



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño e implementación de un Firewall Perimetral de
Nueva Generación (NGFW) para las sedes de Lima y
Parcoy de una unidad minera en el año 2023**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniera de
Telecomunicaciones

AUTOR

Stefanny María LUME CARRASCO

ASESOR

Mg. Juan Antonio APESTEGUIA INFANTES

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Lume, S. (2024). *Diseño e implementación de un Firewall Perimetral de Nueva Generación (NGFW) para las sedes de Lima y Parcoy de una unidad minera en el año 2023*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Stefanny María Lume Carrasco
Tipo de documento de identidad	DNI
Número de documento de identidad	74219976
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Juan Antonio Apesteguia Infantes
Tipo de documento de identidad	DNI
Número de documento de identidad	10423762
URL de ORCID	https://orcid.org/0000-0003-2545-0764
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Nicanor Raúl Benites Saravia
Tipo de documento	DNI
Número de documento de identidad	10189914
Miembro del jurado 1	
Nombres y apellidos	Luis Ernesto Cruzado Montañez
Tipo de documento	DNI
Número de documento de identidad	32920395
Miembro del jurado 2	
Nombres y apellidos	Manuel Francisco Bermeo Noriega
Tipo de documento	DNI
Número de documento de identidad	08437735
Datos de investigación	
Línea de investigación	C.0.3.10 Redes de datos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: San Borja Latitud: - 12.0864779 Longitud: -76.9898365
Año o rango de años en que se realizó la investigación	Febrero 2023 - mayo 2023
URL de disciplinas OCDE	Hardware, Arquitectura de Computadoras https://purl.org/pe-repo/ocde/ford#2.02.06 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN TRABAJO DE SUFICIENCIA PROFESIONAL

ACTA N°074/FIEE-CTGT/2024

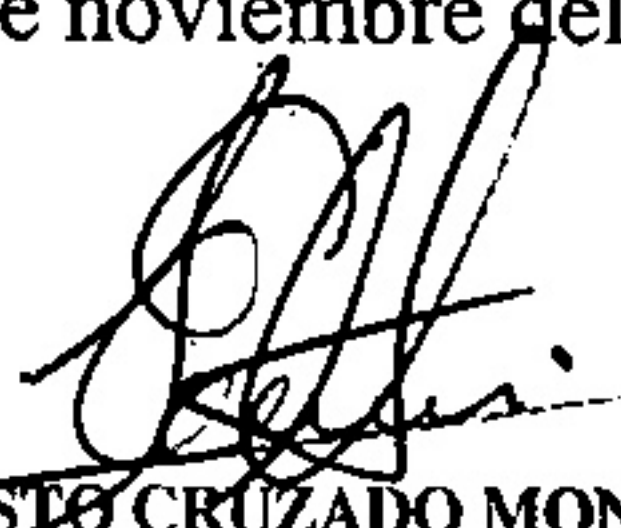
Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 26 de noviembre del 2024, como presidente de Jurado el **DR. NICANOR RAÚL BENITES SARAVIA**, integrado por el Miembro de Jurado el **MG. LUIS ERNESTO CRUZADO MONTAÑEZ**, el Miembro de Jurado **MG. MANUEL FRANCISCO BERMEO NORIEGA** y Miembro Asesor el **MG. JUAN ANTONIO APESTEGUIA INFANTES**.

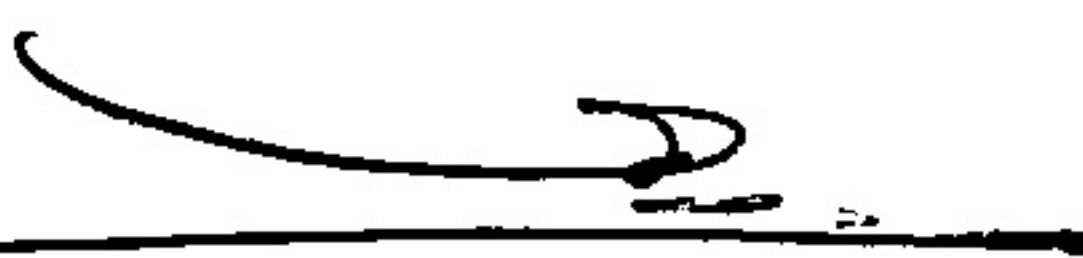
Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional de la Bachiller **STEFANNY MARÍA LUME CARRASCO** código N° 13190119 que para optar el Título Profesional de Ingeniera de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PERIMETRAL DE NUEVA GENERACIÓN (NGFW) PARA LAS SEDES DE LIMA Y PARCOY DE UNA UNIDAD MINERA EN EL AÑO 2023**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de **APROBADO... (1.6.)**.....

Ciudad Universitaria, 26 de noviembre del 2024


DR. NICANOR RAÚL BENITES SARAVIA
Presidente Jurado


MG. LUIS ERNESTO CRUZADO MONTAÑEZ
Miembro Jurado


MG. MANUEL FRANCISCO BERMEO NORIEGA
Miembro Jurado


MG. JUAN ANTONIO APESTEGUIA INFANTES
Miembro Asesor



Universidad Nacional Mayor de San Marcos

Universidad del Perú, Decana de América

Vicerrectorado de Investigación y Posgrado



CERTIFICADO DE SIMILITUD

Yo **JUAN ANTONIO APESTEGUIA INFANTES** mi condición de asesor acreditado con el Acta de Sustentación de Trabajo de Suficiencia Profesional **DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PERIMETRAL DE NUEVA GENERACIÓN (NGFW) PARA LAS SEDES DE LIMA Y PARCOY DE UNA UNIDAD MINERA EN EL AÑO 2023**, presentado por la bachiller **Stefanny María Lume Carrasco** para optar al título profesional de Ingeniera de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de **9%** de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**. Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado correspondiente.

Firma del Asesor

DNI: 10423762

Nombres y apellidos del asesor:

Mg. Juan Antonio Apesteguia Infantes

DEDICATORIA

Este trabajo está dedicado a mi madre con todo mi amor, por ser el cimiento de mi vida, por su amor, por su confianza, por su desprendimiento y su apoyo incondicional.

A mi hermana Yajaira por su amor y por su aceptación incondicional conmigo.

AGRADECIMIENTOS

A Dios por las bendiciones derramadas en mí.

A mi madre que es la gran motivación en cada paso de mi vida y por su increíble lección de superación.

A mi hermana, por motivarme y acompañarme a concretar los sueños que compartimos desde la infancia.

A mi asesor Mg. Juan Apesteguía por la orientación, por el apoyo y por la retroalimentación constructiva brindada durante el desarrollo del presente trabajo.

Agradezco a los profesores que formaron parte de mi vida académica.

A la contribución invaluable del equipo de trabajo con quienes laboré y laboro.

RESUMEN

El presente trabajo de suficiencia profesional detalla 'El diseño e Implementación de un Firewall de Nueva Generación (NGFW) para dos sedes de una Unidad Minera' en la empresa Consorcio Minero Horizonte, se enfoca como objetivo fortalecer la seguridad y proteger los activos críticos de la red dentro del Consorcio.

Asimismo, también, se explica el diseño, implementación, metodología y la gestión de un sistema de seguridad perimetral.

En efecto la implementación de un Firewall sopesa factores relevantes de la seguridad de la red como elementos: Prevención de amenazas (exploits, virus, spyware y comunicaciones de malware), comparación de firmas, prevención de pérdida de datos (DLP), filtrado de URL, identificación de usuarios (USER-ID), identificación de aplicaciones (APP-ID), identificación de dispositivos (DEVICE-ID), entre otros, donde se explica la configuración y funcionamiento de cada uno reduce los incidentes de seguridad en la red, mejora en el tiempo de respuesta a amenazas, fortalece la capacidad de la red para resistir ataques, garantiza que solo los usuarios autorizados tengan acceso a la información sensible. Se aplicó las buenas prácticas y recomendaciones sugeridas.

Palabras Clave: Firewall de Nueva Generación (NGFW), seguridad de la red, buenas prácticas, amenazas, URL.

ABSTRACT

The present work of professional sufficiency details 'The design and implementation of a Next Generation Firewall (NGFW) for two headquarters of a Mining Unit' in the company Consorcio Minero Horizonte, focuses on strengthening security and protecting critical assets of the network within the Consortium.

It also explains the design, implementation, methodology and management of a perimeter security system.

In fact, the implementation of a Firewall weighs relevant factors of the network security as elements: Threat prevention (exploits, viruses, spyware and malware communications), signature matching, data loss prevention (DLP), URL filtering, user identification (USER-ID), application identification (APP-ID), device identification (DEVICE-ID), among others, where the configuration and operation of each one is explained reduces network security incidents, improves response time to threats, strengthens the network's ability to resist attacks, ensures that only authorized users have access to sensitive information. The suggested best practices and recommendations were applied.

Keywords: Next Generation Firewall (NGFW), network security, best practices, threats, URL.

TABLA DE CONTENIDO

RESUMEN	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	x
CAPÍTULO I: INTRODUCCIÓN	1
CAPÍTULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
2.1 Institución - Actividad que desarrolla	3
2.2 Periodo de duración de la Actividad	4
2.3 Finalidad y Objetivo de la Entidad	4
2.4 Razón Social	5
2.5 Dirección Postal	5
2.6 Correo Electrónico del Profesional a Cargo	5
CAPÍTULO III: DESCRIPCIÓN DE LA ACTIVIDAD	6
3.1 Organización de la Actividad	6
3.2 Finalidad y Objetivo de la Actividad	6
3.2.1 Finalidad	6
3.2.2 Objetivos	7
3.3 Problemática	7
3.3.1 Problema General	7

3.3.2 Problemas Específicos	8
3.3.3 Justificación e Importancia de la investigación	8
3.4 Metodología	9
3.4.1 Bases Teóricas	9
3.4.2 Marco Conceptual	12
A) Definiciones de red	12
B) Firewall de Nueva Generación	14
C) Arquitectura de Firewall de Nueva Generación	14
D) Principios fundamentales de Seguridad	18
3.5 Procedimientos	18
3.5.1 Recolección de información	18
3.5.2 Configuración del Firewall	21
3.5.3 Diseño de la red	28
3.6 Resultado de la Actividad	30
CAPITULO IV: DISCUSIÓN DE RESULTADOS	34
4.1 Descripción de la Implementación	34
4.2 Presentación de Resultados y Evaluación económica	35
4.2.1 Seguridad	35
4.2.2 Evaluación Económica	37
CAPÍTULO V: CONCLUSIONES	38
CAPÍTULO VI: RECOMENDACIONES	39
CAPÍTULO VII: BIBLIOGRAFÍA	40
CAPÍTULO VIII: ANEXOS	42

