de protección en toda la red. Como se muestra en la figura 12, el firewall de próxima generación suma la mayoría de ventajas de los anteriores firewalls en uno solo". (redfibra,2020)

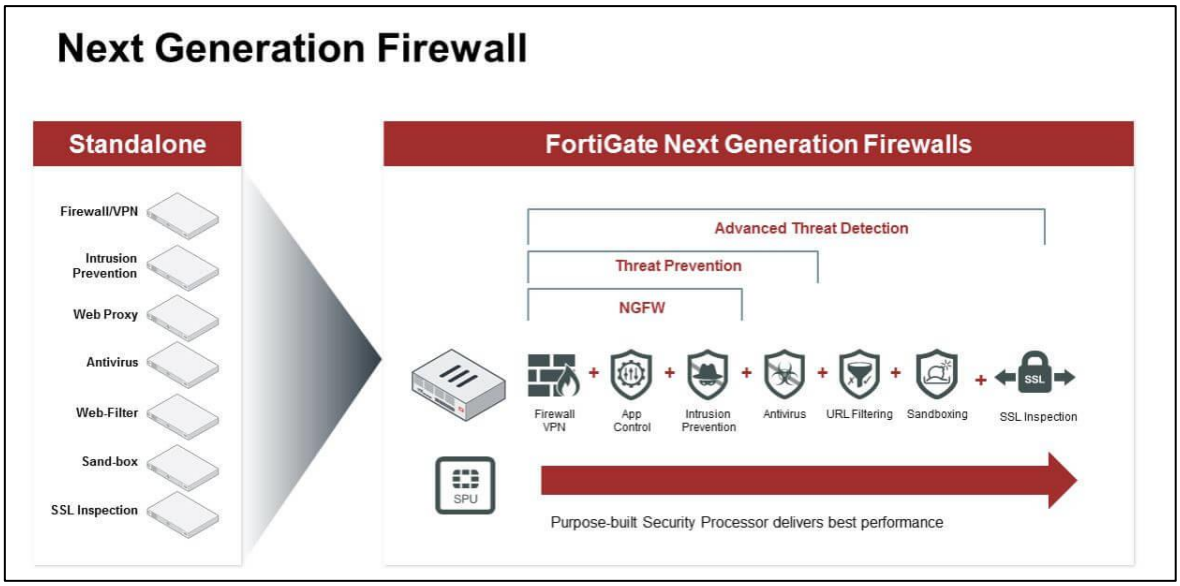


Figura 12: Funciones que integra un firewall de próxima generación.

Fuente: https://www.adaptixnetworks.com/firewalls-nueva-generacion/

2.2.3 Respaldo de Internet

Podemos definir respaldo para términos de redes e informática como el apoyo de una copia o backup para situaciones de caída de internet o datos. También se conoce como contingencia.

Los niveles de servicio en Internet se mantienen gracias a la colaboración de los numerosos proveedores de servicios de Internet, que trabajan juntos para mantener en funcionamiento sus propias redes y las interconexiones entre ellas, por lo que al unir estos servicios de los proveedores se logra el respaldo deseado para asegurar el flujo continuo para el acceso a internet. (Iplan, s.f, pág. 2)

"Es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea al mínimo. como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total." (Verdú, 2015).

De acuerdo a la figura 13, se muestra un diagrama de respaldo a internet usando dos enrutadores ISP y el equipo de seguridad firewall.

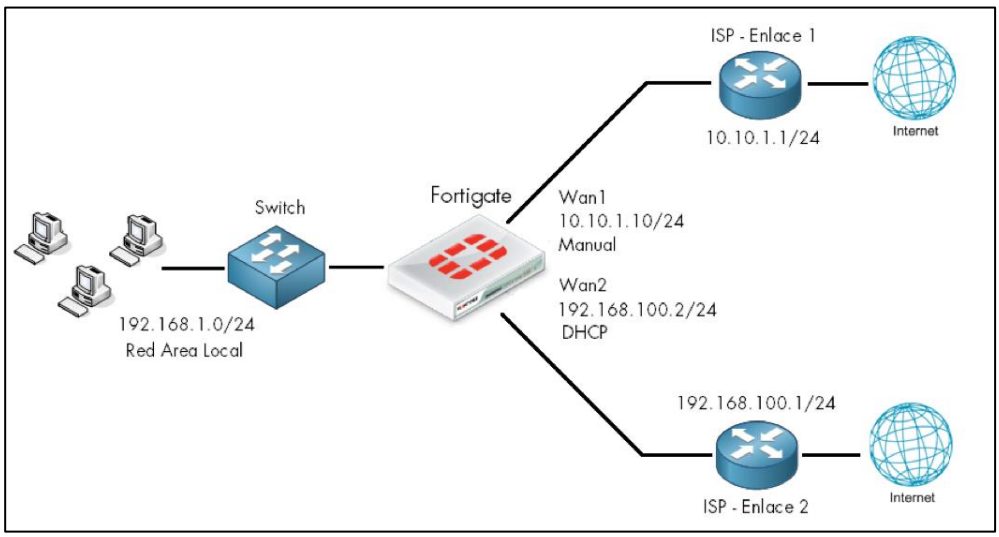


Figura 13: Representación de un respaldo de internet con un equipo fortigate.

Fuente: https://cerounosoftware.com.mx

2.2.3.1 Tipos de enlaces para respaldo a internet

2.2.3.1.1 Analógica (Dial Up)

“Es la conexión más antigua, lenta pero económica. Funciona con un Módem que se conecta a una línea telefónica. Con el número de teléfono la PC recibe el proveedor por medio del cual se conecta a Internet. Las señales recibidas por el ordenador se convierten en señales digitales, y luego se transforman en señales analógicas las señales digitales que el ordenador quiere que se transmitan por la red”. (Iptel, 2015)

Según la figura 14, se observa un esquema de conexión dialup tradicional.

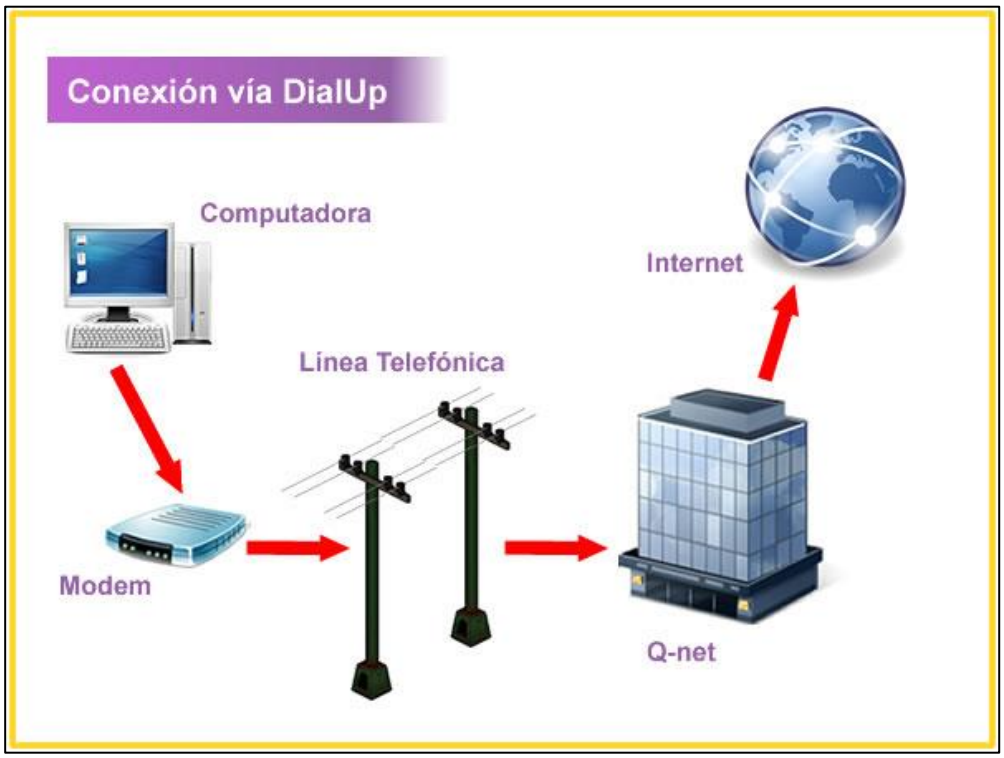


Figura 14: Esquema de una conexión DialUp

Fuente: http://tuconexionainternet.blogspot.com/2015/08/dial-up.html

2.2.3.1.2 RDSI

“Llamada red digital de servicios integrados traducidas de las siglas en inglés ISDN (Integrated services digital network), es una trasmisión de datos por voz enteramente digital de punta a punta. Este servicio de transmisión digital ofrece canales independientes de 64kbps, que permiten hablar y conectarse a internet simultáneamente, o con el hardware adecuado aprovechar los dos canales juntos para navegar a 128 kbps. Esta nueva tecnología para la época permitía ofrecer a los usuarios en su casa la transmisión de datos además de la tradicional comunicación por voz” (Íñigo y Barceló, 2008, p.29)

De acuerdo a la figura 15, se muestra el diseño clásico de una conexión RDSI.

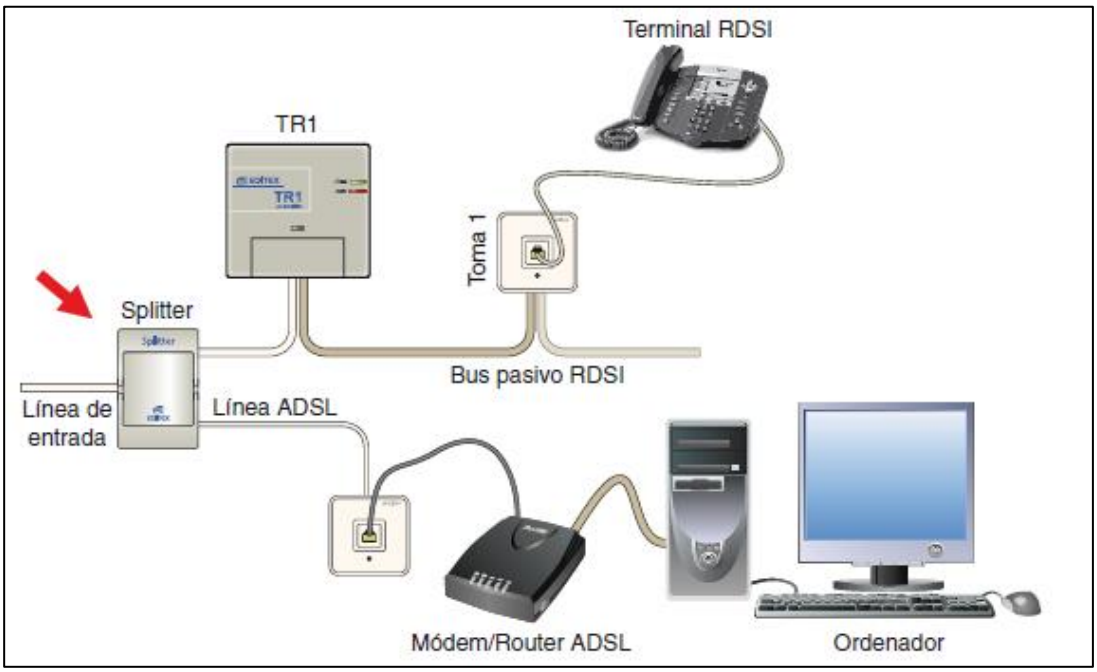


Figura 15: Representación de una conexión RDSI

Fuente: https://inevid.blogspot.com/2014/09/internet-en-una-linea-rdsi.html

2.2.3.1.3 ADSL

“Es una línea de abonado digital asimétrica que permite la transmisión de datos a mayor velocidad en un sentido que en el otro. Cuando estamos conectados a internet el flujo de datos es asimétrico, la mayor parte de los datos viajan en sentido internet a usuario, mientras que unos pocos datos viajan en sentido usuario a internet. Es decir, cuando hacemos una petición en un navegador de internet enviamos pocos datos, la dirección de la página y poco más, mientras que al recibir esa página recibimos muchos datos, imágenes, texto, etc. Bajo el nombre de ADSL se definen unas tecnologías que permiten el uso de una línea de cobre para la transmisión de datos de alta velocidad y a la vez para el uso normal como línea telefónica.”. (González, 2015, p.25)

Según la figura 16, se muestra la conexión por adsl que hasta hoy en día se utiliza.

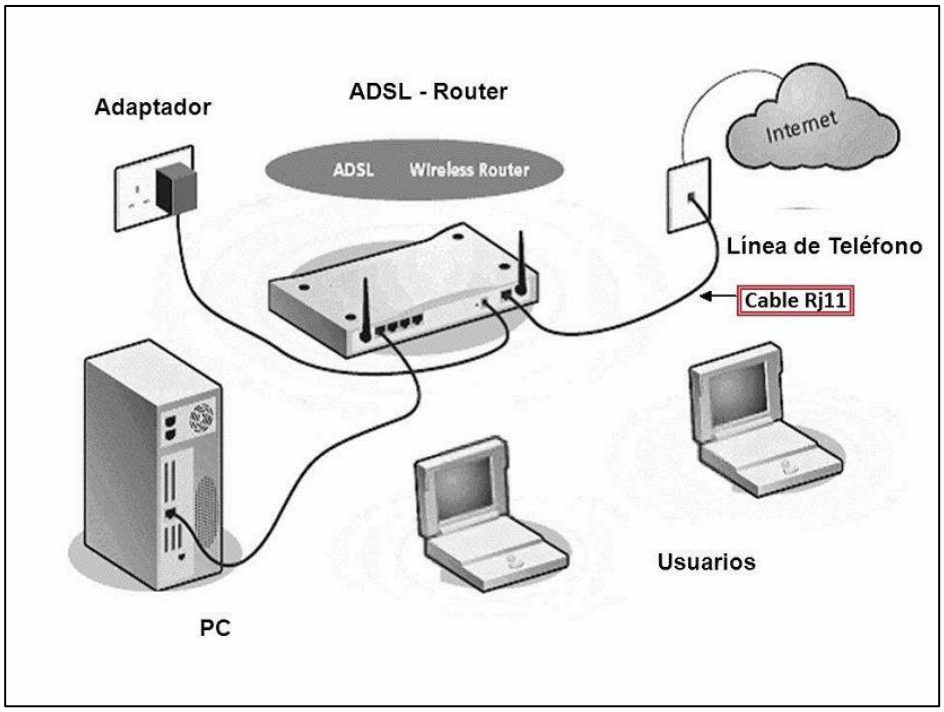


Figura 16: Representación de una conexión ADSL

Fuente: https://www.tiposde.com/conexion-adsl.html

2.2.3.1.4 Cable

Es la forma de conexión más tradicional y utilizada para transferir información. Esta tecnología usa dos variantes de conexión fibra óptica y cable coaxial:

- **Fibra Óptica**

Es posible transferir información en forma de pulsos de luz a través de grandes distancias mediante la tecnología de la fibra óptica, que utiliza hilos de fibra de vidrio o plástico para transportar la información.

Un cable de fibra óptica está formado por fibras ópticas que tienen aproximadamente el diámetro de un cabello humano y que, al unirse, permiten transportar más datos a través de mayores distancias y a mayor velocidad que otros medios. Es la tecnología que hace posible el suministro de servicios de Internet, teléfono y televisión a los hogares y empresas mediante sistemas de cable de fibra óptica. (Verizon, 2021)

De acuerdo a la figura 17, se muestra la composición física de la fibra óptica común.

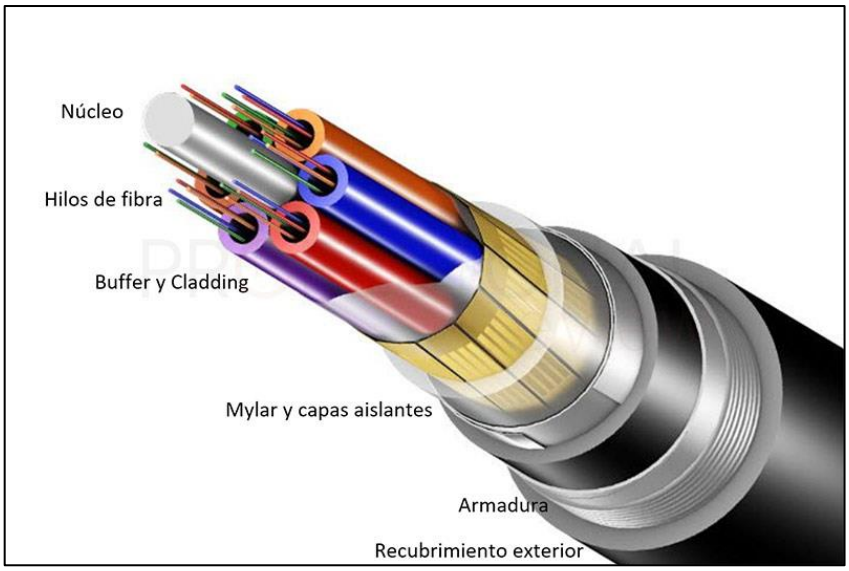


Figura 17: Composición de la fibra óptica

Fuente: https://www.profesionalreview.com/2019/02/15/fibra-optica-que-es/

- **Coaxial**

Las señales eléctricas de alta frecuencia son transportadas por este cable, que tiene un núcleo conductor central formado por uno o varios hilos sólidos o trenzados, generalmente de cobre, que está cubierto por un material aislante dieléctrico, que a su vez está cubierto por una lámina exterior de metal conductor, generalmente de cobre, y se utiliza para transmitir señales eléctricas de alta frecuencia superiores a las transportadas por los pares trenzados. El revestimiento metálico exterior proporciona un segundo conductor, que también funciona como barrera contra el ruido. Hay una pantalla aislante que cubre este conductor y una vaina de plástico que cubre todo el cable. (Nayeli, s.f.)

Según la figura 18, se puede observar la estructura de un cable coaxial.

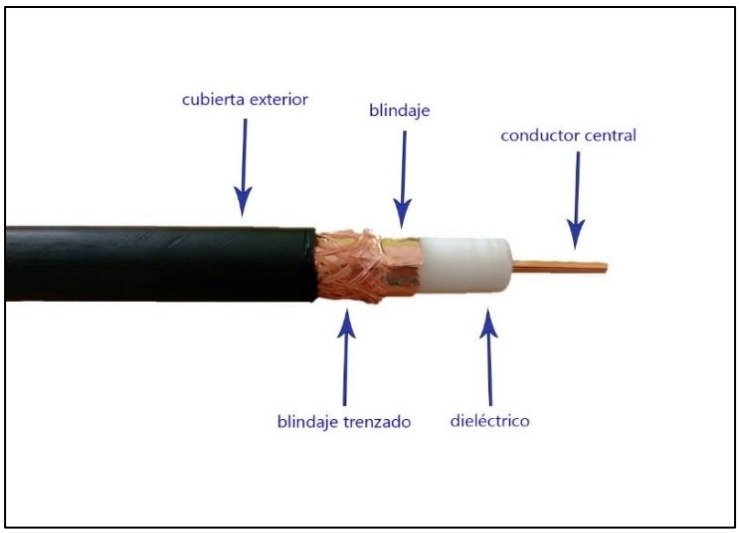


Figura 18: Composición de un cable coaxial.

Fuente: https://blog.gruponovelec.com/redes-vdi/cable-coaxial-tipos-y-caracteristicas/

De acuerdo a la tabla 1, se presenta las diferencias entre la conexión por fibra óptica y coaxial.

Tabla 1.
Ventajas y desventajas entre fibra y óptica y coaxial

CARACTERÍSTICA	FIBRA ÓPTICA	CABLE COAXIAL
Conexión	FTTH	HFC
Tipo de transmisión	PULSOS DE LUZ	ELECTRICIDAD
Interferencias electromagnéticas	NO	SI
Conexión largas distancias	SI	NO
Segura ante terceros	NO	SI
Resistente y manipulable	NO	SI
Compartida con vecinos	NO	SI

Fuente: https://queadslcontratar.com/guias/diferencias-fibra-optica-cable-coaxial

2.2.3.1.5 Inalámbrico

"Son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas. Las redes inalámbricas no solo se emplean para realizar conexión de datos, con frecuencia se utilizan para emitir señal de televisión, en telefonía, para seguridad (webcam), para sensores y domótica." (Andreu, 2010, p.212)

De acuerdo a la figura 19, se observa un diagrama tradicional de la conexión inalámbrica.

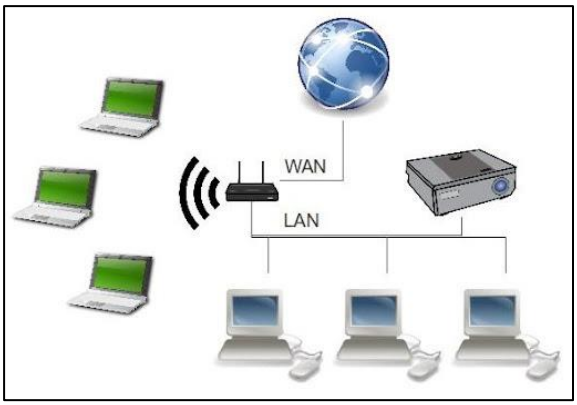


Figura 19: Representación de una conexión inalámbrica.

Fuente: http://www.iered.org/

2.2.3.1.6 Satelital

Es una conexión a internet mediante ondras electromagnéticas utilizando como medio de comunicación un satélite y una estación terrena. La tecnología satelital más conocida como VSAT, hace uso de un aparato para descodificar la señal y proporcionar la señal correcta a la instalación del usuario. Es habitual utilizar cable coaxial para enlazar la antena parabólica y el equipo decodificador. Cuando se conecta el decodificador al equipo del cliente, se utiliza un cable ethernet o USB para enlazar ambos dispositivos. (Santos, 2014, p.376).

Según la figura 20, se muestra el diagrama de una conexión satelital.

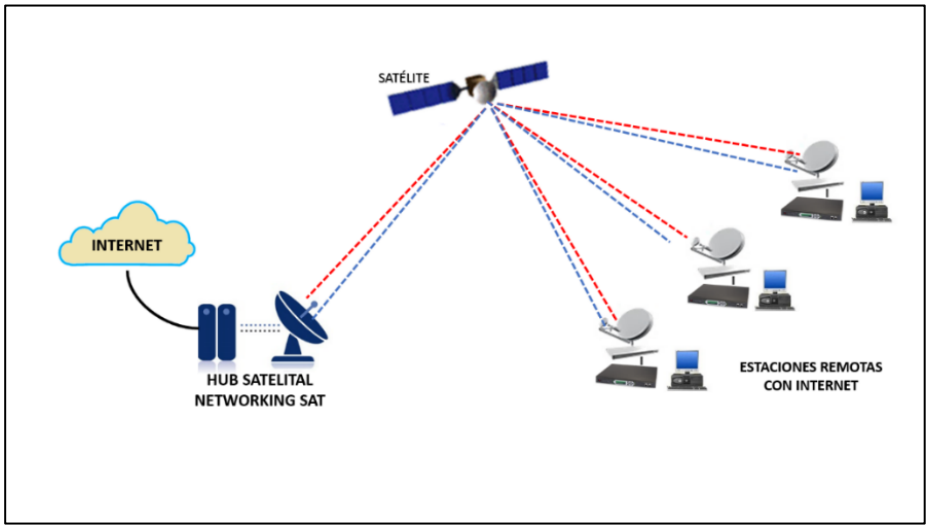


Figura 20: Representación de una conexión satelital

Fuente: https://networkingsat.com/blog/que-es-internet-satelital/

2.3 Definición de términos básicos

- Enlace a internet: Cuando se vincula cierta información con otra, se está conectando de un lugar a otro. (Sistemas, 2021)

- Firewall: La configuración de un dispositivo o grupo de dispositivos para restringir el acceso no autorizado a una determinada región de una red, permitiendo al mismo tiempo que las comunicaciones permitidas viajen a través de la zona. (Aguilera, 2011, p.154)

- Fortiwan: se trata de un dispositivo perimetral de Fortinet que proporciona las capacidades de equilibrio de carga distribuible para el tráfico dentro de una red, túneles de enrutamiento que distribuyen el tráfico de Internet a través de redes de área amplia, y otras características. (CISRT,2019)

- Internet: se trata de una red mundial de redes vinculadas, cada una de las cuales es independiente y autónoma por derecho propio. (Rodriguez, 2007, p.3)

- Ips: Se trata de dispositivos situados en lugares estratégicos de una red interna que evalúan continuamente el tráfico y registran los resultados en una base de datos para poder realizar acciones en tiempo real con el fin de contrarrestar la actividad hostil. (Sarubbi, 2008, p.14)

- Isp: Cuando se trata del diseño de su red interna, su funcionamiento y los métodos utilizados para suministrar los servicios que ofrecen, los proveedores de servicios de Internet (ISP) son empresas que revelan muy poca información. (Villa y Villanueva, 2013, p.14)

- Lan: Puede caracterizarse como un conjunto de piezas físicas y lógicas que conectan entre sí una gran variedad de dispositivos en un área restringida, como un edificio, un campus u otro entorno similar. (Berral, 2014, p.6)Nat: La traducción de direcciones de red es el proceso de cambiar una dirección

IP por otra en la cabecera del paquete IP, y también se conoce como traducción de direcciones. (Íñigo y Barceló, 2008, p.314)

- Políticas en seguridad: Hacen posible el bloqueo o la autorización de ciertas categorías de tráfico de red que no están definidas en una política de excepción. También especifica qué funcionalidades del cortafuegos están activas y cuáles están desactivadas en el firewall. (idgrup, s.f.)

- Red de Comunicación: Sistema que hace posible que los usuarios de ordenadores y dispositivos, compartir el equipamiento de los ordenadores conectados, programas informáticos, datos, voz, videos, etc. (Berral, 2014, p.2)

- Router: En cuanto a la conexión en red, se distingue de la competencia por su capacidad para enlazar redes internas y externas al mismo tiempo. (Benchimol, 2010, p.43)

- Servidor: En el contexto de una red, los servidores son piezas de hardware informático que prestan servicios a otros ordenadores de la red. Los servidores y los usuarios pueden acceder a la información que suministran. En comparación con los ordenadores de sobremesa, son más grandes y más potentes. (Marchionni, 2011, p.23)

- Switch: Es aquel dispositivo de red que conecta estaciones de trabajo, servidores, routers, hubs y otros switches actuando como punto de conexión. (Valdivia, 2015, p.37)

- Wan: “Wide Area Network” (Red de Área Amplia). Una red que permite enviar datos a grandes distancias, lo que hace posible transportar información por todo el mundo. (Severance, 2015, p.19)

CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL

3.1 Determinación y análisis del problema:

El grupo Dalisa S.A.C es una empresa colaboradora, de América Móvil Perú SAC (Claro), evidenció que muchas empresas corporativas, de diferentes rubros laborales, no contaban con una eficiente calidad de servicio de internet dedicado y seguridad perimetral. De acuerdo a las estadísticas, el Perú ocupa el Puesto 17 del ranking Latinoamericano en seguridad perimetral de red, también llamado ciberseguridad y sufriendo más de 613 millones de ataques cibernéticos, según informa la plataforma Threat Intelligence Insider Latin America de Fortinet (gestión, 2020).

Por esta razón, según nos muestra la tabla 2, la empresa mediante su área de preventa efectuó un estudio de mercado a finales del 2019, del servicio de seguridad a las empresas que aún no contaban con este sistema importante de protección, entre ellas el cliente SONEPAR.

Tabla 2.
Aumento de usuarios consumidores por internet en el Perú.

AÑO	CANTIDAD DE USUARIOS
2018	6.000.000
2019	11.800.000
Crecimiento	5.800.000

Fuente: https://branch.com.co/

Como consecuencia, el cliente SONEPAR guiándose de la información sobre el aumento constante de personas que utilizan el internet para adquirir u ofrecer productos; solicito un servicio con respaldo de internet para evitar inconvenientes en sus ventas virtuales.

La empresa SONEPAR se dedica a la venta de todo tipo de herramientas eléctricas y electrónicas a nivel nacional e internacional decidió adquirir los servicios para el respaldo de internet y seguridad de su red, por lo que opto con contratar a la empresa Grupo Dalisa.

El cliente informo que su primer problema, era que solo contaba con un proveedor de internet llamado Americatel con un ancho de banda 30 Mbps, el cual para mi grupo de trabajo era de baja eficiencia para una empresa en crecimiento de usuarios y actividades de producción.

El segundo problema era que también presentaba una protección de red básica mediante un filtrado de paquetes aplicado por el mismo router de 30 Mbps y una zona desmilitarizada (DMZ) para sus servidores, observando con mi equipo de trabajo que no poseía un firewall para su seguridad perimetral.

Considerando estos dos problemas procedí con el proceso de gestión para la optimización del servicio del cliente, participando desde el diseño de la topología, continuando con la implementación de los equipos en sede. Finalizando con la validación y correcta operación de actividades de los equipos en producción siendo esta última mi principal labor en la empresa como analista de soporte.

3.2 Modelo de solución propuesto

La solución propuesta se basó mediante un proceso de coordinación con el cliente para ejecutar las etapas de actividades según observamos el diagrama de la figura 21.