LISTA DE FIGURAS

Figura 1 Ubicación geográfica de la sede en Parcoy	3
Figura 2 Ubicación geográfica de la sede en Lima	4
Figura 3 Arquitectura de procesamiento paralelo de paso único del Firewall Palo Alto	14
Figura 4 Procesos clave de la arquitectura de un solo paso NGFW Palo Alto	16
Figura 5 Arquitectura de Hardware del Firewall Palo Alto	17
Figura 6 Registro de amenazas bloqueadas provenientes de Internet por el Firewall Anterior Sede Parcoy	19
Figura 7 Registro de amenazas bloqueadas por el Firewall Anterior Sede Parcoy	20
Figura 8 Registro de amenazas bloqueadas provenientes de Internet por el Firewall Anterior Sede Lima	20
Figura 9 Firewall Palo Alto modelo PA-450	21
Figura 10 Dashboard del Firewall	21
Figura 11 Configuración de Rutas de servicios	22
Figura 12 Configuración de administración del Firewall	23
Figura 13 Configuraciones Generales del Firewall	23
Figura 14 Configuración de complejidad de credenciales	24
Figura 15 Actualizaciones dinámicas	24
Figura 16 Configuración de AD	25
Figura 17 Perfil de Seguridad	25
Figura 18 Política de Seguridad de Protección DoS	26
Figura 19 Perfil Calidad y Servicio (QoS)	26
Figura 20 Políticas de Seguridad	27
Figura 21 Políticas Nat	27
Figura 22 Configuración de Alta Disponibilidad	28

Figura 23 Topología referencial Sede Parcoy	29
Figura 24 Topología referencial Sede Lima	29
Figura 25 Logs de registros	30
Figura 26 Mapa de tráfico	31
Figura 27 Registro de amenazas bloqueadas hacia la Wan Sede Parcoy	31
Figura 28 Registro de amenazas bloqueadas en la red de Parcoy	32
Figura 29 Registro de amenazas bloqueadas hacia la Wan Sede Lima	32
Figura 30 Actividad de aplicación bloqueada	33
Figura 31 Log de Alta Disponibilidad	33
Figura 32 Procesos de un enfoque de múltiples pasos	34
Figura 33 Cuadrante mágico para Firewalls	35

LISTA DE TABLAS

Tabla 1

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto sede Lima conexión hacia Internet.

Tabla 2

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto sede Parcoy conexión hacia Internet. 36

Tabla 3

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto en toda la red sede Parcoy. 37

Tabla 4

Costo de implementación de NGFW Palo Alto Networks. 37

CAPÍTULO I: INTRODUCCIÓN

Actualmente, las entidades buscan ser más competitivas con el objetivo de proporcionar un servicio de calidad que satisfaga las necesidades de sus usuarios y reduzca los desplazamientos no necesarios. Para lograrlo, están constantemente explorando nuevas herramientas tecnológicas que les permitan mejorar la comunicación y ofrecer servicios más eficientes. No obstante, es primordial no pasar por alto los riesgos asociados con la falta de controles y medidas para garantizar el correcto funcionamiento de los procesos. Estas medidas no solo preservan la eficiencia, sino que también evitan pérdidas financieras y protegen la reputación de la empresa, al mismo tiempo que reducen los plazos establecidos de los proyectos (Chicaiza, 2017, p. 13).

El objetivo del presente trabajo es mejorar y fortalecer la seguridad de la red para dos sedes de la Entidad y asegurar la disponibilidad de los activos críticos, a través del diseño e implementación de un Firewall de Nueva Generación. El cual presenta las características de: prevención y detección de intrusos, antivirus, análisis de archivos, filtrado de URL, identificación de usuarios, identificación de aplicaciones y dispositivos.

En el capítulo II, se expone la información acerca del lugar donde se desarrolló, la duración del trabajo en las sedes de la entidad, por otro lado, también se detalla el personal encargado.

En el capítulo III, se presentan los datos de la Organización donde se desarrolla el proyecto, se perfila la finalidad, objetivos y problemática, metodología apoyada en trabajos internacionales como nacionales. Sumado a la revisión de los principios fundamentales de la seguridad, la arquitectura y funcionalidad del Firewall de Nueva Generación que incluyen la prevención y

detección intrusos, el uso de antivirus, el análisis de archivos, el filtrado URLs y la identificación de usuarios, aplicaciones y dispositivos. Así también la configuración de la alta disponibilidad del Firewall.

En el capítulo IV, se muestra la discusión de los resultados donde se explica la justificación económica y técnica. En el capítulo V, las conclusiones.

Por último, se presentarán las recomendaciones aplicadas en los siguientes capítulos, donde se evidencia la seguridad presente en las sedes de la entidad y los anexos.

CAPÍTULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución - Actividad que desarrolla

La compañía en la cual se desarrolló el Trabajo de Suficiencia Profesional es Consorcio Minero Horizonte para dos de sus sedes que son Lima y Parcoy, las actividades fueron realizadas por la empresa Imperia Soluciones Tecnológicas S.A.C.

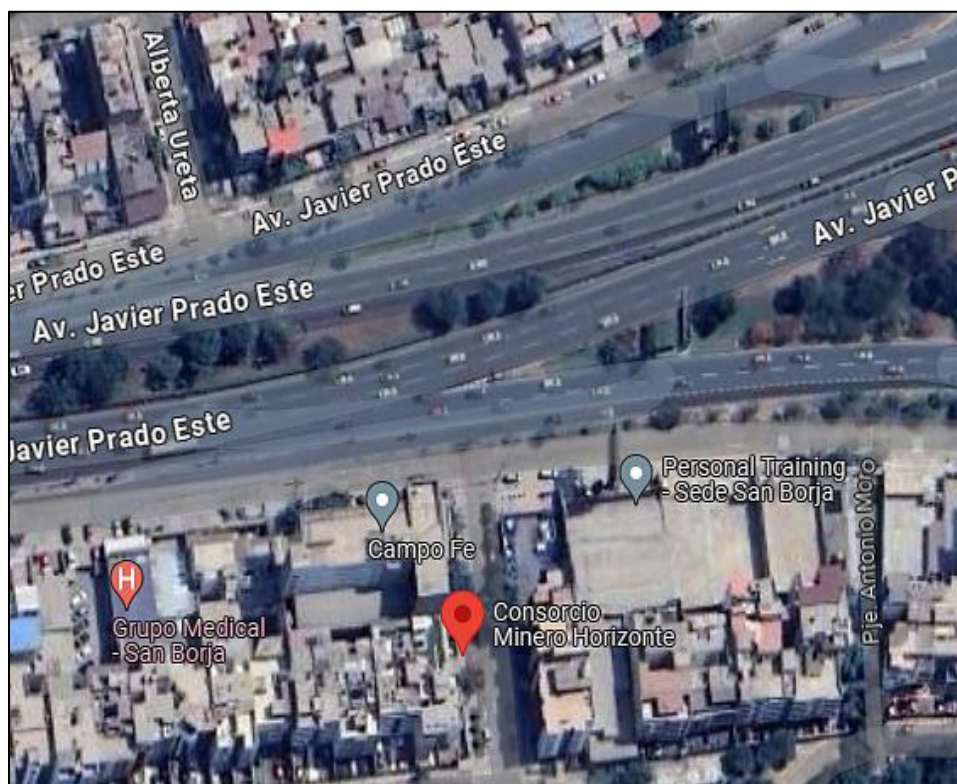
Figura 1

Ubicación geográfica de la sede en Parcoy.



Nota: El gráfico muestra la ubicación geográfica de la sede Parcoy. Tomado de Google Maps.

Figura 2
Ubicación geográfica de la sede en Lima



Nota: El gráfico muestra la ubicación geográfica de la sede Lima. Tomado de Google Maps.

2.2 Periodo de duración de la Actividad

El desarrollo de elaboración del presente trabajo se llevó a cabo entre los meses de febrero del año 2023 a mayo del 2023.

2.3 Finalidad y Objetivo de la Entidad

Imperia Soluciones Tecnológicas S.A.C es una compañía peruana con amplia experiencia en tecnología de la información y ciberseguridad.

Se compromete a brindar soluciones tecnológicas de vanguardia que optimizan y garantizan la confiabilidad de los procesos de negocio. Asegurando mayor productividad, alta calidad en sus servicios y crecimiento.

El compromiso de la empresa con la excelencia y la plena satisfacción del cliente los motiva a convertirse en un aliado de confianza en el camino hacia el éxito digital. a proveer los recursos necesarios para la implementación, control y mejoramiento de la Gestión de la Calidad.

2.4 Razón Social

Imperia Soluciones Tecnológicas S.A.C.

2.5 Dirección Postal

Av. José Pardo 434, Oficina 401, Miraflores, Lima.

2.6 Correo Electrónico del Profesional a Cargo

Nombres y Apellidos: Antonio Pereda Bardales

Correo: antonio.pereda@imperia.com.pe

CAPÍTULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la Actividad

Se llevaron a cabo las actividades con un enfoque progresivo para su aplicación en tres fases, las cuales se ejecutaron desde febrero de 2023 hasta mayo del mismo año.

En la Fase inicial, se enfocó en la recolección de información, la cual incluyó: la identificación de los equipos, la topología de red existente, las políticas configuradas y los antecedentes de vulneraciones. Esta recolección se llevó a cabo mediante Kickoff, correos y sesiones en conjunto con el cliente.

En la Segunda Fase, se procedió a modificar la topología de red y mejorar la configuración basándonos en recomendaciones proporcionadas por el fabricante del firewall, con el objetivo de mitigar las amenazas hacia la red.

Finalmente, en la última fase, se realizaron ajustes en la configuración a través del monitoreo y se corroboraron los resultados de eficiencia en la seguridad.

3.2 Finalidad y Objetivo de la Actividad

3.2.1 Finalidad

En el vigente documento de suficiencia profesional se propone la implementación de Firewall de Nueva Generación para mejorar y fortalecer la seguridad de la red para dos sedes de la Unidad Minera.

3.2.2 Objetivos

3.2.2.1 Objetivo General

Implementar un Firewall de Nueva generación (NGFW) en dos sedes de una Unidad Minera en el año 2023 para fortalecer la seguridad de la red y proteger los activos críticos de la empresa.