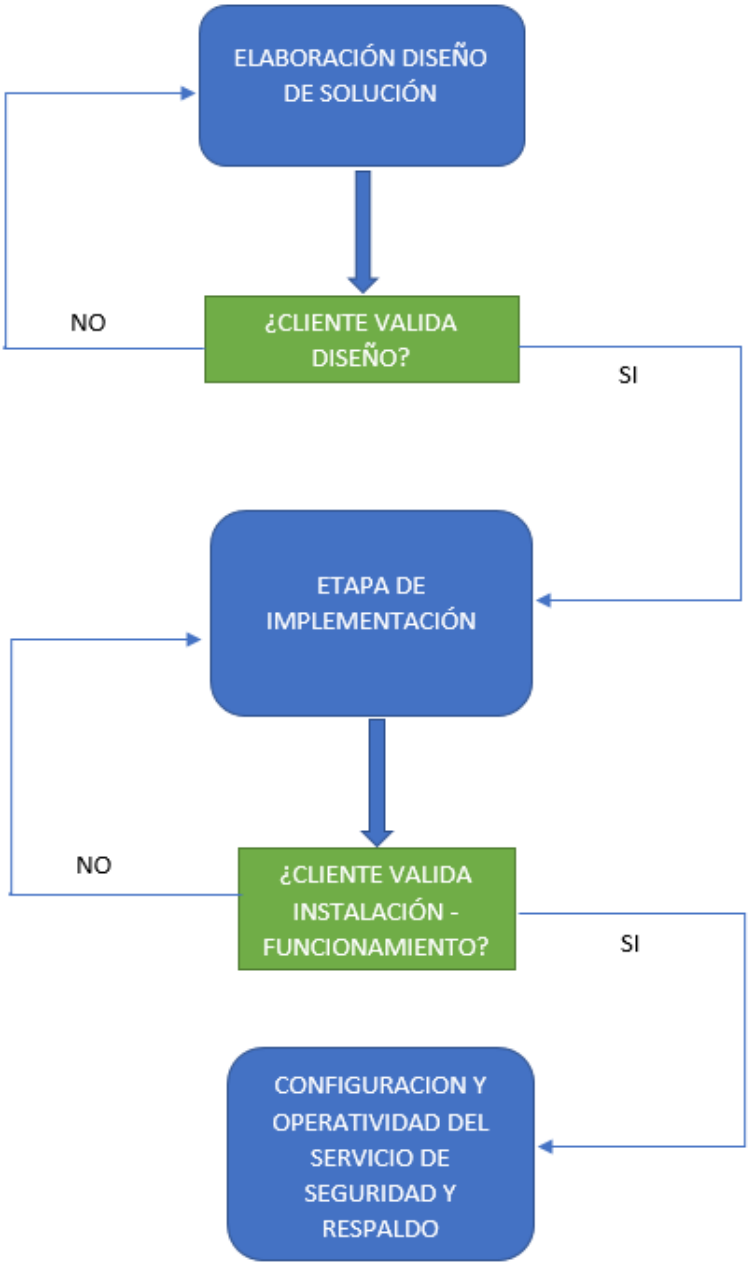


Figura 21: Diagrama de Flujo como proceso de solución para el cliente Sonepar

Fuente: Elaboración Propia

A continuación, según se muestra en la tabla 3, se presentó el cronograma del proceso de las 3 actividades de solución realizadas para el cliente SONEPAR

Tabla 3.
Cronograma de ejecución para el proyecto de seguridad de SONEPAR

FECHA	ACTIVIDAD A DESARROLLAR	PERSONAL A CARGO
01/09/19 AL 13/09/19	DISEÑO	1 TÉCNICO, 1 INGENIERO
16/09/19 AL 11/10/19	IMPLEMENTACION	2 TÉCNICOS, 1 INGENIERO
12/10/19 - ACTUALIDAD	OPERATIVIDAD	ÁREA SOPORTE

Fuente: Elaboración propia

3.2.1 Diseño

La topología del diseño previamente se realizó con una visita al cliente para observar y confirmar el estado de los equipos y el acceso a internet con los que contaba y efectuar un diagnóstico situacional para obtener un orden en la implementación de los equipos de seguridad y del respaldo de internet.

De acuerdo a lo mostrado en la figura 22, se observó que inicialmente contaba con un equipo router, su switch de capa 2, una zona desmilitarizada para sus servidores y un servicio RPV ya establecidas para la comunicación con sus sedes remotas. Comprobando que no poseía los equipos de respaldo y seguridad.

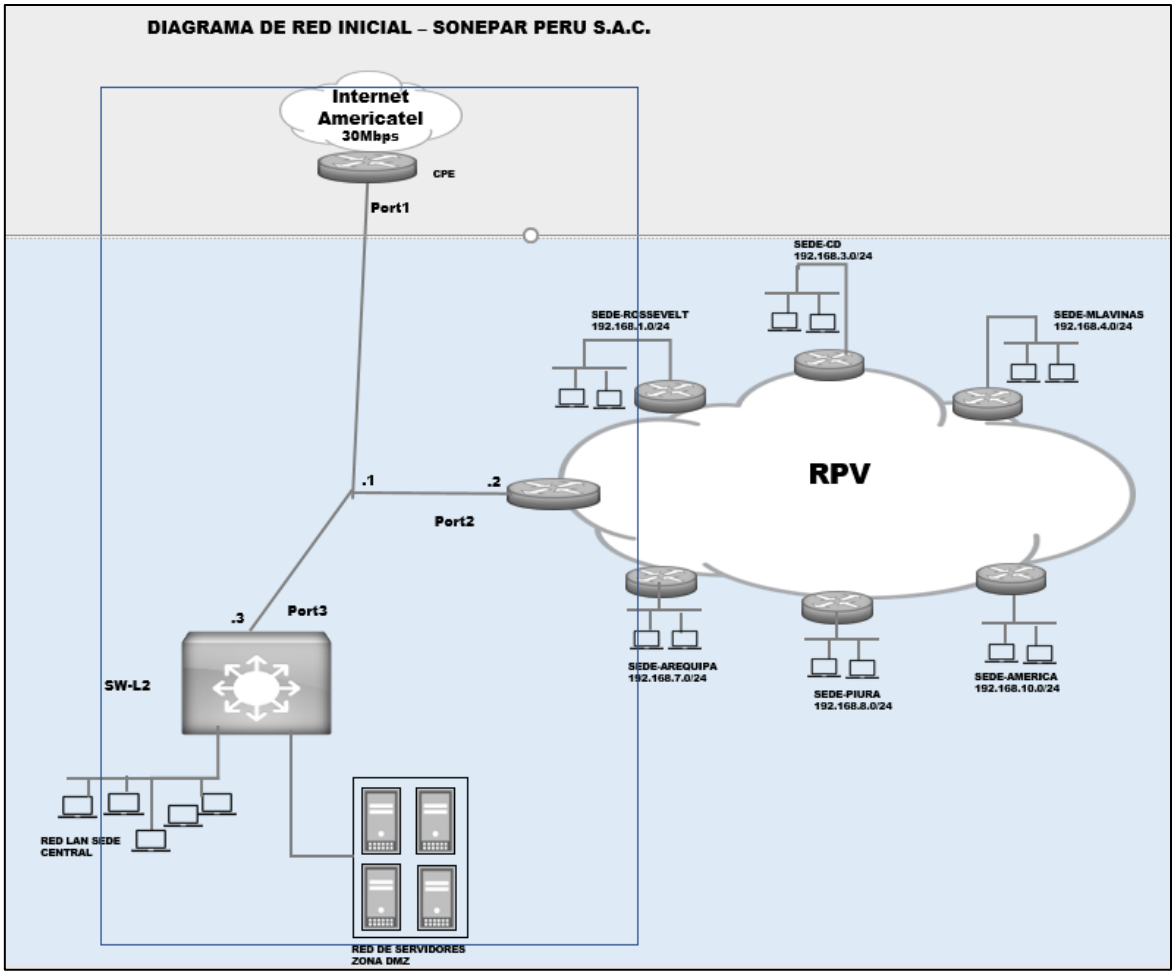


Figura 22: Topología inicial empresa SONEPAR

Fuente: Elaboración propia

A continuación, en la figura 23 se presentó la topología de nuestra propuesta de solución, donde se realizó la adición del equipo de respaldo de internet FORTIWAN 200B más el equipo de seguridad perimetral firewall FORTIGATE 200E en el diseño final para el cliente, teniendo en cuenta que el nuevo router agregado a la topología para lograr el respaldo de internet, instalado por el área de planta externa de la empresa América Móvil Perú.

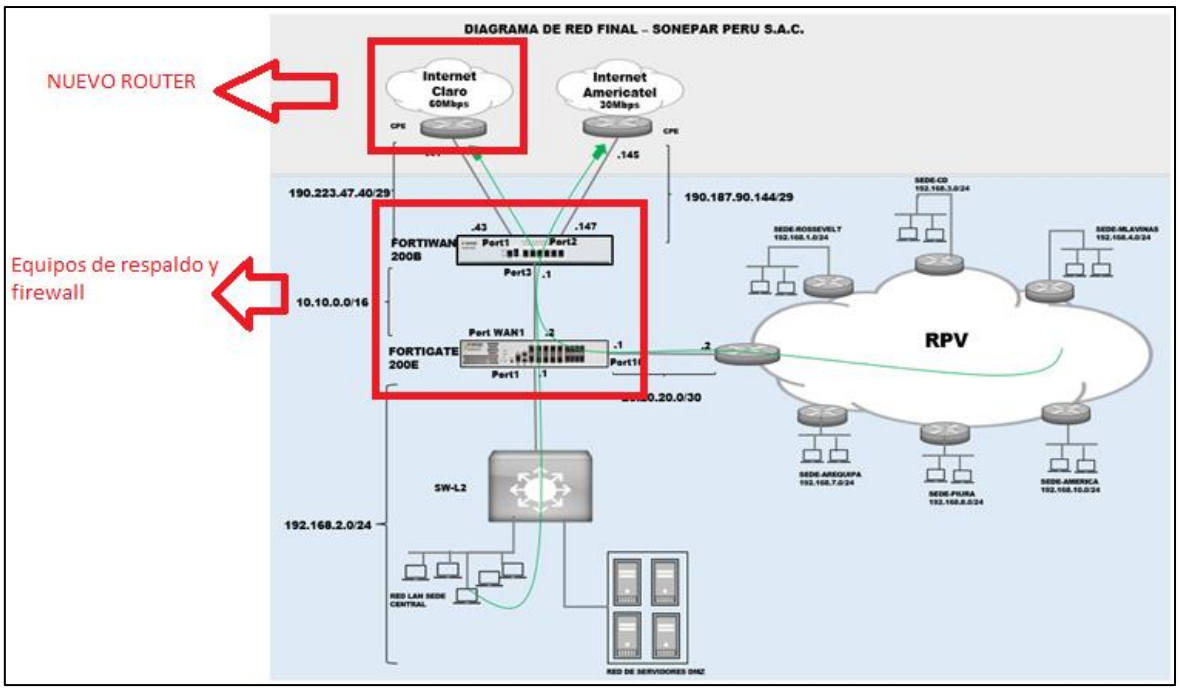


Figura 23: Topología final empresa SONEPAR

Fuente: Elaboración propia

Este diseño se envió al cliente SONEPAR para su conocimiento y posterior autorización continuando con la segunda actividad: la implementación.

3.2.2 Implementación del servicio

El cliente al quedar conforme con el diseño elaborado, autorizó la instalación de los equipos ofrecidos. Como se puede observar en la figura 24, el data center del cliente consta de 3 gabinetes divididos para una mejor identificación de los equipos de internet seguridad.

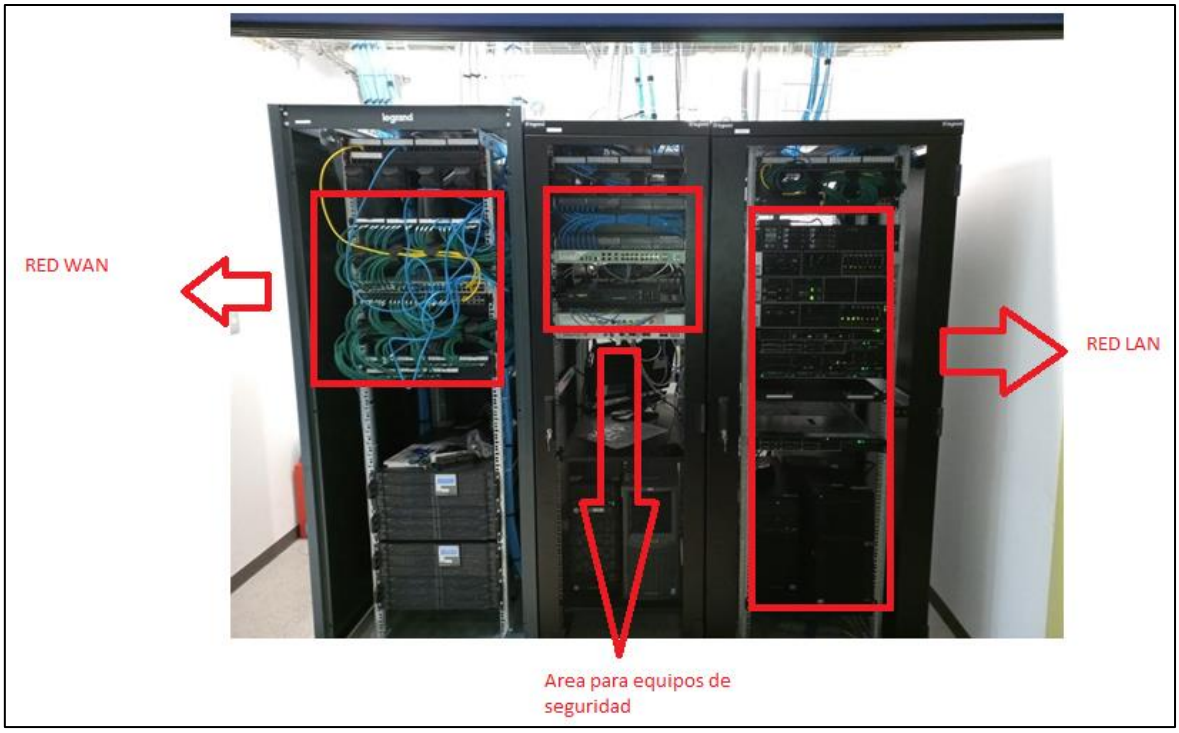


Figura 24: Datacenter principal del cliente SONEPAR

Fuente: Elaboración propia

A continuación, se procedió a identificar el equipo router como se muestra en la figura 25 instalado por el área de planta externa de América Móvil Perú (Claro) para conectarlo al equipo balanceador Fortiwan 200B y Fiewall 200E que es nuestra propuesta de solución para el respaldo de internet.

Figura 25: Equipos enrutadores de la empresa sonepar

Fuente: Elaboración propia

Después se instaló los equipos de respaldo y seguridad en el gabinete correspondiente al área de seguridad se encienden, como se puede observar en la figura 26:

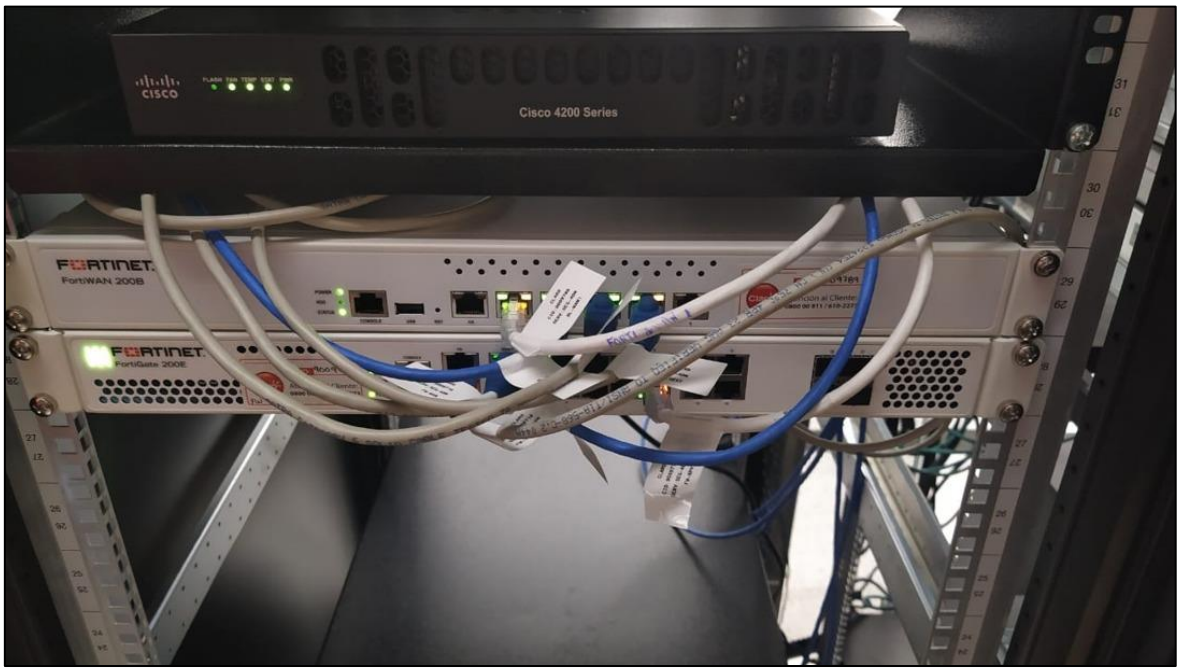


Figura 26: Equipos fortiwan 200b y fortigate 200E instalados en sede

Fuente: Elaboración propia

El primer equipo implementado fue el de respaldo de internet como nos muestra la figura 27, un FORTIWAN 200B es un balanceador de carga para el respaldo de internet, entre sus principales características tenemos:

- Tiene un rendimiento de ancho de banda límite 200 Mbps
- Posee 6 interfaces WAN base RJ-45, 1 interfaz consola rj45 y 2 puertos USB tipo A
- Su voltaje requerido es de 120/230v (50 A 60HZ)
- Un Peso de 9,92 libras
- Tecnología de conexión por cableado

Figura 27: Equipo fortiwan 200B

Fuente: https://www.avfirewalls.com/FortiWAN-200B.asp

Para la conexión entre el enrutador – balanceador – firewall – switch se usarán cables UTP con sus respectivos conectores RJ45 según podemos observar en la figura 28:

Figura 28: Conectores rj45 para cables utp

Fuente: https://cornershopapp.com/

El segundo equipo implementado fue para la seguridad perimetral, como se observa en la figura 29, un firewall FORTIGATE 200E, entre sus principales características tenemos:

- Tiene un rendimiento de ancho de banda límite: 1.8 Gbps
- Posee 2 interfaces WAN rj45, 14 interfaces LAN rj45, 1interfaz consola rj45
- Su voltaje requerido es de 120/230v (50 A 60HZ)
- Peso de 11,9 libras
- Tecnología de conexión por cableado

Figura 29: Equipo fortigate 200E

Fuente: https://gridsolutionsperu.com/

3.2.3 Configuración y operatividad

- Equipo de respaldo

Al tener el balanceador Fortiwan 200B instalado, se verifico el encendido en la información del sistema del equipo y la conexión de ambos enlaces de internet, como nos muestra las figuras 30, 31 y 32 respectivamente:

System Information

	Host	Peer
Version	V4.05.0-build0317 171004	None
Model	FWN200B	None
Serial Number	FWN2HBT218000278	None
Uptime	18 day(s), 00:21:37	None
State	Master	None
Max Bandwidth	200 Mbps	
VRRP State	VRRP Disabled	

Figura 30: Información del sistema del equipo Fortiwan 200B

Fuente: Sistema Operativo FortiOS

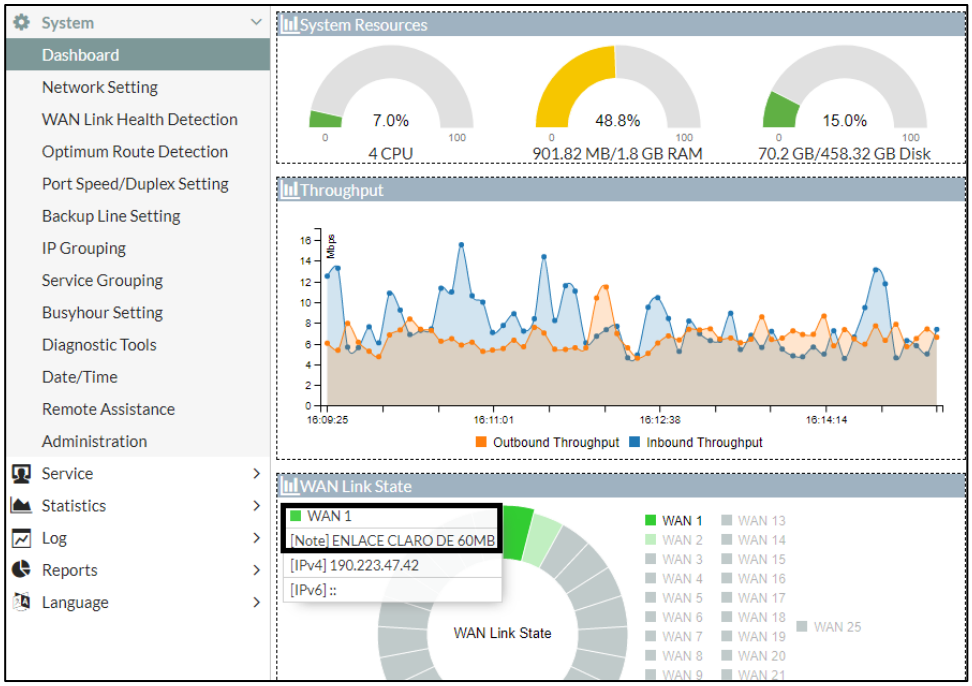


Figura 31: Enlace WAN 1 de Claro conectado

Fuente: Sistema Operativo FortiOS

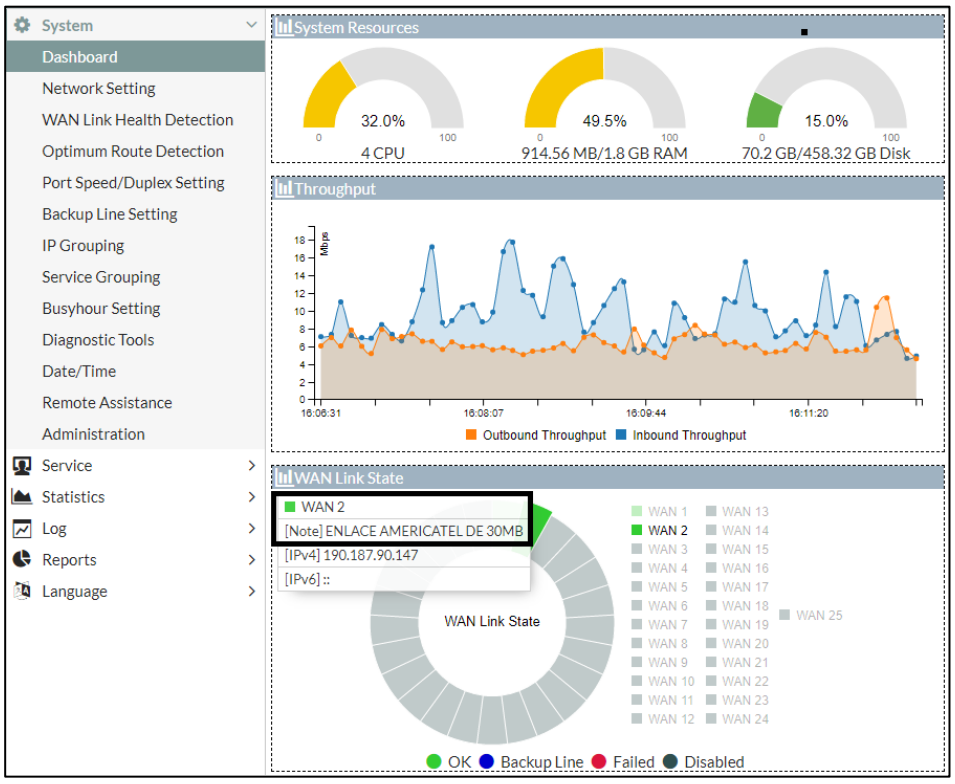


Figura 32: Enlace WAN 2 Americatel conectado

Fuente: Sistema Operativo FortiOS

Después de ver el encendido del equipo de respaldo de internet se configuró lo siguiente:

1.- Los puertos WAN para ambos enlaces de internet (CLARO Y AMERICATEL), según se observa en las figuras 33 y 34 respectivamente.

```
wan-array {
        wan@1 {
                enable 1
                note "ENLACE CLARO DE 60MB"
                wan-type "Routing Mode"
                downstream 61440
                upstream 61440
                default-gateway 190.223.47.41
                wan-port port1
                basic-subnet-array {
                        subnet { # 1
                                subnet-type "Subnet in WAN"
                                localhost-ip-array {
                                        ip 190.223.47.42 # 1
                                        ip 190.223.47.43 # 2
                                        ip 190.223.47.44 # 3
                                        ip 190.223.47.45 # 4
                                        ip 190.223.47.46 # 5
                                }
                                netmask 255.255.255.248
                        }
                        subnet { # 2
                                subnet-type "Subnet in WAN"
                                localhost-ip-array {
                                        ip 190.119.229.162 # 1
                                        ip 190.119.229.163 # 2
                                        ip 190.119.229.164 # 3
                                        ip 190.119.229.165 # 4
                                        ip 190.119.229.166 # 5
                                }
                                netmask 255.255.255.248
                        }
                }
        }
```

Figura 33: Configuración de interfaz WAN de claro

Fuente: Elaboración propia

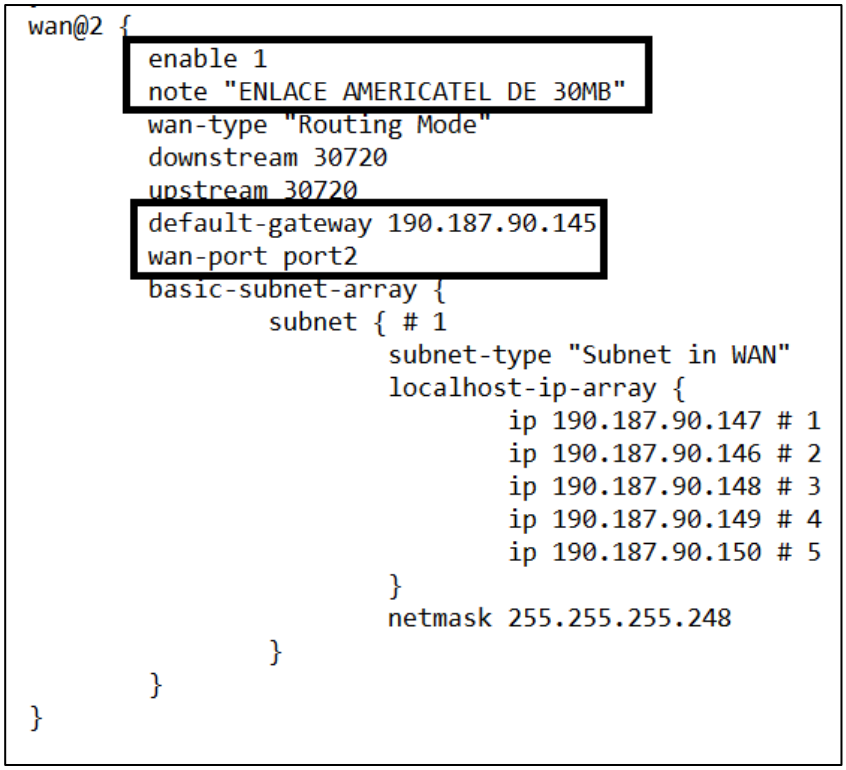


Figura 34: Configuración de interfaz WAN de Americatel

Fuente: Elaboración propia

2.- Declaración de los segmentos para la red LAN del cliente en el equipo, como se muestra en la figura 35:

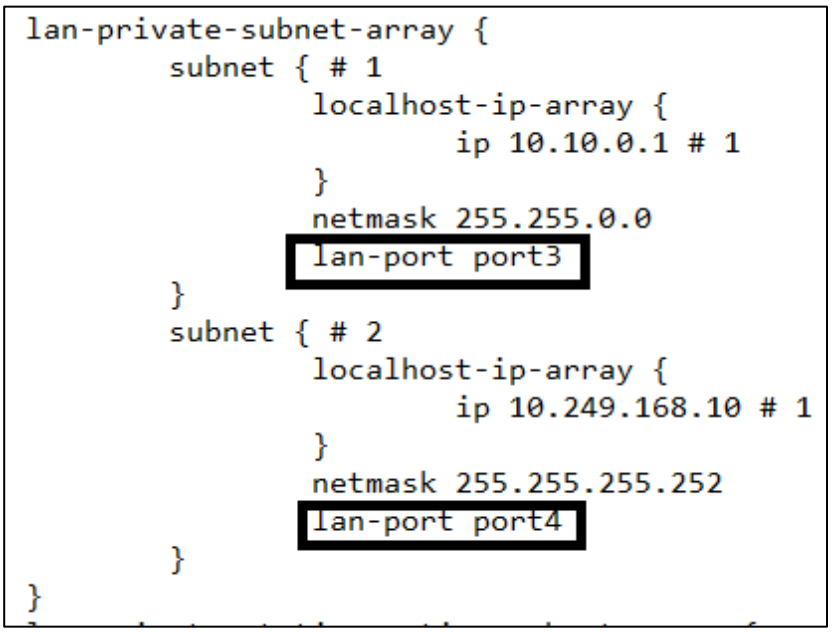


Figura 35: Configuración puertos LAN del cliente

Fuente: Elaboración propia

3.- Las reglas de NAT el cual brinda la comunicación de sus servidores y navegación a internet mediante la ips públicas, ya que el equipo fortiwan 200B también actúa como una primera capa de seguridad, como se ve en la figura 36 se configuró las reglas de NAT para la WAN 1.