3.2.2.2 Objetivos Específicos

- Reducir incidentes de seguridad para fortalecer la capacidad de la red frente a los ataques mediante el cumplimiento de las normativas de seguridad de datos y la garantía de que solo usuarios autorizados tengan acceso a la información crítica.
- Implementar la alta disponibilidad en el dispositivo de seguridad que administra la red en caso de falla e interrupciones para asegurar el funcionamiento de los servicios críticos.
- Validar el rendimiento obtenido posterior a la implementación del Firewall de Nueva Generación en la red y corregir posibles fallos.

3.3 Problemática

3.3.1 Problema General

¿Cómo mejorar la seguridad de la red para dos sedes de una unidad minera mediante el diseño e implementación de un Firewall Perimetral de Nueva Generación (NGFW) en el año 2023?

3.3.2 Problemas Específicos

- ¿Cómo la identificación de amenazas en la red podría evitar la explotación de éstas y cómo detectar la presencia de tráfico no autorizado?
- ¿Qué consideraciones se debe realizar para asegurar la disponibilidad del dispositivo de seguridad que administra la red en caso de fallas y/o interrupciones?
- ¿En qué medida evaluar los resultados de la implementación de un NGFW en la red?

3.3.3 Justificación e Importancia de la investigación

El presente trabajo justifica la implementación de un firewall de nueva generación en dos sedes de la entidad para garantizar la seguridad y la resiliencia. Este firewall ofrecerá una mejor inspección del tráfico de red, garantizará mayor visibilidad de las actividades de la red, control granular de aplicaciones y políticas y un enfoque de seguridad avanzada diseñado para hacer frente a amenazas cibernéticas lo que ayudará a proteger los activos y la información confidencial de la entidad contra posibles amenazas de manera más efectiva.

A) Justificación Teórica: La propuesta se centra en abordar la importancia de la seguridad de la información en el contexto de las amenazas cibernéticas, como el malware, los ataques de denegación de servicio y la inyección de código, entre otros. La implementación de un firewall se presenta como una medida fundamental para proteger los activos críticos y ayudará a cumplir con las normativas de seguridad de la información; reduciendo el riesgo de multas, sanciones legales y como una barrera defensiva entre la red interna y la red exterior, filtrando el tráfico de red entrante y saliente según reglas predefinidas.

B) Justificación Práctica: La propuesta se centra en la necesidad de cómo implementar un firewall puede mejorar la productividad de los empleados al filtrar el acceso a sitios web y prevenir descarga de archivos maliciosos, como garantizar que los recursos de la red se utilicen con más eficiencia eliminando tráfico no deseado optimizando el ancho de banda disponible donde la velocidad y confidencialidad de la red es crítica en las operaciones del día a día, cómo ayuda a cumplir las normativas de seguridad. Brinda herramientas para monitoreo y control del tráfico de la red. La implementación de un firewall ayuda con los costos asociados a prevención de incidentes de seguridad.

C) Justificación Metodológica: La propuesta de instalación de firewall de nueva generación propone seguir una serie de pasos para diseñar e implementar de un firewall en la red para la prevención de amenazas de la red y protección de los activos críticos.

3.4 Metodología

3.4.1 Bases Teóricas

3.4.1.1 Internacional

Alvarez y Caruzo (2015), en su trabajo de grado titulado Diseño e Implementación de un Sistema de seguridad utilizando el Firewall IPCop para el control del acceso a internet y a la red de datos de la Universidad de Córdoba, tiene como objetivo implementar un sistema de seguridad utilizando el firewall IPCop para controlar el acceso hacia Internet y a la red de la Universidad de Córdoba (p. 12).

Los autores concluyeron y resaltaron la importancia de un enfoque integral sobre la seguridad de la red que incluya responsabilidad, control, conocimientos de los recursos, políticas adaptadas a la

organización a su misión y visión de negocio, más allá de la concentración propia del firewall. También concluyó que IPCop es la mejor opción para garantizar seguridad y flexibilidad en instalaciones SOHO y se adapta adecuadamente a las instalaciones medianas o pequeñas.

Ardila (2013), elaboró un proyecto de grado titulado Diseño e implementación de un firewall para redes basadas en el protocolo modbus TCP por medio de NetFPGA con el objetivo de diseñar e implementar un firewall basado en el sistema NetFPGA para redes industriales que se fundamente en tecnología de modbus TCP (p. 16). El autor concluye que es primordial establecer políticas de seguridad que reduzcan riesgos potenciales conocidos y futuros, menciona cómo un mal manejo de la seguridad puede afectar a las personas, destaca la importancia del uso de la tarjeta NetFPGA en la elaboración de un firewall el cual fortaleció la seguridad de la red mediante el impedimento de programas no deseados. Así como también el uso de Linux Backtrack para el análisis e identificación de problemas en la red resulta muy útil sin embargo éste debe poseer niveles de seguridad correctos.

Chicaiza (2017), elaboró un proyecto de grado titulado Implementación de un firewall construido a partir de software y una placa de circuitos compacta o SBC (single board computer) en la empresa Taio Systems de la ciudad de Popayán, con el objetivo de mejorar la seguridad perimetral de la empresa Taio Systems mediante un equipo de seguridad de costo reducido basado en software libre y circuitos, siguiendo los lineamientos de la entidad (p. 18).

El autor concluyó que, al establecer objetivos definidos, recopilar información y realizar un estudio adecuado, logró diseñar e implementar eficazmente un firewall de seguridad perimetral originado a partir de una placa SBC y software libre. Este dispositivo posibilitó la configuración de políticas de seguridad de acuerdo a los lineamientos de la empresa, adecuó los controles de los datos de la red, mejoró la latencia y demostró hacer frente a ataques probados durante sus

pruebas logrando el mejoramiento de la seguridad perimetral de la entidad.

Pascuas et al. (2015), elaboraron un trabajo de grado titulado Implementación de dispositivo firewall con reglas de tráfico en la clínica Medilaser S.A. sede Neiva, con el objetivo de implementar un dispositivo de protección de amenazas tipo Firewall para el control de políticas de seguridad mediante la configuración de reglas (p. 12).

Los autores concluyeron que, la implementación del Firewall UTM resultó exitosa porque fortalece la infraestructura de la seguridad de la clínica mediante una protección integral y garantiza la continuidad operativa de sus sistemas. Facilita al administrador la gestión de la red de forma que no se tenga complicaciones y mantenga la protección.

3.4.1.2 Nacional

Caballa y Torres (2010), elaboraron una tesina titulada Implementación de una solución de seguridad informática bajo la plataforma de gestión unificada de amenazas, con el objetivo de demostrar a través de un caso práctico que los equipos UTM simplificarán y mejorarán la administración de la seguridad informática (p. 7).

Los autores concluyeron que la opción elegida se fundamentó en la protección de la red en los diferentes niveles: Firewall, Antivirus, IDS/IPS, Antispam y Web Filtering, administración centralizada de la gestión de la seguridad de la red, el control del tráfico según la relevancia de aplicaciones mediante traffic shaping. Por lo cual se implementó firewalls en alta disponibilidad que ayudó en la conmutación del tráfico en caso de desperfectos y también satisfizo los aspectos económicos deseados.

Pitancur (2019), elaboró una tesina titulada Diseño e Implementación de una Red de datos y seguridad perimetral de la empresa Corporación Cayman S.A.C y señala como objetivo diseñar una red de datos para

la empresa Corporación Cayman en la seguridad perimetral del mismo (p. 10).

El autor concluyó que el firewall implementado ayudó a fortalecer la seguridad al centralizar la red, proporcionar acceso controlado de usuarios locales y remotos, otorgó protección a servicios internos, optimizó la navegación hacia internet y brindó seguridad en la zona DMZ donde se encuentran los servidores accesibles desde el exterior.

Montes e Iturrigaza (2015), elaboraron una tesis titulada Diseño de arquitectura de seguridad perimetral para una empresa dedicada a la actividad inmobiliaria, tiene como objetivo desarrollar una arquitectura robusta que brinde seguridad garantizando la confiabilidad de la información de la entidad (p. 6).

Los autores llegaron a la conclusión cómo el diseño e implementación de un equipo de seguridad actualizado permite proteger eficazmente la red de la empresa. Para asegurar la efectividad de las configuraciones y funcionalidades del equipo de seguridad, llevaron a cabo pruebas exhaustivas. Estas pruebas fueron fundamentales para validar el desempeño y la adecuación del sistema antes de su implementación definitiva en la red del cliente. Las validaciones garantizaron que las medidas de seguridad estuvieran correctamente configuradas y operativas, proporcionando así una protección robusta y confiable contra posibles amenazas cibernéticas en el contexto de la empresa Inmobiliaria.

3.4.2 Marco Conceptual

A) Definiciones de red

a) LAN

Son redes de área local que se limitan a la conexión de dispositivos dentro de un área física.

- b) WAN
Es una red de área extensa, que transmite datos a través de grandes extensiones geográficas. Se utilizan en redes públicas como en redes privadas.
- c) DMZ
Actúa como una capa adicional de seguridad entre la red interna y el mundo exterior, se utiliza para separar una red interna local de redes externas no confiables, ya sea subred física o lógica.
- d) DNS
Es una base de datos que contiene información para la traducción de los nombres de dominio en identificadores de red para facilitar el acceso a los usuarios.
- e) GATEWAY
Es una puerta de enlace asociado a un dispositivo de red que permite la interconexión de los dispositivos en la red.
- f) ISP
Es un proveedor de servicios de Internet que brinda conexión a Internet.
- g) EDL
Facilita el uso de listas de identificadores de red, dominios o vínculo web de manera dinámica. Se refrescan a partir con información de datos recientes de amenazas.
- h) SANDOXING
Identifica y evalúa el comportamiento del malware de modo regulado y confiable, está cimentado en un entorno virtual.
- i) SUPERFICIE DE ATAQUE
Son vías de acceso susceptibles a la posibilidad de ser aprovechados por los atacantes.