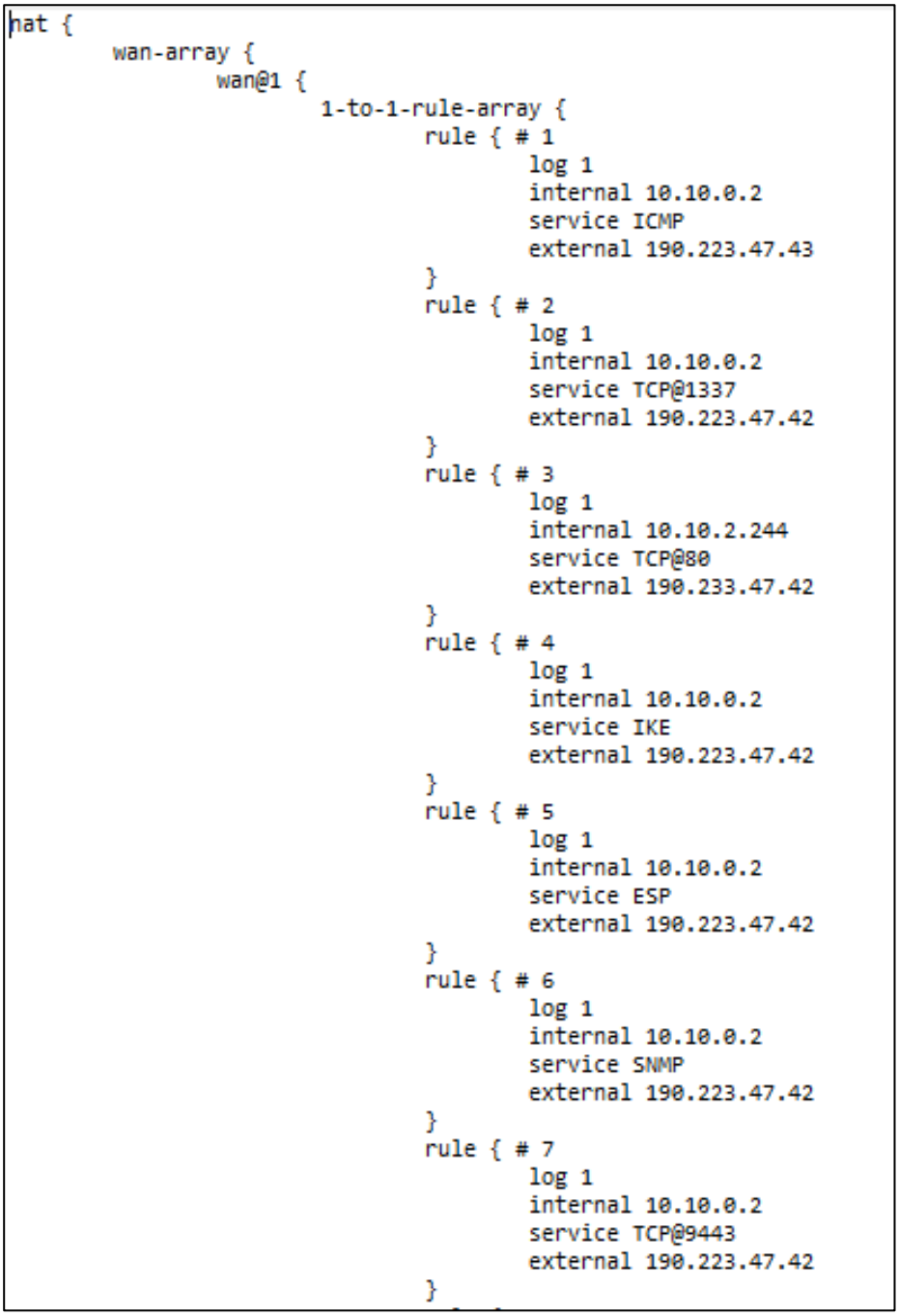


Figura 36: Configuración NAT para la WAN 1 de claro

Fuente: Elaboración Propia

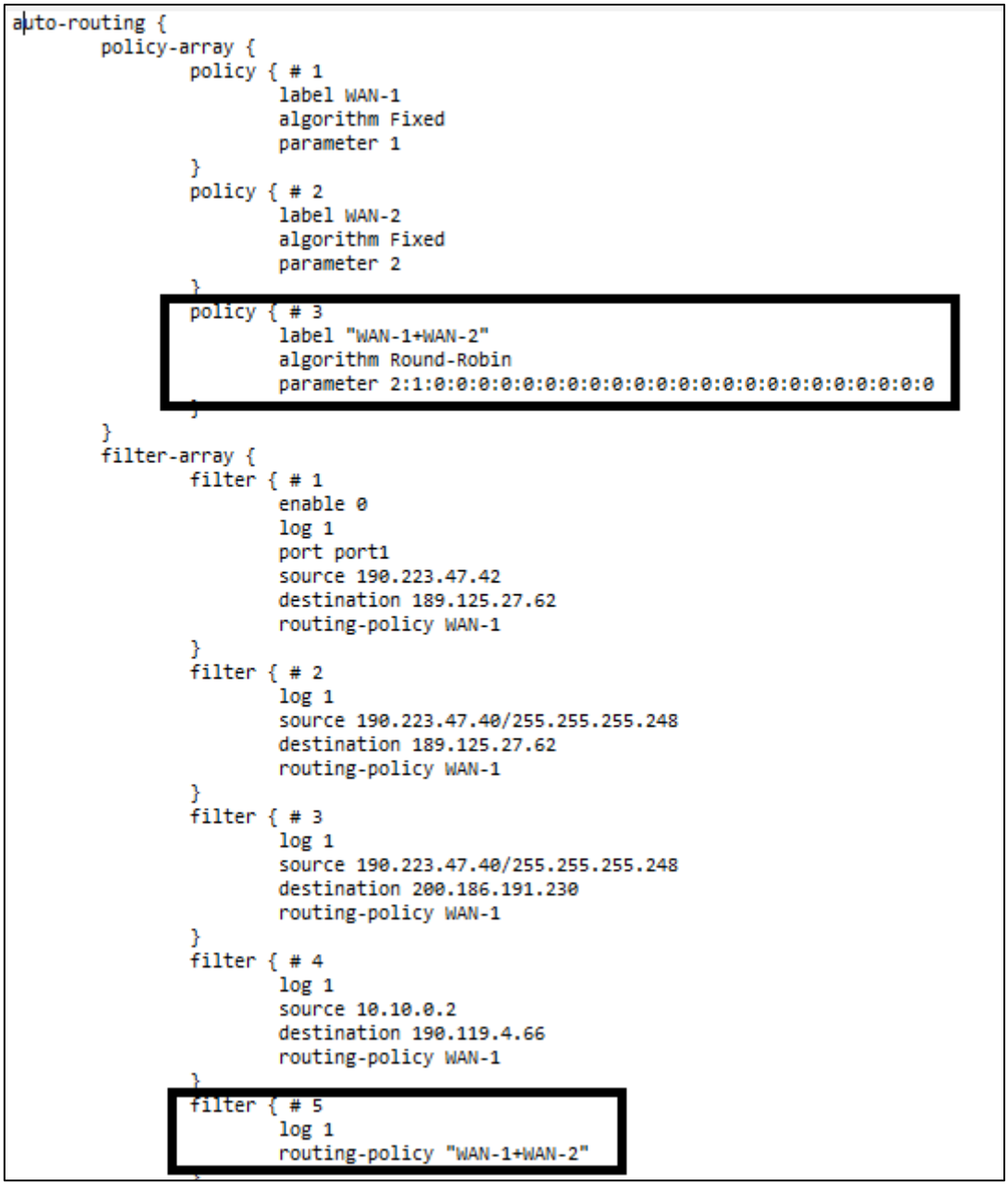
Según podemos observar en la figura 37, también se configuró las reglas de NAT para la WAN 2.

```
        wan@2 {
                1-to-1-rule-array {
                        rule { # 1
                                log 1
                                internal 10.10.0.2
                                service TCP@9443
                                external 190.187.90.146
                        }
                }
                rule-array {
                        rule { # 1
                                source 190.187.90.146-190.187.90.150
                                translated "No NAT"
                        }
                        rule { # 2
                                log 1
                                translated 190.187.90.147
                        }
                }
        }
}
```

Figura 37: Configuración NAT para la WAN 2 de Americatel

Fuente: Elaboración propia

4.- Continuamos con el paso importante de realizar la configuración de conmutación como el respaldo mutuo de ambos enlaces de internet para evitar caídas de servicio. Como se muestra en la figura 38:



```
auto-routing {
        policy-array {
                policy { # 1
                        label WAN-1
                        algorithm Fixed
                        parameter 1
                }
                policy { # 2
                        label WAN-2
                        algorithm Fixed
                        parameter 2
                }
                policy { # 3
                        label "WAN-1+WAN-2"
                        algorithm Round-Robin
                        parameter 2:1:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
                }
        }
        filter-array {
                filter { # 1
                        enable 0
                        log 1
                        port port1
                        source 190.223.47.42
                        destination 189.125.27.62
                        routing-policy WAN-1
                }
                filter { # 2
                        log 1
                        source 190.223.47.40/255.255.255.248
                        destination 189.125.27.62
                        routing-policy WAN-1
                }
                filter { # 3
                        log 1
                        source 190.223.47.40/255.255.255.248
                        destination 200.186.191.230
                        routing-policy WAN-1
                }
                filter { # 4
                        log 1
                        source 10.10.0.2
                        destination 190.119.4.66
                        routing-policy WAN-1
                }
                filter { # 5
                        log 1
                        routing-policy "WAN-1+WAN-2"
                }
```

Figura 38: Configuración para lograr el respaldo de internet solicitado

Fuente: Elaboración propia

5.- Finalmente se validó la salida hacia internet desde ambos enlaces, según se observa en la figura 39 para enlace WAN1 de Claro.

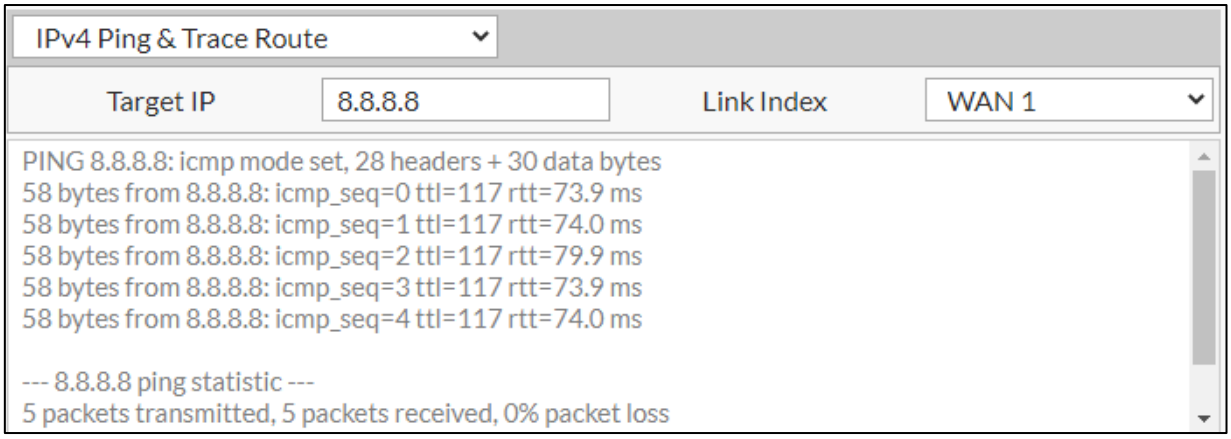


Figura 39: Conexión a internet desde la WAN 1 de claro

Fuente: Elaboración propia

Y para el enlace WAN2 de Americatel como se muestra en la figura 40.

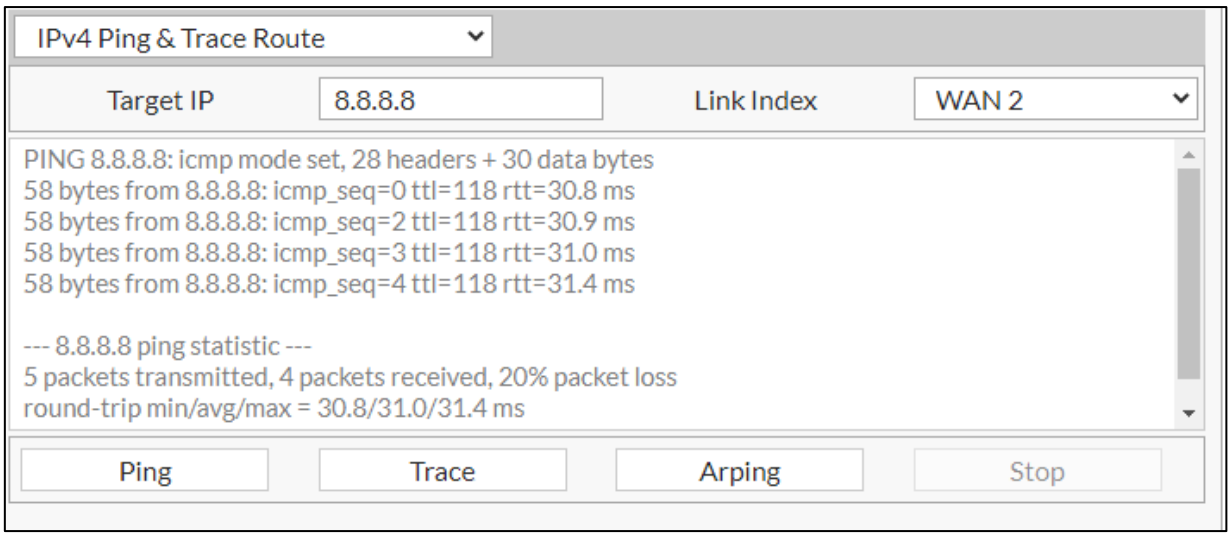


Figura 40: Conexión a internet desde la WAN 2 de Americatel

Fuente: Elaboración propia

-SEGURIDAD PERIMETRAL

Con el firewall ya instalado, se verifico su funcionamiento mediante la interfaz de estado del equipo, como se muestra en la figura 41:

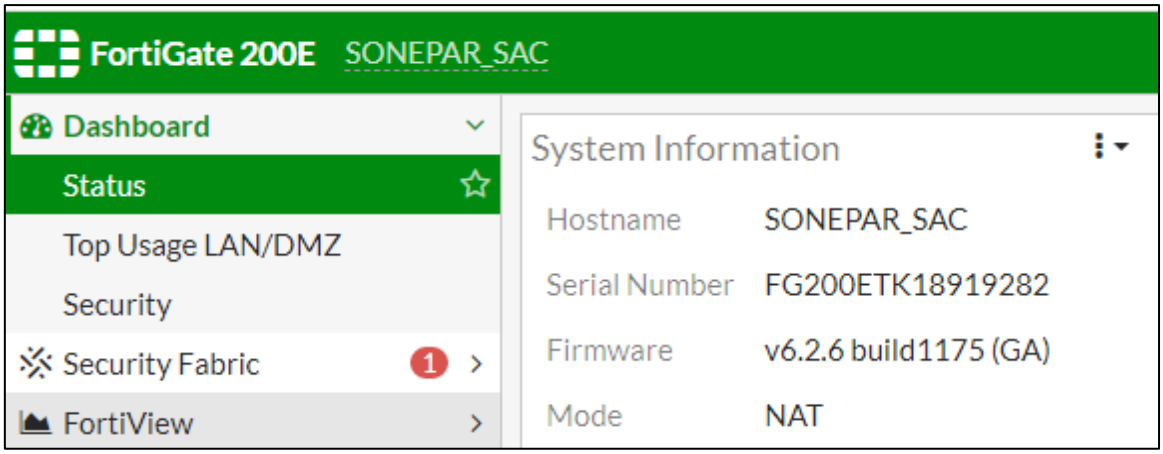


Figura 41: Interfaz de encendido del Fortigate 200E

Fuente: Sistema Operativo FortiOS

Después de ver el encendido del equipo de seguridad perimetral se configuró lo siguiente:

1.- Parámetros de acceso al equipo, como se muestra en la figura 42:

```
#config-version=FG200E-6.2.6-FW-build1175-201110:opmode=0:vdom=
0:user=NSOC-CONNECT
#conf_file_ver=4867791380368186
#buildno=1175
#global_vdom=1
config system global
    set admin-sport 9443
    set admin-ssh-port 1337
    set admintimeout 60
    set alias "FG200ETK18919282"
    set gui-device-latitude "-12.098283903433646"
    set gui-device-longitude "-77.01952457427979"
    set hostname "SONEPAR_SAC"
    set switch-controller enable
    set timezone 11
end
```

Figura 42: Configuración de acceso al equipo Fortigate 200E

Fuente: Elaboración propia

2.- Interfaces LAN Y WAN, para la comunicación con el balanceador Fortiwan 200B y red interna del cliente (switch), según se muestra en la figura 43:

```
config system switch-interface
    edit "LAN"
        set vdom "root"
        set member "port1"
    next
end
config system interface
    edit "mgmt"
        set vdom "root"
        set ip 10.249.161.154 255.255.255.252
        set allowaccess ping https ssh http fgfm
        set type physical
        set dedicated-to management
        set alias "VRF-GESTION"
        set role lan
        set snmp-index 1
    next
    edit "ha"
        set vdom "root"
        set status down
        set type physical
        set snmp-index 2
    next
    edit "wan1"
        set vdom "root"
        set ip 10.10.0.2 255.255.0.0
        set allowaccess ping https ssh snmp http fgfm fabric
        set type physical
        set alias "WAN"
        set snmp-index 3
    next
    edit "wan2"
        set vdom "root"
        set allowaccess ping fgfm
        set status down
        set type physical
        set snmp-index 4
    next
```

Figura 43: Configuración interfaces WAN y LAN del Fortigate 200E

Fuente: Elaboración propia

3.- Rutas estáticas para definir la comunicación externa e interna, según se observa en la figura 44:

```
config router static
    edit 1
        set gateway 10.10.0.1
        set device "wan1"
    next
    edit 2
        set dst 192.168.1.0 255.255.255.0
        set gateway 20.20.20.2
        set device "port10"
        set comment "ROSSEVELT"
    next
    edit 3
        set dst 192.168.3.0 255.255.255.0
        set gateway 20.20.20.2
        set device "port10"
        set comment "CD"
    next
    edit 4
        set dst 192.168.4.0 255.255.255.0
        set gateway 20.20.20.2
        set device "port10"
        set comment "MALVINAS"
    next
    edit 5
        set dst 192.168.7.0 255.255.255.0
        set gateway 20.20.20.2
        set device "port10"
        set comment "AREQUIPA"
    next
```

Figura 44: Configuración de rutas estáticas para la comunicación en general

Fuente: Elaboración propia

4.- Políticas de seguridad para la navegación segura de los usuarios de la empresa del cliente, según se muestra en la figura 45:

```
config firewall policy
    edit 57
        set name "WHITE LIST-IP"
        set uuid 3b775f12-7ad8-51eb-150b-df7b947fbfb2
        set srcintf "LAN"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "46.105.85.33"
        set action accept
        set schedule "always"
        set service "TCP_8443" "UDP_8443" "TCP_8444" "UDP_8444"
        set logtraffic all
        set nat enable
    next
    edit 59
        set name "WHITE LIST"
        set uuid 46d26a86-7ad9-51eb-d51c-10161df57bed
        set srcintf "LAN"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "appliance.cloud.tenable.com"
"cloud.tenable.com" "deb.debian.org" "downloads.nessus.org"
"gateway.eva-sonepar.com" "nessus.org" "ocsp.digicert.com"
"plugins-customers.nessus.org" "plugins-us.nessus.org"
"plugins.cloud.tenable.com" "plugins.nessus.org" "tenable.com"
"tenablesecurity.com"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set comments " (Copy of WHITE LIST-IP)"
        set nat enable
    next
    edit 58
```

Figura 45: Configuración de políticas de seguridad para la navegar a internet

Fuente: Elaboración propia

5.- Filtros web para las políticas de navegación de los usuarios de la empresa del cliente, como se observa en la figura 46:

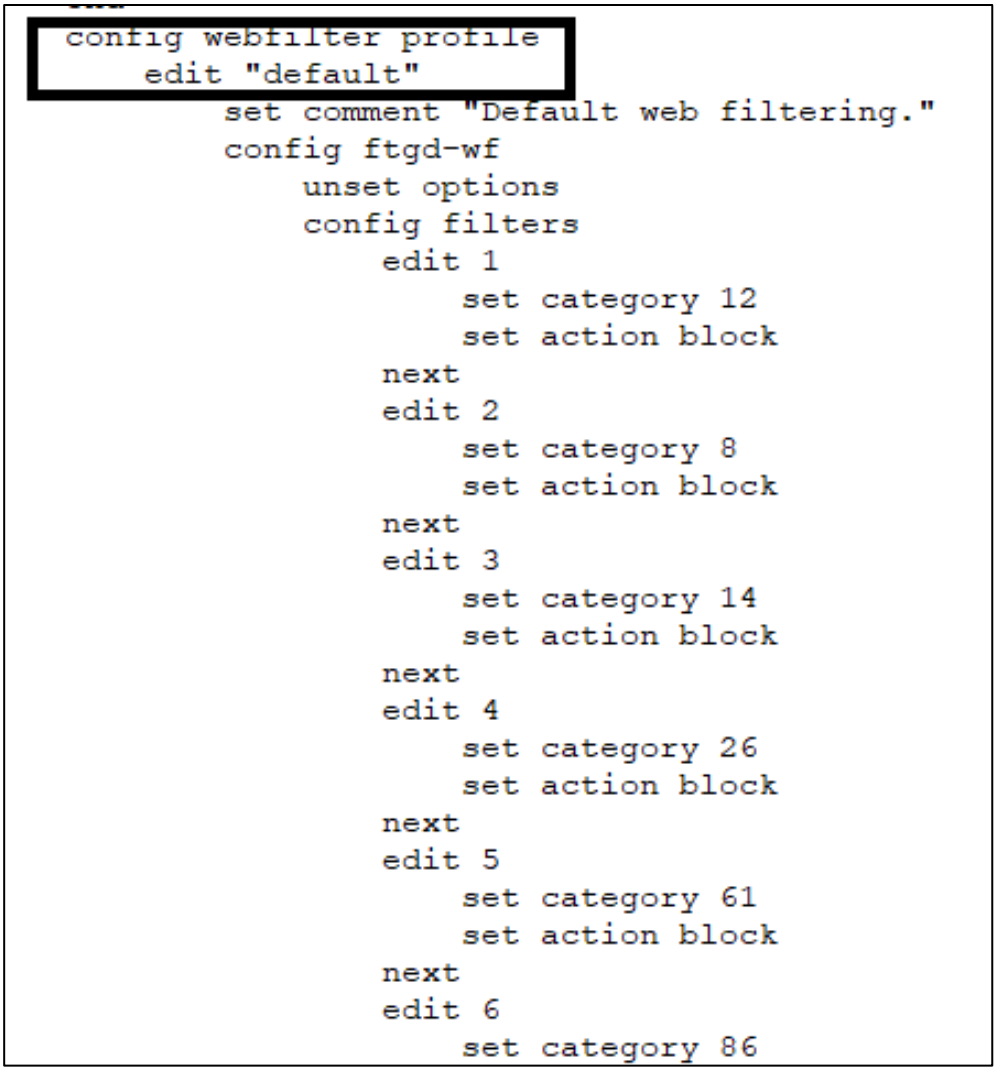


Figura 46: Configuración filtros web para la navegación de usuarios

Fuente: Elaboración propia

6.- Reglas de NAT para la comunicación con el balanceador y publicación de información de los servidores y servicios del cliente, según se muestra en la figura 47:

```
config firewall vip
    edit "VIP_8082_244"
        set uuid 4c310db0-f421-51e9-e5ed-f68b287989ac
        set extip 10.10.2.244
        set extintf "any"
        set portforward enable
        set mappedip "192.168.2.130"
        set extport 8082
        set mappedport 8082
    next
    edit "VIP_8085_236"
        set uuid e3b59268-f422-51e9-85da-e916271afaec
        set extip 10.10.2.236
        set extintf "any"
        set portforward enable
        set mappedip "192.168.2.236"
        set extport 8085
        set mappedport 8085
    next
    edit "VIP_3395_245"
        set uuid 2637217e-f423-51e9-6755-41ad39351e81
        set extip 10.10.2.245
        set extintf "any"
        set portforward enable
        set mappedip "192.168.2.245"
        set extport 3395
        set mappedport 3389
    next
```

Figura 47: Configuración de reglas NAT para la comunicación de los servidores

Fuente: Elaboración propia

7.- Configuración de seguridad VPN para el acceso del personal de la empresa desde una red externa, como se ve en la figura 48:

```
config vpn ssl settings
    set ssl-min-proto-ver tls1-1
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set source-interface "wan1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "full-access"
    config authentication-rule
        edit 1
            set groups "VPN-GROUP"
            set portal "VPNSONEPAR"
        next
    end
end
```

Figura 48: Configuración VPN para el acceso de usuario de la empresa

Fuente: Elaboración propia

8.- Finalmente se logra el acceso a internet desde el equipo de seguridad firewall comprobando la interacción entre la seguridad y el respaldo objetivo de nuestro trabajo, según se observa en la figura 49:

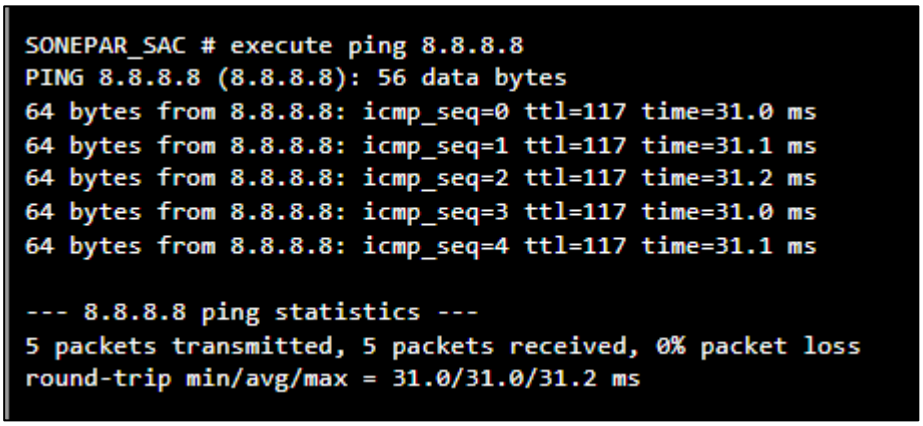


Figura 49: Conexión a internet desde el equipo de seguridad fortigate 200E

Fuente: Elaboración propia

9.- Se firma el acta de instalación como registro de conformidad del cliente (Véase Anexo 1)

3.3 Resultados

El resultado obtenido logró beneficiar a la empresa Grupo Dalisa con una ganancia económica de 3950 dólares americanos por el costo adicional de los equipos y servicio ejecutado al cliente por 3 años de contrato aproximadamente, mediante una inversión total de 12785 dólares americanos, como se muestra en la tabla 4.

Tabla 4.
Presupuesto de inversión del cliente y ganancia para GRUPO DALISA

EQUIPO / ACTIVIDAD	PRECIO ($)	GANANCIA ($)	SUB TOTAL
Fortiwan 200B	2058	300	2358
Fortigate 200E	7077	200	7277
Diseño e Instalación	-	750	750
Operatividad/Soporte	-	2400	2400
	TOTAL	3950	12785

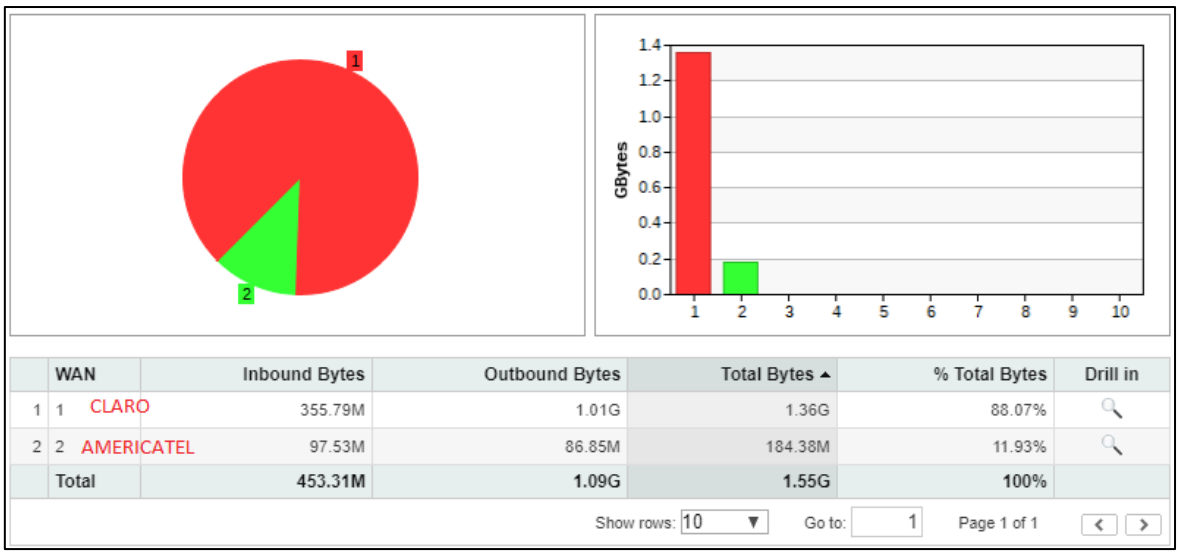
Fuente: Elaboración propia

A continuación, se detalla los resultados para el respaldo de internet y seguridad perimetral logrados para beneficio del cliente.

3.3.1 Respaldo de internet

1.- El cliente pudo contar con el respaldo permanente a internet, que se comprobó:

Verificando en el equipo Fortiwan 200B con ambos enlaces WAN activos y operando con sus respectivas funciones donde la interface WAN 1 principal es de Claro por la cantidad mayor de consumo de internet y su respaldo a internet el enlace WAN 2 de Americatel con menor consumo, según nos muestra la figura 50:



	WAN	Inbound Bytes	Outbound Bytes	Total Bytes ▲	% Total Bytes	Drill in
1	1 CLARO	355.79M	1.01G	1.36G	88.07%	
2	2 AMERICATEL	97.53M	86.85M	184.38M	11.93%	
	Total	453.31M	1.09G	1.55G	100%	

Show rows: 10 Go to: 1 Page 1 of 1

Figura 50: Medición del consumo de internet de ambos enlaces WAN

Fuente: Sistema Operativo FortiOS

2.- Se comprobó que la actividad de ventas online se mantuvo constante mediante:

La página oficial sonepar.pe, opción compra online redirigiéndose a la página sonemas.pe con ip publica 190.119.229.165, verificándose conexión exitosa y constante logrando evitar algún tipo de caída de su servicio de venta.

Según podemos observar en la figura 51 se ingresa a la opción compra online.

Figura 51: Página oficial de la empresa Sonepar

Fuente: www.sonepar.pe

Esto direcciona automáticamente a la página de venta sonemas.pe con ip 190.119.229.165, como se observa en la figura 52.