B) Firewall de Nueva Generación

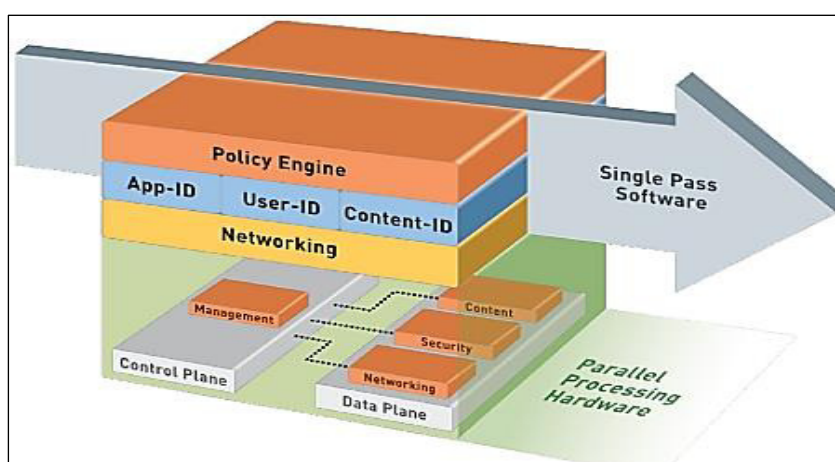
Es el motor de la Seguridad de Next-Generation Firewall, está diseñado desde su arranque para afrontar las amenazas más sofisticadas. Examina rigurosamente el tráfico, incluyendo el de aplicaciones, amenazas y contenido, y lo asocia con el usuario, independientemente de su ubicación o del dispositivo utilizado. Las aplicaciones, contenido y usuarios se convierten en elementos esenciales de la política de seguridad. Se acorta significativamente el periodo que transcurre desde que se produce un incidente hasta la resolución, identifica amenazas no conocidas y mejora la eficiencia en la seguridad de la red (Palo Alto Networks, 2016).

C) Arquitectura de Firewall de Nueva Generación

Los Next-Generation Firewall de Palo Alto se basan en una arquitectura única de procesamiento paralelo de paso único (SP3), que permite una seguridad de red de alto rendimiento y baja latencia, incluso incorporando nuevas características (Paloguard, s.f.).

Figura 3

Arquitectura de procesamiento paralelo de paso único del Firewall Palo Alto.



Nota: El gráfico muestra la arquitectura de procesamiento. Tomado de la página web firewall.cx.

Esta arquitectura combina dos componentes complementarios:

- **Software de paso único**

El software Palo Alto Networks Single Pass cumple dos funciones clave dentro del firewall de nueva generación.

Primero, el software de paso único realiza operaciones una vez por paquete. A medida que se procesa un paquete, las funciones de red, las tareas de análisis de políticas, la identificación y decodificación de aplicaciones como la validación de firmas para las amenazas y contenido se efectúan una sola vez.

En segundo lugar, el paso de escaneo de contenido en el software Single Pass de Palo Alto Networks se basa en transmisiones y utiliza una coincidencia de firmas uniforme para detectar y bloquear amenazas.

Este procesamiento de tráfico de paso único permite un rendimiento muy alto y una latencia baja, con todas las funciones de seguridad activas. También ofrece el beneficio adicional de una política única y totalmente integrada, que permite una gestión sencilla (Paloguard, s.f.).

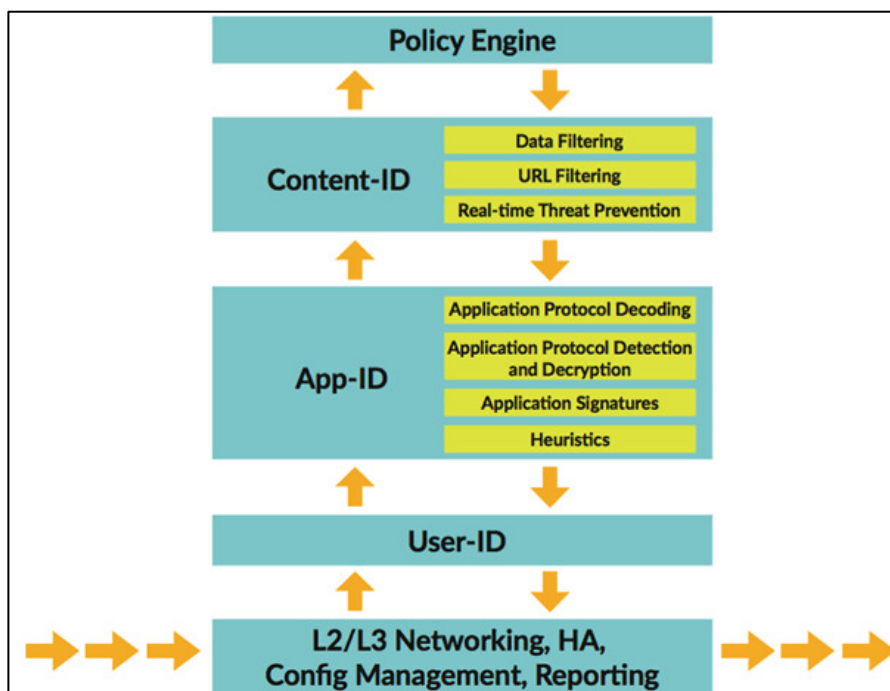
Según Palo Alto Networks (2021), las funciones de procesamiento del firewall de nueva generación son las siguientes:

- ❖ Las funcionalidades de red y de gestión en el núcleo de todo el procesamiento del tráfico forman una base de red común con una estructura de gestión común.
- ❖ La tecnología User-ID asigna direcciones IP a usuarios (por ejemplo, Active Directory) y usuarios a grupos (roles) para permitir la visibilidad y la aplicación de políticas por usuario y por grupo.
- ❖ La tecnología Device-ID asigna direcciones IP a dispositivos específicos para permitir la visibilidad y las políticas basadas en la identidad del dispositivo.
- ❖ La tecnología App-ID identifica las aplicaciones con una combinación de firmas de aplicaciones, detección y descifrado de protocolos, decodificación de protocolos y heurística. Esto se traslada a Content-ID para analizar e inspeccionar las aplicaciones adecuadas a su uso, así como al motor de políticas y otros servicios.

- ❖ La tecnología Content-ID utiliza un formato de firma uniforme para analizar el tráfico en busca de amenazas (exploits, virus, spyware y comunicaciones de malware) y patrones de datos confidenciales (por ejemplo, números de seguro social y de tarjetas de crédito, patrones personalizados). Además de un motor de comparación de firmas, el plano de datos del firewall aplica machine learning sobre scripts PowerShell, archivos ejecutables portátiles (PE), JavaScript y archivos de formato ejecutable y enlazado (ELF) en tiempo real para prevenir los ataques basados en archivos y en la Web.
- ❖ El motor de políticas permite la inspección de amenazas y la decisión de aplicar el reenvío o no en una sola política. Una sola política puede contener User-ID, Device-ID, App-ID, Threat Prevention, URL filtering, análisis de malware, data loss prevention (prevención de pérdida de datos - DLP), etc.

Figura 4

Procesos clave de la arquitectura de un solo paso NGFW Palo Alto.



Nota: El gráfico muestra los procesos claves de un Firewall Nex Generation. Tomado de la página web firewall.cx.

- **Hardware de procesamiento paralelo**

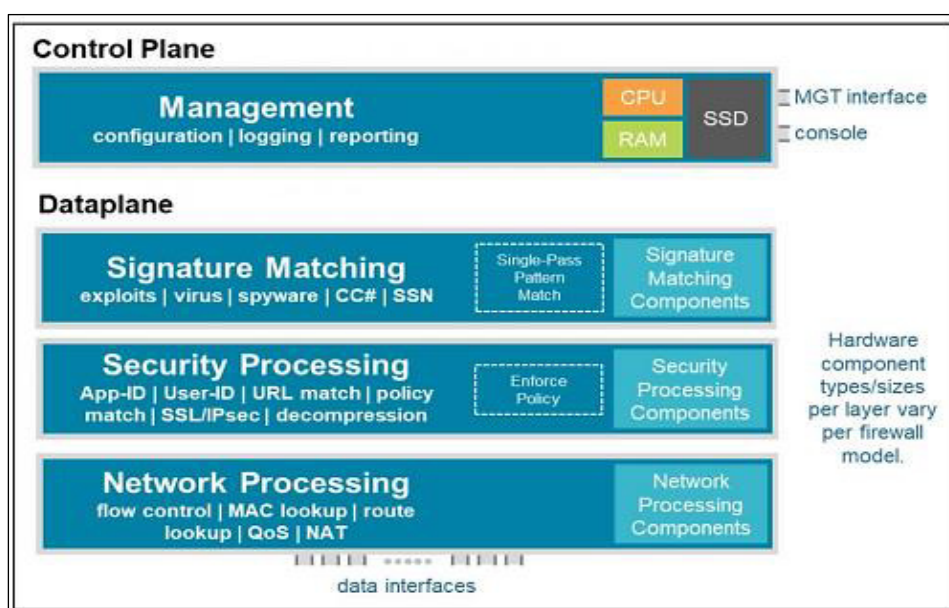
Los Next-Generation Firewall de Palo Alto utilizan hardware de procesamiento paralelo para garantizar que el software Single Pass se ejecute rápidamente.

Primero, los ingenieros de Palo Alto Networks diseñaron planos de control y datos separados. Esta separación significa que el uso intensivo de uno no afectará negativamente al otro.

El segundo elemento importante del hardware de procesamiento paralelo es el uso de grupos de procesamiento discretos y especializados que trabajan en armonía para realizar varias funciones críticas como: Redes, Id de usuario, análisis de contenido, en el plano de control, un procesador de gestión dedicado (con disco y RAM dedicados) gestiona la gestión de la configuración, el registro y la generación de informes sin tocar el hardware de procesamiento de datos (Paloguard, s.f.).

Figura 5

Arquitectura de Hardware del Firewall Palo Alto.



Nota: El gráfico muestra la arquitectura de hardware. Tomado de *la página web firewall.cx*.

D) Principios fundamentales de Seguridad

- **Confidencialidad**

Caballa y Torres (2010) menciona que la Confidencialidad, garantiza que el grado necesario de discreción se halla protegido en todas las etapas del procesamiento de información, con el fin de evitar su difusión a personas indebidas a tener conocimiento de ello. En otras palabras, la Confidencialidad de la Información se refiere a la obligación de restringir el acceso solamente al personal permitido. (pp. 11-12).

- **Integridad**

Caballa y Torres (2010) describe que la Integridad de la Información es la característica que hace posible garantizar su exactitud y confiabilidad, velando por que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, de modo autorizado y mediante procesos autorizados. A su vez, es de suma importancia que esta modificación sea registrada para posteriores controles o auditorias (pp. 12-13).