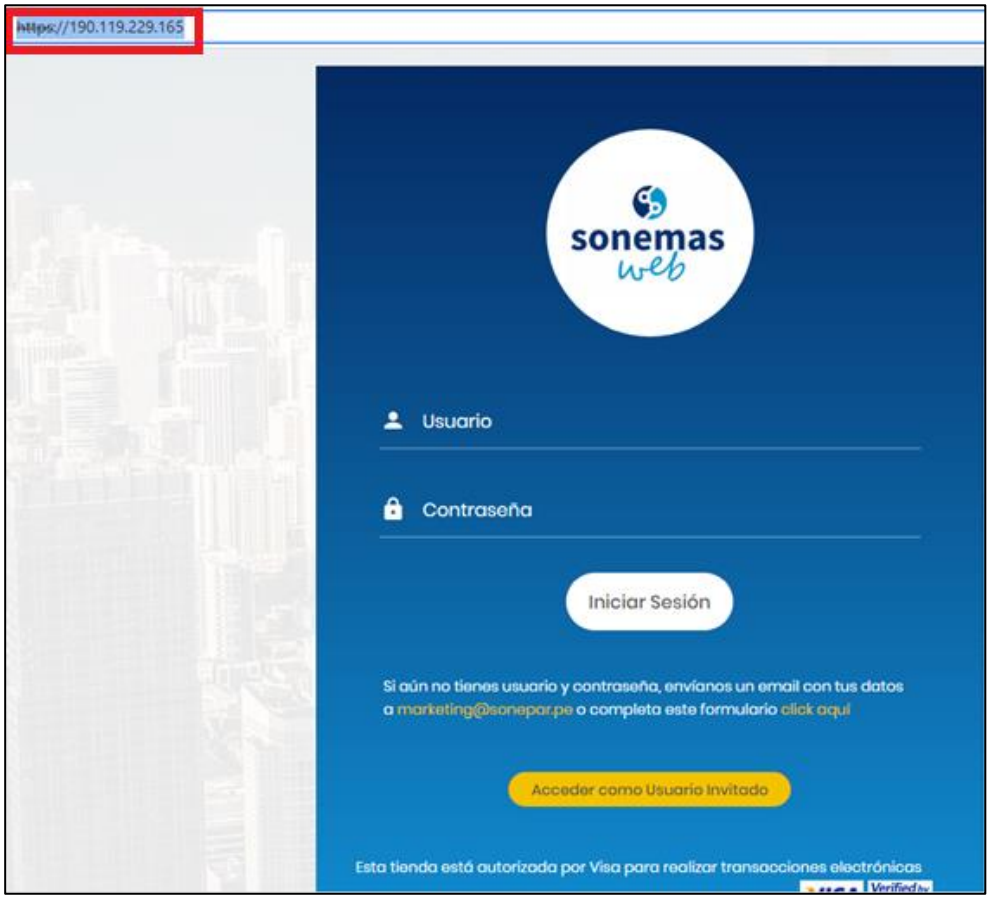


Figura 52: Página de venta online del cliente con ip 190.119.229.165

Fuente: www.sonemas.pe

Desde una red externa se valida comunicación a la dirección de la página mediante el comando ping, como se muestra en la figura 53.

```
C:\Users\COMPUSYSTEEM>ping sonemas.pe -t

Haciendo ping a sonemas.pe [190.119.229.165] con 32 bytes de datos:
Respuesta desde 190.119.229.165: bytes=32 tiempo=26ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=24ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=17ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=14ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=21ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=14ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=44ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=23ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=35ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=19ms TTL=53
Respuesta desde 190.119.229.165: bytes=32 tiempo=11ms TTL=53
```

Figura 53: Conexión desde una red externa a la página de venta sonemas.pe

Fuente: Elaboración propia

3.3.2 Seguridad perimetral

Cliente mediante este trabajo profesional ya cuenta con la seguridad de red y se comprobó:

1.- Con la protección externa que brinda el firewall fortigate 200E para los servicios que publican los servidores de la empresa. Como se puede observar en la figura 54, se tiene 12,750 registros de bloqueo de ataques.

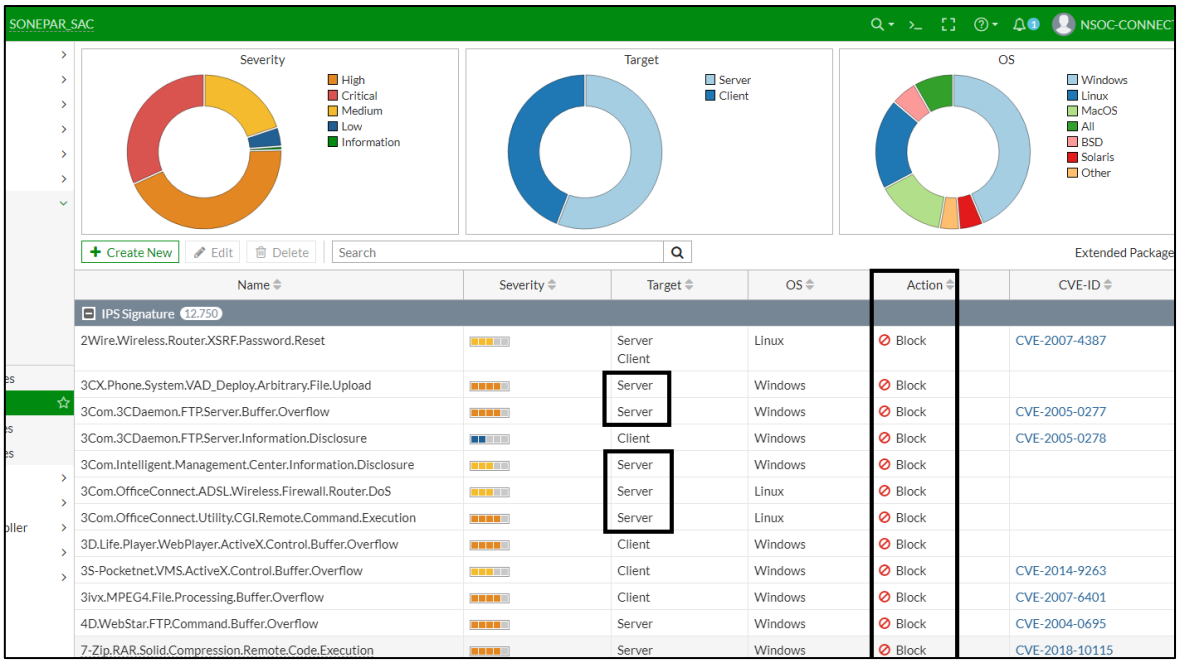


Figura 54: Ataques bloqueados por el equipo firewall fortigate 200E

Fuente: Sistema Operativo FortiOS

2.- Con el bloqueo de las ip públicas que intentan atacar a la red interna del cliente, como se muestra en la figura 55, se tiene aproximadamente 19 ip atacantes bloqueadas por el nombre del ataque.

Severity	Source	Protocol	User	Action	Count	Attack Name
	131.159.24.205	6		dropped		Linux.Kernel.TCP.SACK.Panic.DoS
	185.128.41.50	6		dropped		Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization
	45.146.164.110	6		dropped		Apache.Solr.SolrResourceLoader.Directory.Traversal
	45.146.164.110	6		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
	58.54.108.10	6		dropped		Dasan.GPON.Remote.Code.Execution
	24.193.52.67	6		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execu...
	45.146.164.110	6		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
	45.146.164.110	6		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
	45.146.164.110	6		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
	45.146.164.110	6		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
	195.154.119.181	6		dropped		Web.Server.Password.Files.Access
	86.181.4.169	6		dropped		ThinkPHP.Controller.Parameter.Remote.Code.Execution
	128.1.248.42	6		dropped		Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upl...
	128.14.134.134	6		dropped		Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upl...
	128.14.133.58	6		dropped		Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upl...
	23.251.102.74	6		dropped		Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upl...
	66.240.205.34	6		dropped		Gh0st.Rat.Botnet
	86.181.4.169	6		dropped		ThinkPHP.Controller.Parameter.Remote.Code.Execution
	128.1.248.26	6		dropped		Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upl...

Figura 55: Atacantes identificados por ip origen y el tipo de ataque que utilizan

Fuente: Sistema Operativo FortiOS

3.- Mediante la conexión segura VPN con el que ya cuentan los usuarios remotos del cliente, como se puede observar en la figura 56 hay dos usuarios conectados,

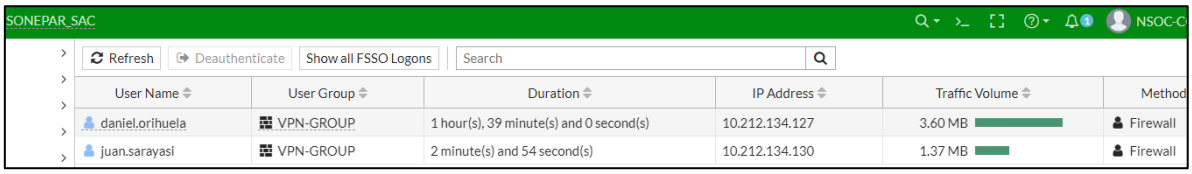
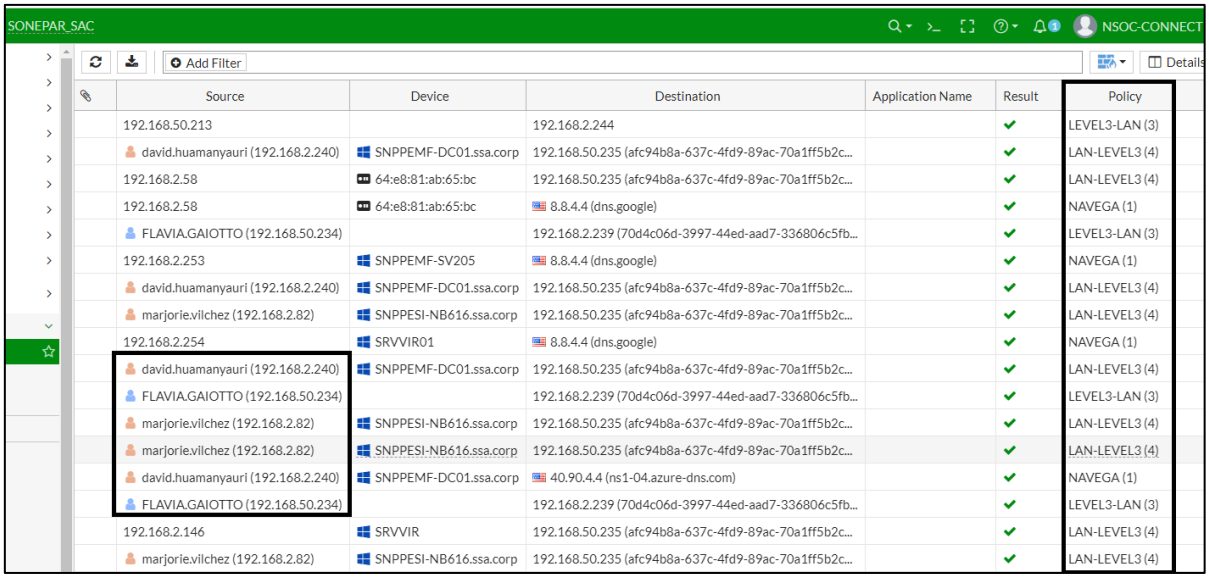


Figura 56: Conexión VPN para usuarios de la empresa Sonepar

Fuente: Sistema Operativo FortiOS

4.- Con la navegación segura a internet desde la red LAN del cliente para los usuarios de la empresa sonepar mediante las políticas creadas, como se muestra en la figura 57, usuarios están navegando por 3 políticas de seguridad:



Source	Device	Destination	Application Name	Result	Policy
192.168.50.213		192.168.2.244		✔	LEVEL3-LAN (3)
david.huamanyauri (192.168.2.240)	SNPPEMF-DC01.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
192.168.2.58	64:e8:81:ab:65:bc	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
192.168.2.58	64:e8:81:ab:65:bc	8.8.4.4 (dns.google)		✔	NAVEGA (1)
FLAVIA.GAIOTTO (192.168.50.234)		192.168.2.239 (70d4c06d-3997-44ed-aad7-336806c5fb...		✔	LEVEL3-LAN (3)
192.168.2.253	SNPPEMF-SV205	8.8.4.4 (dns.google)		✔	NAVEGA (1)
david.huamanyauri (192.168.2.240)	SNPPEMF-DC01.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
marjorie.vilchez (192.168.2.82)	SNPPESI-NB616.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
192.168.2.254	SRVVIR01	8.8.4.4 (dns.google)		✔	NAVEGA (1)
david.huamanyauri (192.168.2.240)	SNPPEMF-DC01.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
FLAVIA.GAIOTTO (192.168.50.234)		192.168.2.239 (70d4c06d-3997-44ed-aad7-336806c5fb...		✔	LEVEL3-LAN (3)
marjorie.vilchez (192.168.2.82)	SNPPESI-NB616.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
marjorie.vilchez (192.168.2.82)	SNPPESI-NB616.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
david.huamanyauri (192.168.2.240)	SNPPEMF-DC01.ssa.corp	40.90.4.4 (ns1-04.azure-dns.com)		✔	NAVEGA (1)
FLAVIA.GAIOTTO (192.168.50.234)		192.168.2.239 (70d4c06d-3997-44ed-aad7-336806c5fb...		✔	LEVEL3-LAN (3)
192.168.2.146	SRVVIR	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)
marjorie.vilchez (192.168.2.82)	SNPPESI-NB616.ssa.corp	192.168.50.235 (afc94b8a-637c-4fd9-89ac-70a1ff5b2c...		✔	LAN-LEVEL3 (4)

Figura 57: Logs de tráfico seguro de navegación de los usuarios de la empresa

Fuente: Sistema Operativo FortiOS

CONCLUSIONES:

- Se realizo la optimización del servicio de internet WAN mediante el equipo de respaldo modelo FortiWAN 200B y la seguridad perimetral con el firewall de próxima generación modelo Fortigate 200E para la sede principal de la empresa SONEPAR PERU, ubicado en Lima. Que está operando correctamente.

- Se logro la seguridad perimetral para la empresa SONEPAR como también para los usuarios de la red interna del cliente, mediante cuatro puntos principales: políticas de seguridad de navegación, conexión VPN, protección de servicios y ataques, configurados en el equipo firewall de la marca FORTINET según lo desarrollado en el punto 3.3.2 de resultados.

- El cliente cuenta con internet constante mediante el respaldo utilizando dos equipos, un enrutador de la marca CISCO con 60Mbps de ancho de banda y el equipo balanceador de enlaces de la marca FORTINET que realiza la conmutación para evitar la caída del servicio. Comprobándose mediante el acceso constante a la página de ventas del cliente según lo desarrollado en el punto 3.3.1 de resultados.

RECOMENDACIONES:

- ✓ Se recomienda utilizar esta solución ante problemas de seguridad y/o respaldo a internet en empresas o instituciones.

- ✓ Se recomienda ejecutar la actualización de las versiones 6.0 de los equipos implementados cada año para evitar vulnerabilidades de riesgo para la empresa.

- ✓ Se recomienda realizar el monitoreo constante del ancho de banda y de la latencia para la salida a internet a fin de prevenir situaciones de congestionamiento en los servicios de los usuarios.

- ✓ Se recomienda no exceder el uso de sesiones de navegación y creación de usuarios permitidos según la ficha de datos de los equipos firewall y respaldo (Véase anexo 2 y 3 respectivamente) para evitar superar la capacidad del equipo.

- ✓ Se recomienda apagar los equipos mediante la interfaz GUI o CLI para evitar averías en el hardware de los equipos implementados cuando se realice algún mantenimiento eléctrico en la empresa.

- ✓ Se recomienda al cliente solicitar la renovación de las licencias de los equipos implementados para evitar la inoperatividad de los filtros de seguridad.

REFERENCIAS BIBLIOGRAFICAS

Aguilera, P. (2011). *Seguridad Informática*. Madrid, España: Editorial Editex.

Andreu, J. (2010). *Servicios en red*. Madrid, España: Editorial Editex.

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Madrid, España: Editorial Paraninfo.

Avansis. (2021). *Seguridad Perimetral.* Recuperado de https://www.avansis.es/sin-categorizar/que-es-seguridad-perimetral/

Benchimol, D. (2010). *Redes Cisco Instalación y Administración de Hardware y Software*. (1era Ed.).Buenos Aires, Argentina. Editorial Gradi.

Berral, I. (2014). *Instalación y mantenimiento de redes para transmisión de datos.* (1era Ed.). Madrid, España: Editorial Paraninfo.

Birt. (2020). *Seguridad Administrada. Implantación de técnicas de acceso remoto.* Recuperado de https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/SAD/SAD03/es_ASIR_SAD03_Contenidos.

CISRT. (2019). *Vulnerabilidad Fortinet FortiWAN*. Recuperado de https://www.csirtasobancaria.com/alertas-de-seguridad/vulnerabilidad-fortinet-fortiwan#

Cloudflare, Inc. (2021). *What is a cloud firewall? What is firewall-as-a-service.* Recuperado de https://www.cloudflare.com/es-la/learning/cloud/what-is-a-cloud-firewall/

Fortinet. (2021). *Seguridad de red*. Recuperado de https://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-security.

Geekflare. (2020). *Diferencia entre hardware, software y firewalls en la nube.* Recuperado de https://geekflare.com/es/hardware-vs-software-cloud-firewall/

Gonzales, J. (2015). *Utilización de las bases de datos relacionales en el sistema de gestión y almacenamiento de datos*. Madrid, España. Editorial Paraninfo.

Guías Practicas. (2021). *Firewall por hardware*. Recuperado de https://www.guiaspracticas.com/seguridad-en-el-ordenador/firewall-por-hardware

Ibiblio. (2003). *Cortafuegos de filtrado de paquetes*. Recuperado de https://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node236.html

Idgrup. (s.f).Qué es un Firewall y cómo funciona. Recuperado de https://idgrup.com/firewall-que-es-y-como-funciona/

Íñigo, J., & Barceló, J. (2008). *Estructura de redes de computadores*. Barcelona, España. Editorial UOC

Iplan. (s.f).Internet content. Recuperado de https://www.iplan.com.ar/docus/conectividad/internet-y-datos/Alcance-INTERNET-CONTENT-IPLAN.pdf

Iptel. (2015). Tipos de conexiones a Internet. Recuperado de https://www.iptel.com.ar/tipos-de-conexiones-a-internet/

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/

Iso27000. (2005). *Serie27000.* Recuperado de http://www.iso27000.es/iso27000.html

Islabit. (2021). *Cortafuegos de hardware y software: estas son las diferencias*. Recuperado de https://www.islabit.com/105707/cortafuegos-de-hardware-y-software-estas-son-las-diferencias.html

KasperskyLab. (2021). *¿Qué es un firewall?* Recuperado de https://latam.kaspersky.com/resource-center/definitions/firewall

Living. (2021). *Diferencia entre firewall y servidor proxy.* Recuperado de https://es.living-in-belgium.com/difference-between-firewall-and-proxy-server-128

Marchionni, E. (2011). *Administrador de servidores*. Buenos Aires, Argentina. Editorial Gradi

Nayeli, L. (s.f). *Medios de transmisión*. Recuperado de https://es.calameo.com/books/00469385153c890c65824

PaloAltoNetworks. (2020).*¿Qué es un firewall de nube pública?* Recuperado de https://www.paloaltonetworks.lat/cyberpedia/what-is-a-public-cloud-firewall

Protección Datos. (2021). *Los 10 mejores Firewall o cortafuegos para Windows*. Recuperado de https://protecciondatos-lopd.com/empresas/mejores-firewall-windows/

Redfibra. (2021). *¿Qué es un Firewall de nueva generación?* Recuperado de https://redfibra.mx/que-es-un-firewall-de-nueva-generacion/

Rodriguez, A. (2007). *Iniciación a la red internet, concepto, funcionamiento, servicios y aplicaciones de internet*. (1era Ed.). Vigo, España. Editorial ideas propias.

Santos, M. (2014). *Sistemas telemáticos*. Madrid, España. Editorial RA-MA.

Sarubbi, J. (2008). *Técnicas de defensa comunes bajo variantes del sistema operativo Unix*. Buenos Aires, Argentina.

Severance, C. (2016). *Introducción a las redes*. Michigan, Estados Unidos. Editorial Sue Blumenberg

Sistemas. (2021). *Definición de Enlace*. Recuperado de https://sistemas.com/enlace.php

Techtarget. (2021). *Inspección de estado*. Recuperado de https://searchdatacenter.techtarget.com/es/definicion/Inspeccion-de-estado

Valdivia, C. (2015). *Redes Telemáticas*. (1era Ed.) Madrid, España. Editorial Paraninfo.

Verizon. (2021). *Fibra óptica*. Recuperado de https://espanol.verizon.com/info/definitions/fiber-optics/

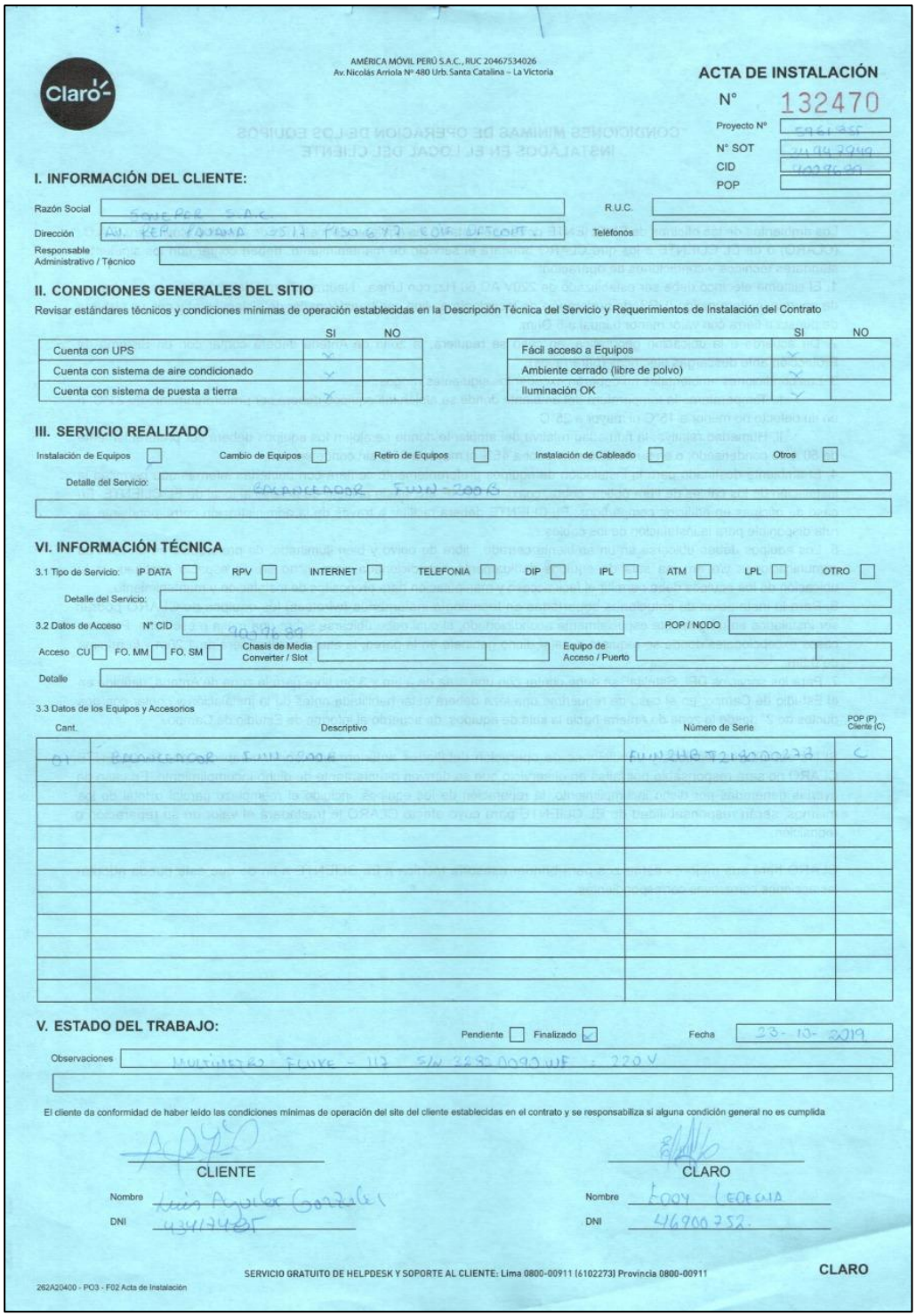
Verdú, J. (2015). *Plan de contingencia para tecnologías de la información en entornos distribuidos*. Recuperado de https://earchivo.uc3m.es/bitstream/handle/10016/22424/PFC_Jose_Ignacio_Verdu_Fernandez.pdf

Vega, E. (2021). *Seguridad de la Información*. Área de innovación y desarrollo. Universidad nacional de Costa Rica

Villa, L., & Villanueva, J. (2013*). Diseño e implementación de un isp con acceso inalámbrico para soportar servicios de internet y telefonía ip en el laboratorio de telecomunicaciones de la universidad autónoma de occidente (Proyecto de tesis)*. Universidad Autónoma de occidente, Cali, Colombia.

ANEXOS

Anexo 1. Documento de Instalación de la empresa América Móvil otorgado a nuestra empresa Dalisa S.A.C para la firma de conformidad del cliente:



AMÉRICA MÓVIL PERÚ S.A.C., RUC 20467534026
Av. Nicolás Arriola Nº 480 Urb. Santa Catalina – La Victoria

ACTA DE INSTALACIÓN

N° 132470

Proyecto N°
N° SOT
CID
POP

I. INFORMACIÓN DEL CLIENTE:

Razón Social
R.U.C.
Dirección
Teléfonos
Responsable Administrativo / Técnico

II. CONDICIONES GENERALES DEL SITIO

Revisar estándares técnicos y condiciones mínimas de operación establecidas en la Descripción Técnica del Servicio y Requerimientos de Instalación del Contrato

	SI	NO		SI	NO
Cuenta con UPS	X		Fácil acceso a Equipos	X	
Cuenta con sistema de aire condicionado	X		Ambiente cerrado (libre de polvo)	X	
Cuenta con sistema de puesta a tierra	X		Iluminación OK	X	

III. SERVICIO REALIZADO

Instalación de Equipos ☐ Cambio de Equipos ☐ Retiro de Equipos ☐ Instalación de Cableado ☐ Otros ☐

Detalle del Servicio:

VI. INFORMACIÓN TÉCNICA

3.1 Tipo de Servicio: IP DATA ☐ RPV ☐ INTERNET ☐ TELEFONIA ☐ DIP ☐ IPL ☐ ATM ☐ LPL ☐ OTRO ☐

Detalle del Servicio:

3.2 Datos de Acceso N° CID POP / NODO

Acceso CU ☐ FO. MM ☐ FO. SM ☐ Chasis de Media Converter / Slot Equipo de Acceso / Puerto

Detalle

3.3 Datos de los Equipos y Accesorios

Cant.	Descriptivo	Número de Serie	POP (P) Cliente (C)
01			C

V. ESTADO DEL TRABAJO:

Pendiente ☐ Finalizado ☑ Fecha 23-10-2019

Observaciones

El cliente da conformidad de haber leido las condiciones mínimas de operación del site del cliente establecidas en el contrato y se responsabiliza si alguna condición general no es cumplida

CLIENTE
Nombre
DNI

CLARO
Nombre
DNI

SERVICIO GRATUITO DE HELPDESK Y SOPORTE AL CLIENTE: Lima 0800-00911 (6102273) Provincia 0800-00911

CLARO

262A20400 - PO3 - F02 Acta de Instalación

Figura 58: Acta de instalación utilizada por la empresa Grupo Dalisa

Fuente: Propia

Anexo 2. Ficha de datos del equipo Perimetral fortigate 200E

SPECIFICATIONS

	FORTIGATE 200E	FORTIGATE 201E
Hardware Specifications		
GE RJ45 WAN Interfaces	2	
GE RJ45 Management/HA Ports	2	
GE RJ45 Ports	14	
GE SFP Slots	4	
USB port	1	
Console (RJ45)	1	
Local Storage	—	1× 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	2.2 Gbps	
NGFW Throughput [2, 4]	1.8 Gbps	
Threat Protection Throughput [2, 5]	1.2 Gbps	
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 9 Gbps	
Firewall Latency (64 byte UDP packets)	3 µs	
Firewall Throughput (Packets Per Second)	13.5 Mpps	
Concurrent Sessions (TCP)	2 Million	
New Sessions/Second (TCP)	135,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) [1]	7.2 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	10,000	
SSL-VPN Throughput	900 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	820 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	240,000	
Application Control Throughput (HTTP 64K) [2]	3.5 Gbps	
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel Mode)	256 / 128	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 200E	FORTIGATE 201E
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 11.9	
Height x Width x Length (mm)	44.45 × 432 × 301	
Weight	11.9 lbs (5.4 kg)	12.12 lbs (5.5 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Power Input	100–240V AC, 50–60 Hz	
Maximum Current	110 V / 3 A, 220 V / 0.42 A	
Power Consumption (Average / Maximum)	70.98 / 109.9 W	
Heat Dissipation	374.9 BTU/h	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	31.1 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6	

Figura 59: Ficha técnica de datos del equipo de seguridad Fortigate 200E

Fuente: https://www.fortinet.com/content/dam/fortinet/assets/datasheets/FortiGate_200E

Anexo 3. Ficha de datos del equipo Balanceador para respaldo de internet fortiwan 200b

	FortiWAN 200B
Hardware Specifications	
WAN Bandwidth	200–600 Mbps*
WAN Links	up to 25**
Network Interfaces	5x GE Cu
Storage	500 GB HDD
HA Ports	1
Power Supply	Single
System Specifications	
Concurrent Connections	800,000
Connections per Second	42,000
Multi-Homing A/AAAA Records	200
Management	any network port
Dimensions	
Form Factor	1U
Height x Width x Length (inches)	1.75 x 17.32 x 10.55
Height x Width x Length (mm)	44 x 440 x 268
Weight	9.9 lbs (4.5 kg)
Environment	
Input Voltage	100–240V AC, 50–60 Hz
Typical Power Consumption	40 W
Maximum Current	110V/0.37A, 220V/0.22A
Heat Dissipation	110V/138 BTU/h, 220V/163 BTU/h
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-4–167°F (-20–75°C)
Humidity	10–85% non-operating, non-condensing

Figura 60: Ficha técnica de datos del equipo de respaldo Fortiwan 200b

Fuente: www.avfirewalls.com