- **Disponibilidad**

Según Caballa y Torres (2010), la disponibilidad u operatividad de la Información es la capacidad de encontrarse siempre disponible, para ser utilizada por las personas autorizadas. A fin de cumplir con este principio, los sistemas y redes deben proveer la capacidad adecuada de procesamiento, actuar de modo previsible y brindar un adecuado nivel de performance. A su vez, ellos deberían ser capaces de recuperarse de interrupciones de manera rápida y segura, a fin de que la productividad no se vea afectada negativamente (p. 13).

3.5 Procedimientos

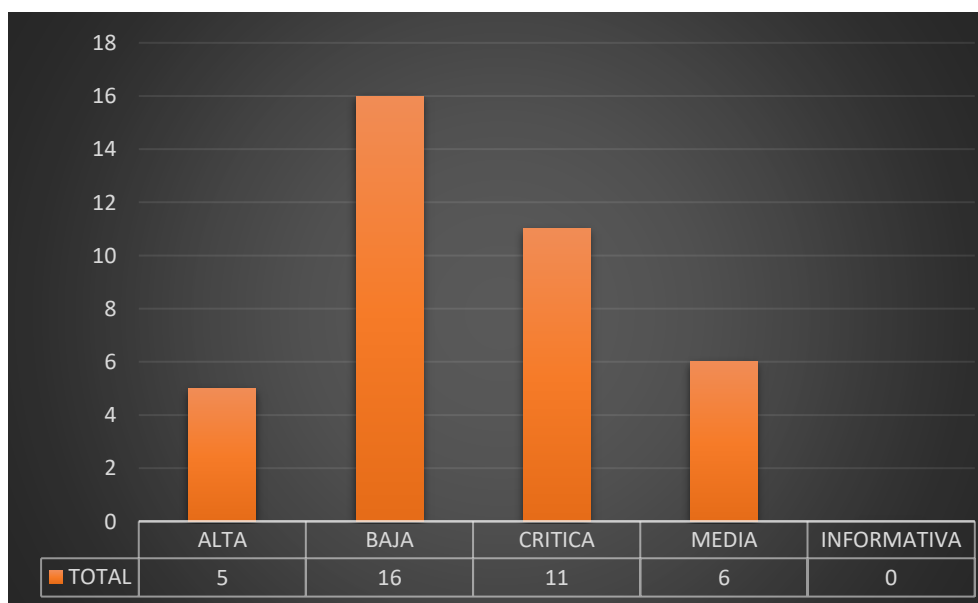
3.5.1 Recolección de información

En esta etapa se genera un plan de trabajo, para la elaboración de éste se necesita analizar la infraestructura de red existente, identificar las necesidades de control, de seguridad y se evalúa los riesgos potenciales, para ellos se seguirá los siguientes pasos:

- Identificación de equipos que conforman la red.
- Conocer la conectividad de los equipos que se interconectan con la red y direcciones IP's.
- Criticidad de los servicios y puertos expuestos a la red externa.
- Autenticación y control de usuarios a los activos internos y externos.
- Espacio donde se encuentra alojado los servicios.
- Antecedentes de vulneraciones anteriores, como se aprecia en los siguientes gráficos:

Figura 6

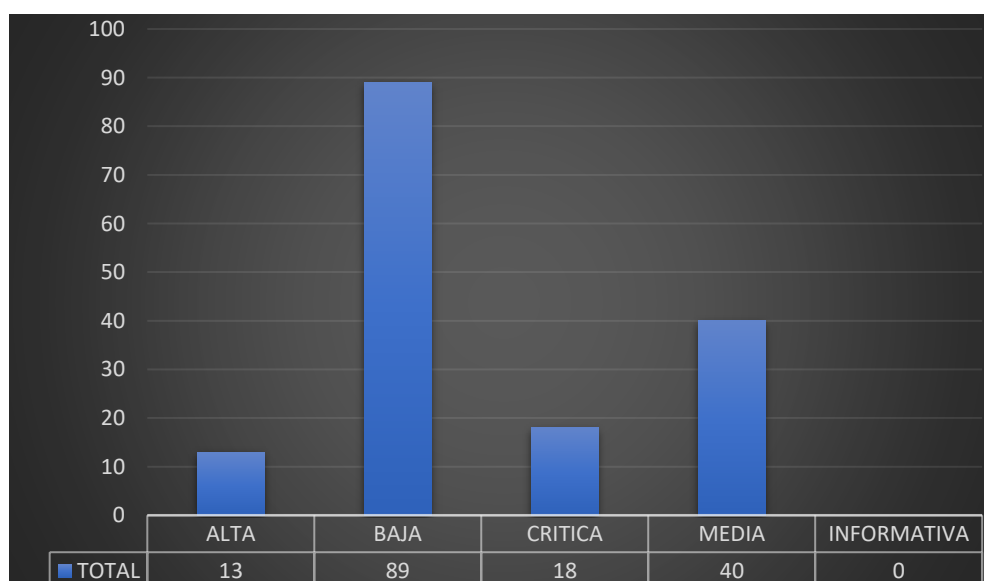
Registro de amenazas bloqueadas provenientes de Internet por el Firewall Anterior Sede Parcoy.



Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad del tráfico proveniente de Internet que han sido bloqueadas por el Firewall Anterior en la sede Parcoy.

Figura 7

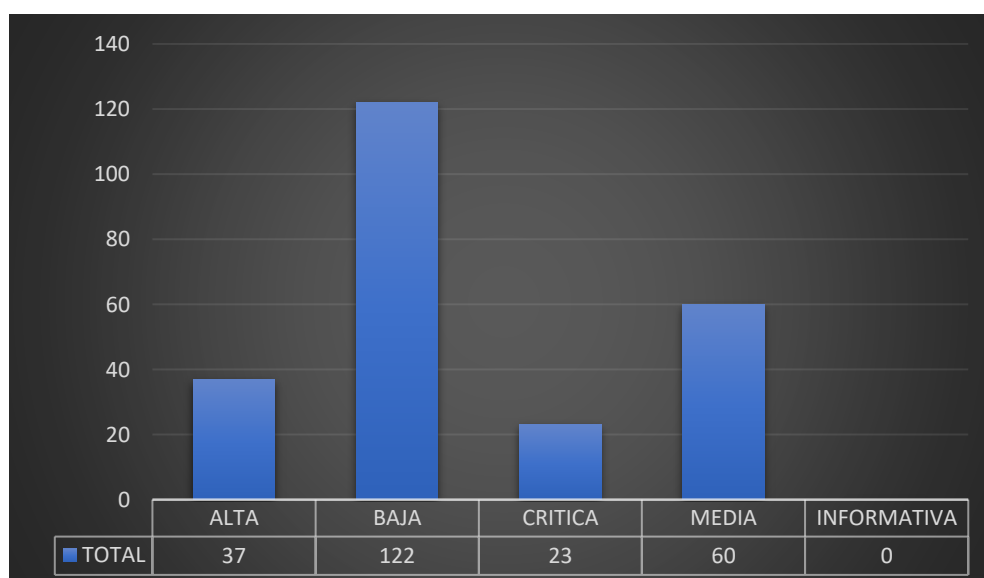
Registro de amenazas bloqueadas por el Firewall Anterior Sede Parcoy.



Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad de todo el tráfico que han sido bloqueadas por el Firewall Anterior en la sede Parcoy.

Figura 8

Registro de amenazas bloqueadas provenientes de Internet por el Firewall Anterior Sede Lima.



Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad del tráfico proveniente de Internet que han sido bloqueadas por el Firewall Anterior en la sede Lima.

3.5.2 Configuración del Firewall

Completada la etapa de recolección, se procede a realizar el nuevo diseño de la red e implementar el Firewall de acuerdo con las especificaciones y requisitos previamente definidos. Se llevarán a cabo las configuraciones necesarias.

Figura 9

Firewall Palo Alto modelo PA-450.

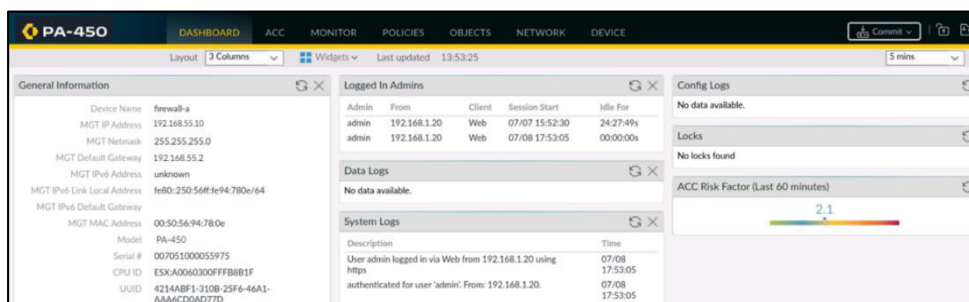


Nota: El gráfico muestra el modelo de Firewall Next Generation de Palo Alto. Tomado de *la página de Palo Alto*.

Al iniciar la configuración del Firewall se debe registrar y activar las licencias del Firewall en portal de Palo Alto. Se accede al Firewall a través de la GUI Web para hacer el cual nos muestra la información general del Firewall como IP, nombre, firmware, acceso al equipo, el factor de riesgo, entre otros.

Figura 10

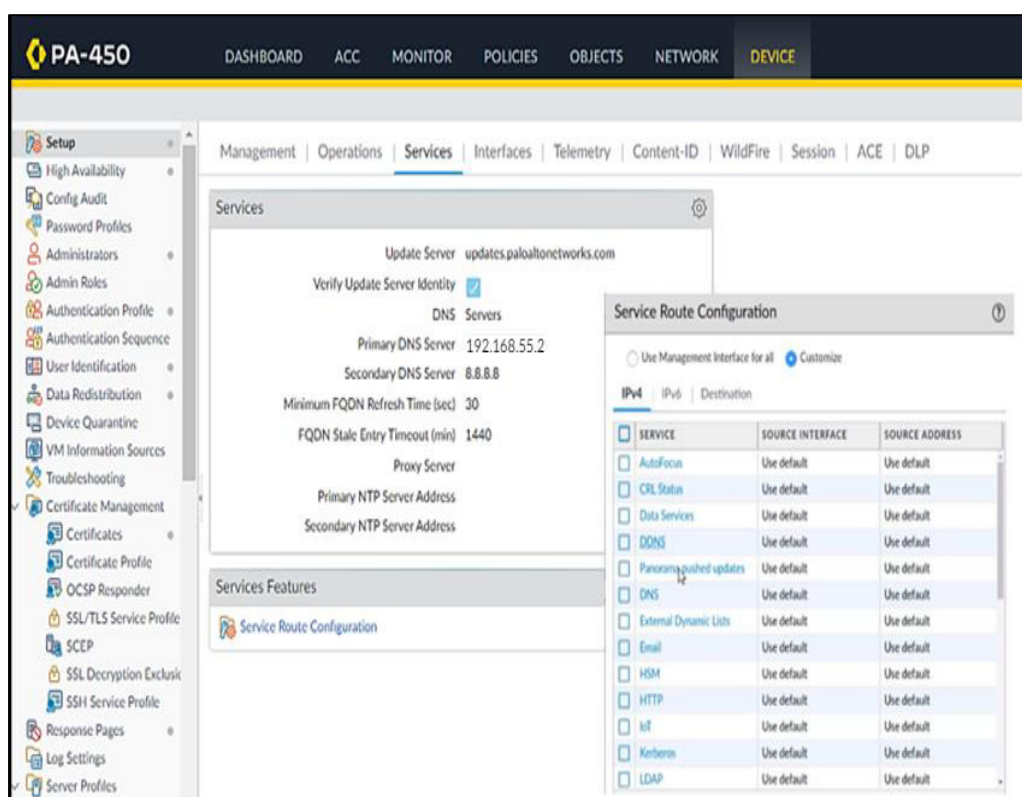
Dashboard del Firewall.



Nota: El gráfico muestra el dashboard, donde se concentra información resumida. Tomado del firewall *de Palo Alto*.

De forma predeterminada, el firewall utiliza la interfaz MGT (administración) para acceder a servicios DNS, servicios de actualización de contenido, servicios de recuperación de licencias, servicios NTP u otros servicios externos.

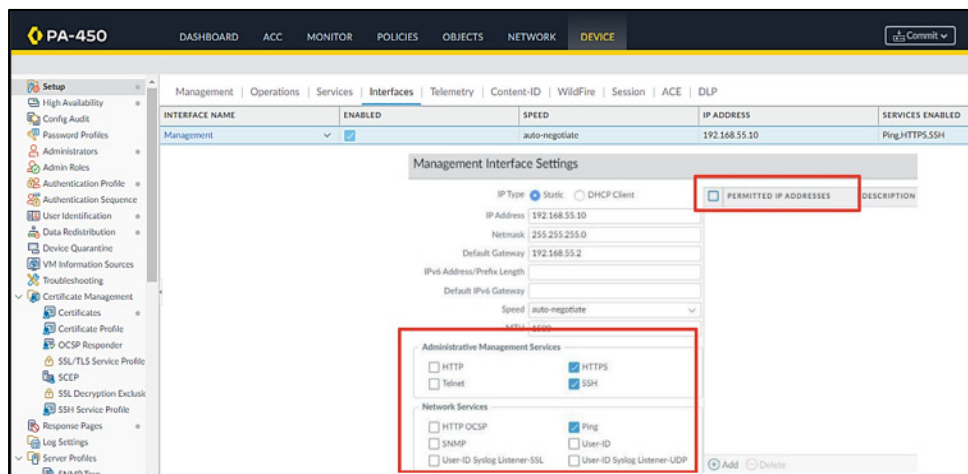
Figura 11
Configuración de Rutas de servicios.



Nota: El gráfico muestra las opciones a configurar de las rutas de servicio, que ayudará a tener conectividad al Firewall y los servicios asociados a éste. Tomado del *firewall de Palo Alto*.

Se realiza la configuración de la IP de administración del firewall y se habilita los permisos que tendrá habilitado, además de, poder gestionar una lista de IP's que solo tendrán permiso de acceder al equipo.

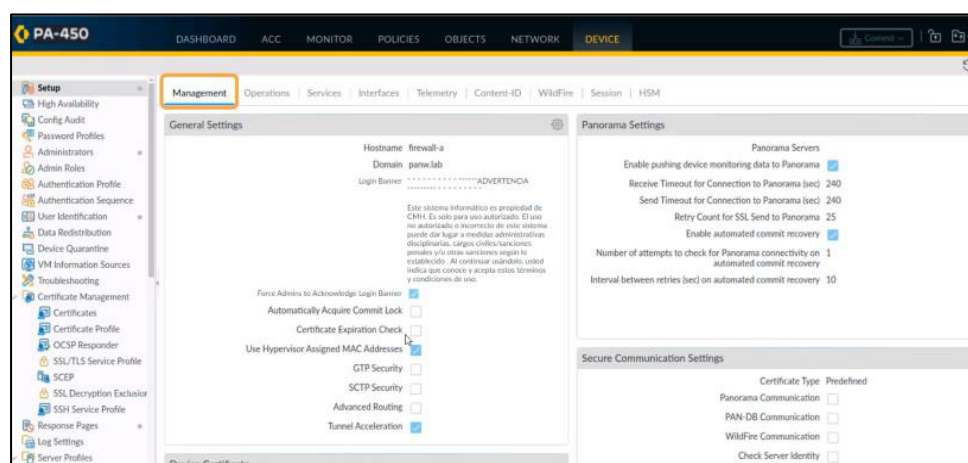
Figura 12
Configuración de administración del Firewall.



Nota: El gráfico muestra la opción de configurar la dirección IP de administración y el perfil de administración de servicio como https, ssh, entre otros. Tomado del *firewall de Palo Alto*.

En la sección de Configuración general, se configura el nombre del equipo, Banner de inicio de sesión como también habilitar para forzar a aceptarlo, la fecha y zona horaria, entre otros.

Figura 13
Configuraciones Generales del Firewall.



Nota: El gráfico muestra las opciones generales, como la zona horaria, banner de seguridad, entre otros. Tomado del *firewall de Palo Alto*.

Como parte de la configuración general y buenas prácticas se configura requisitos mínimos que aseguren el acceso al firewall de un usuario.

Figura 14

Configuración de complejidad de credenciales.

Nota: El gráfico muestra las opciones de los valores de contraseña de los usuarios administradores. Tomado del *firewall de Palo Alto*.

Posterior a la activación de las licencias adquiridas, se configura el horario para que éstas realicen la comunicación con la base de datos y proceda a la actualización.

Figura 15

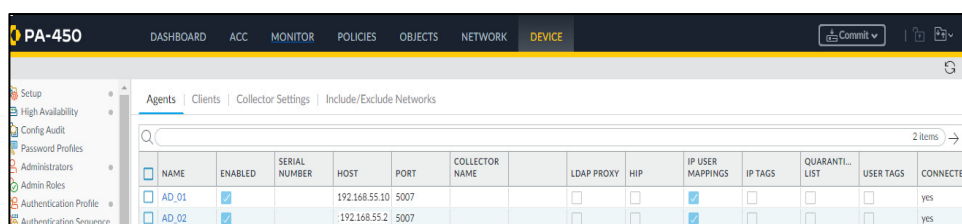
Actualizaciones dinámicas.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNL
> Antivirus	Last checked: 2023/11/03 16:16:39 -05	Schedule: Every hour (Download and Install)					
> Applications and Threats	Last checked: 2023/11/03 16:16:39 -05	Schedule: Every 30 minutes at 25 minutes past half-hour (Download and Install)					
> Device Dictionary	Last checked: 2023/11/03 16:16:39 -05						
> WildFire	Last checked: 2023/11/03 16:16:39 -05	Schedule: Every minute (Download and Install)					

Nota: El gráfico muestra las opciones de horario, descarga e instalación de las actualizaciones dinámicas. Tomado del *firewall de Palo Alto*.

También se configuró los permisos para la sincronización del Firewall con el Directorio Activo.

Figura 16
Configuración de AD.

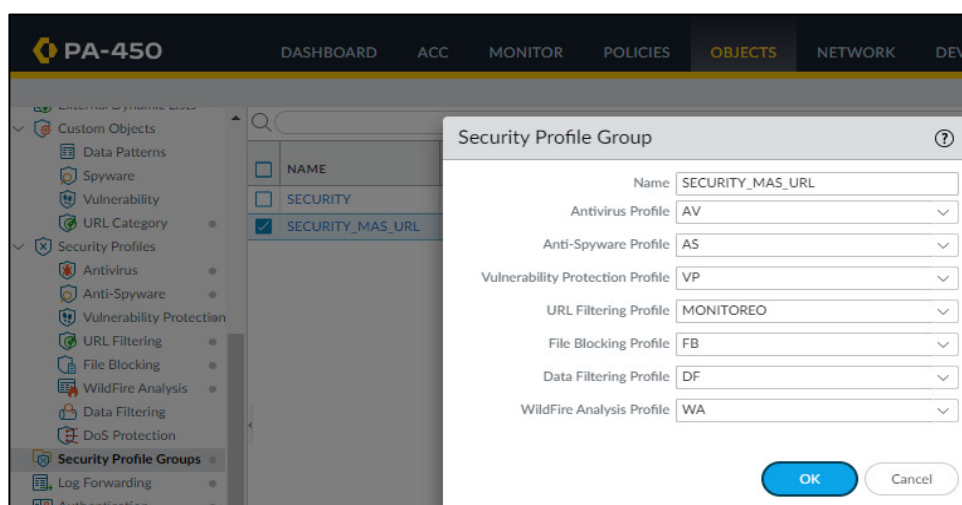


NAME	ENABLED	SERIAL NUMBER	HOST	PORT	COLLECTOR NAME	LDAP PROXY	HIP	IP USER MAPPINGS	IP TAGS	QUARANTILI...	USER TAGS	CONNECTED
AD_01	☒		192.168.55.10	5007		☐	☐	☒	☐	☐	☐	yes
AD_02	☒		192.168.55.2	5007		☐	☐	☒	☐	☐	☐	yes

Nota: El gráfico muestra la conectividad y monitoreo de los agentes User-Id instalado en los directorios activos. Tomado del *firewall de Palo Alto*.

Parte fundamental para el fortalecimiento de la seguridad en la red, se configuraron los perfiles de seguridad.

Figura 17
Perfil de Seguridad.



Security Profile Group

Name: SECURITY_MAS_URL

Antivirus Profile: AV

Anti-Spyware Profile: AS

Vulnerability Protection Profile: VP

URL Filtering Profile: MONITOREO

File Blocking Profile: FB

Data Filtering Profile: DF

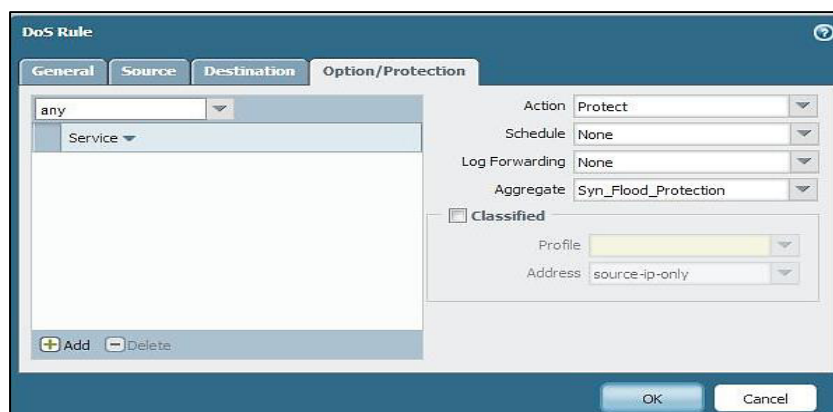
WildFire Analysis Profile: WA

OK Cancel

Nota: El gráfico muestra la configuración de un grupo que reúne los perfiles de seguridad. Tomado del *firewall de Palo Alto*.

Se configuró el perfil DoS, que evita saturándolos con una cantidad excesiva de tráfico.

Figura 18
Política de Seguridad de Protección DoS.



Nota: El gráfico muestra la configuración de la política DoS. Tomado del *firewall de Palo Alto*.

La política de calidad de servicio permite brindar calidad a la navegación del tráfico, configurando la clase y tipo de servicio.

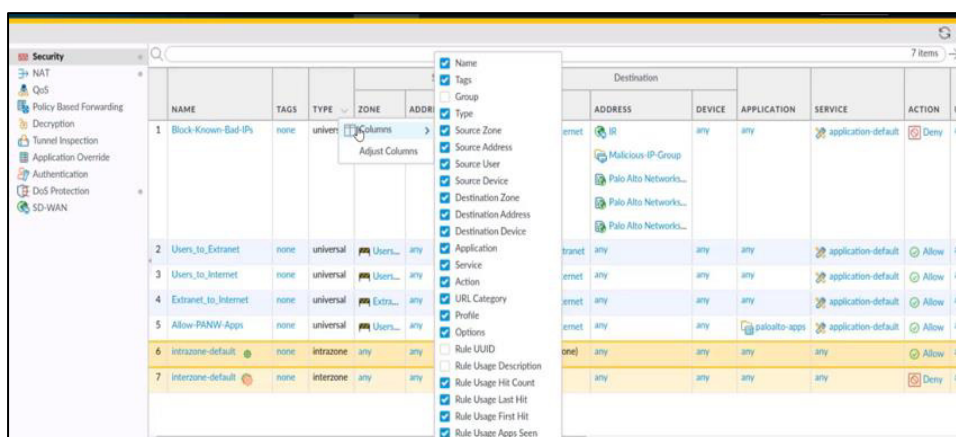
Figura 19
Perfil Calidad y Servicio (QoS).

PA-450											
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE											
POLICIES											
NAME TAGS ZONE ADDRESS USER DEVICE ZONE ADDRESS DEVICE APPLICATION											
1	QoS Team	none	LAN	any	any	any	WAN	any	any	any	ms-teams, ms-teams-audio-video, ms-teams-download, ms-teams-editing, ms-teams-file-event, ms-teams-sharing, more...
2	QoS Team-1	none	LAN	any	any	any	INTERNET WAN	any	any	any	ms-teams, ms-teams-audio-video, ms-teams-download, ms-teams-editing, ms-teams-file-event, ms-teams-sharing, more...
NAME GUARANTEED EGRESS MAXIMUM EGRESS PRIORITY											
default											
class1											
class2											
class3											
class4											
class5											
class6											
class7											
class8											
PRIORITY INETS											
class1											

Nota: El gráfico muestra la configuración de la política de Calidad y Servicio. Tomado del *firewall de Palo Alto*.

Se configura la política de seguridad asignada de acuerdo a los accesos de las redes, sea permitir o denegar.

Figura 20
Políticas de Seguridad.



Nota: El gráfico muestra la configuración de las políticas de seguridad. Tomado del *firewall de Palo Alto*.

Se configura para cambiar la dirección IP de origen que salen y destino que ingresan de una red hacia otra red, sean públicas o privadas.

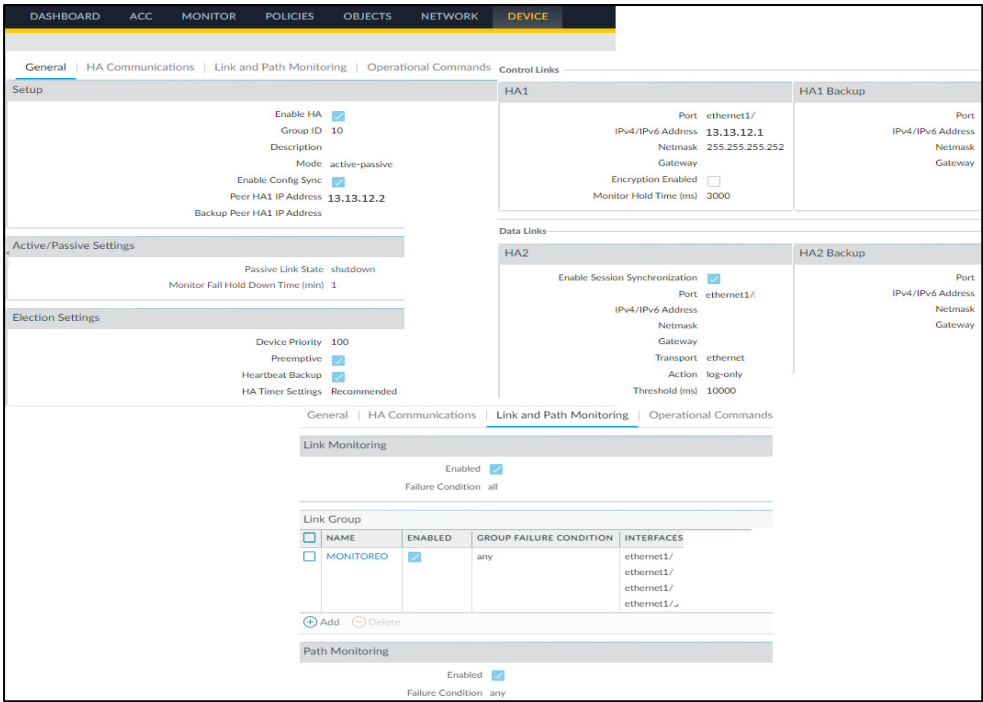
Figura 21
Políticas Nat.

NAME	TAGS	Original Packet					Translated Packet		
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
PRUEBA_SALIDA EXTERNA	none	LAN	INTERNET	any	any	any	any	dynamic-ip-and-port ethernet1/	none
PRUEBA_SALIDA	none	VPN_GP	WAN	any	any	any	any	dynamic-ip-and-port ethernet1/	none
PRUEBA_SALIDA EXTERNA-V...	none	Inet6 Inet6 Inet6 Inet6	INTERNET	any	any	any	any	dynamic-ip-and-port	none

Nota: El gráfico muestra la configuración de las políticas Nat. Tomado del *firewall de Palo Alto*.

La implementación de Alta disponibilidad, asegura la continuidad del funcionamiento de la red.

Figura 22
Configuración de Alta Disponibilidad.



Nota: El gráfico muestra la configuración de Alta disponibilidad para la habilitación de la contingencia y conmutación del Firewall en caso de error o falla. Tomado del *firewall de Palo Alto*.

3.5.3 Diseño de la red

Se presenta las topologías de red propuestas para cada una de las sedes de la entidad. Este análisis se ha llevado a cabo con el objetivo de optimizar la infraestructura de red, mejorando tanto la eficiencia como la seguridad de las comunicaciones internas y externas.

Figura 23
Topología referencial Sede Parcoy.

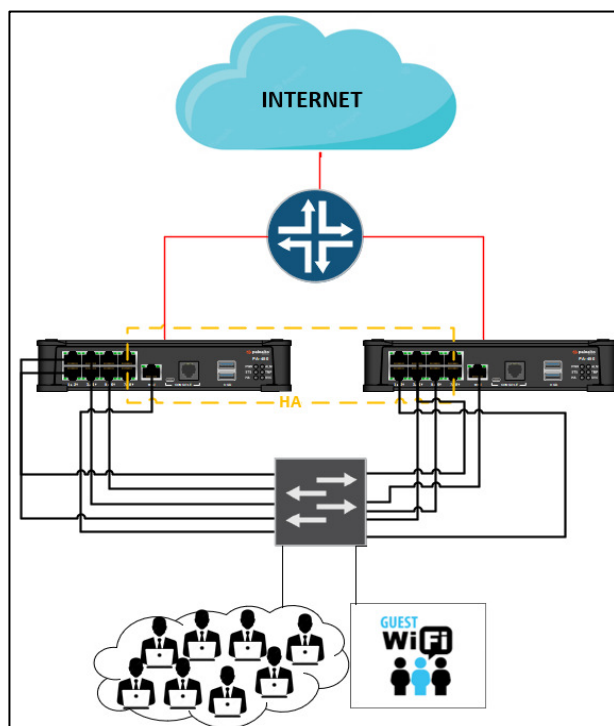
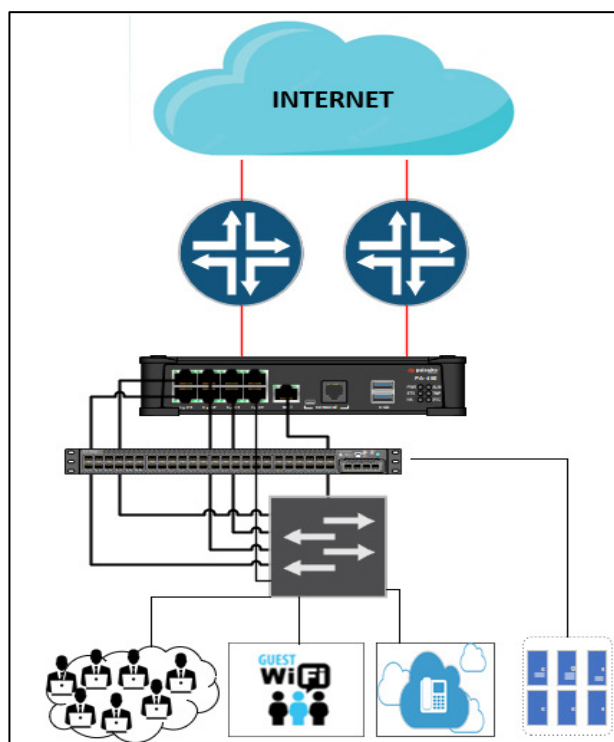


Figura 24
Topología referencial Sede Lima.



3.6 Resultado de la Actividad

Se evidencia la mejora en el fortalecimiento de la seguridad de la red, estos resultados se observan a partir de la cantidad de amenazas evidenciadas y bloqueadas con el firewall de nueva generación durante un periodo de 30 días posterior a la implementación.

Registro de conexiones

Se logra visualizar en los logs de tráfico: La hora, usuario, zona, dirección IP, política de seguridad asociada, razón por la que culminó la sesión, el puerto, aplicaciones y la acción de permitir o denegar. Nos brinda un mayor panorama para un mejor análisis.

Figura 25
Logs de registros.

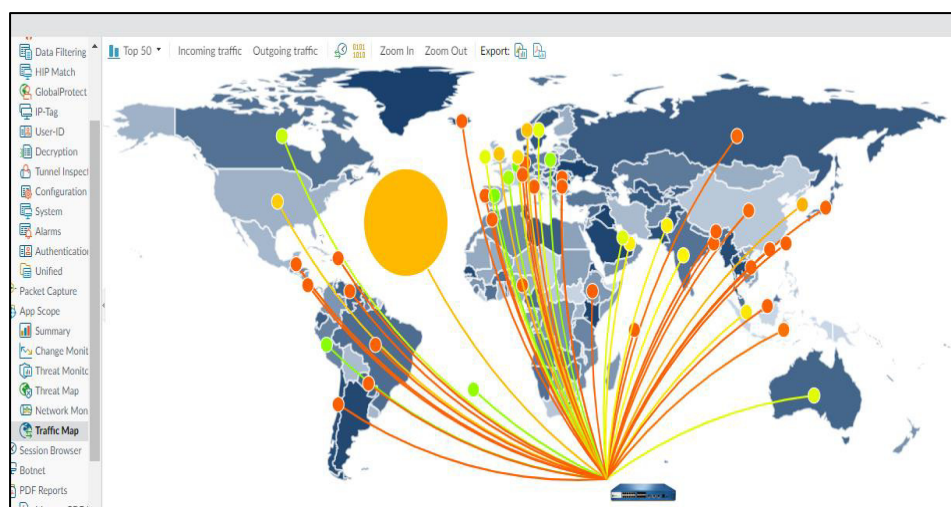
	RECEIVE TIME	TYPE	SOURCE USER	INGRESS I/F	EGRESS I/F	FROM ZONE	SOURCE	TO ZONE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
	05/22 23:05:14	drop		ethernet1/		LAN		INTERNET...	20.42.65.92	443	not-applicable	deny	Bloqueo_internet-1	policy-deny	0
	05/22 23:05:14	drop	lab/marketing	ethernet1/		LAN		INTERNET...	20.190.173...	443	not-applicable	deny	Bloqueo_internet-1	policy-deny	0
	05/22 23:05:14	drop		ethernet1/		LAN		INTERNET...	172.217.192...	443	not-applicable	deny	Bloqueo_internet-1	policy-deny	0
	05/22 23:05:14	drop	lab/marketing	ethernet1/		LAN		INTERNET...	20.190.173...	443	not-applicable	deny	Bloqueo_internet-1	policy-deny	0
	05/22 23:05:14	end		ethernet1/	ethernet1/	LAN		WAN	13.107.42.12	443	ssl	allow	Salida Internet-CLASE_FULL	threat	427
	05/22 23:05:14	end	lab/marketing	ethernet1/	ethernet1/	InetV	10.10.14.88	LAN	192.168.1.2	53	dns-base	allow	COMUNICACION-INTERNAL	aged-out	436
	05/22 23:05:14	end		ethernet1/	ethernet1/	LAN		WAN	172.16.105.48	7680	insufficient-data	allow	Salida Internet-CLASE_FULL	tcp-fin	561
	05/22 23:05:14	end	lab/marketing	ethernet1/	ethernet1/	LAN		WAN	192.168.3.31	1500	informis	allow	COMUNICACION-PARCOY...	tcp-fin	276

Nota: El gráfico muestra los eventos de tráfico entrante y saliente. Tomado del *firewall de Palo Alto*.

Mapa de tráfico

En el apartado del Mapa de Tráfico se observa de manera gráfica hacia qué región se establece las comunicaciones salientes de la red.

Figura 26
Mapa de tráfico.

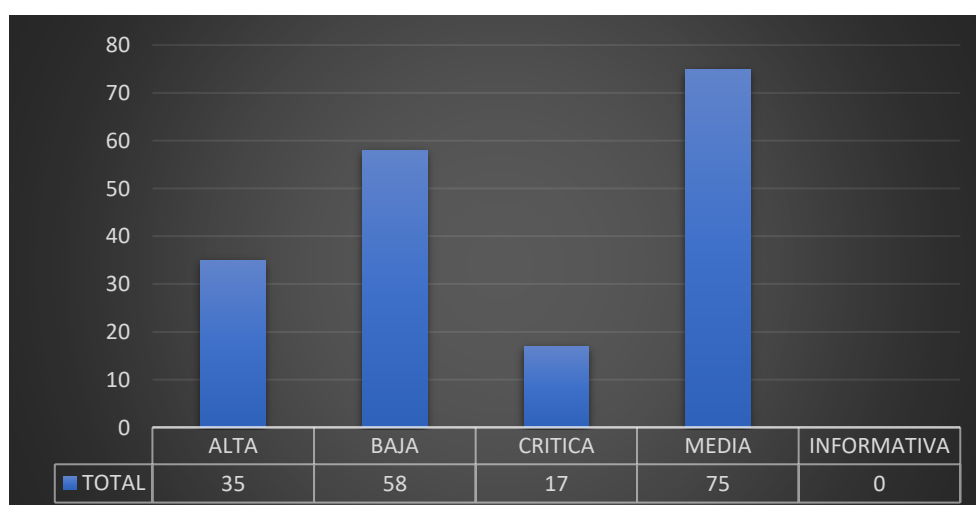


Nota: El gráfico muestra el mapa de tráfico indicando los países destino. Tomado del *firewall de Palo Alto*.

Registro de bloqueos de amenazas.

Según la recolección de logs con la implementación del Firewall de Nueva Generación se muestra la cantidad de amenazas bloqueadas.

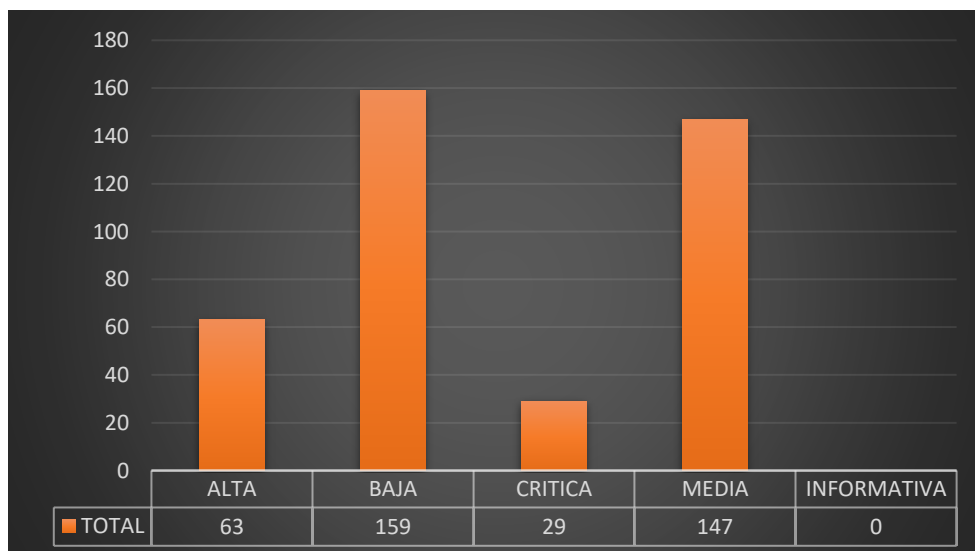
Figura 27
Registro de amenazas bloqueadas hacia la Wan Sede Parcoy.



Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad del tráfico proveniente de Internet que han sido bloqueadas por el Firewall Palo Alto en la sede Parcoy.

Figura 28

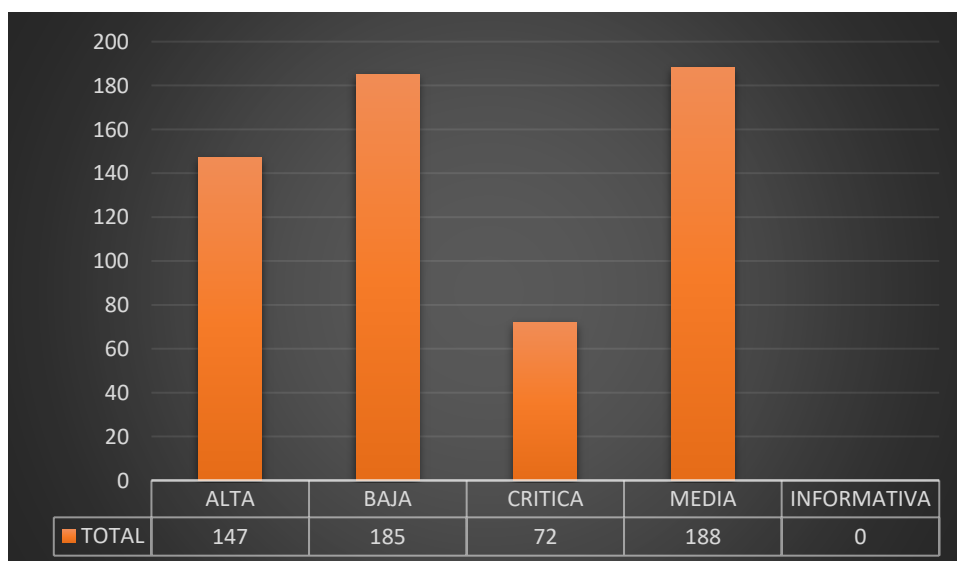
Registro de amenazas bloqueadas en la red de Parcoy.



Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad de todo el tráfico que han sido bloqueadas por el Firewall Palo Alto en la sede Parcoy.

Figura 29

Registro de amenazas bloqueadas hacia la Wan Sede Lima.



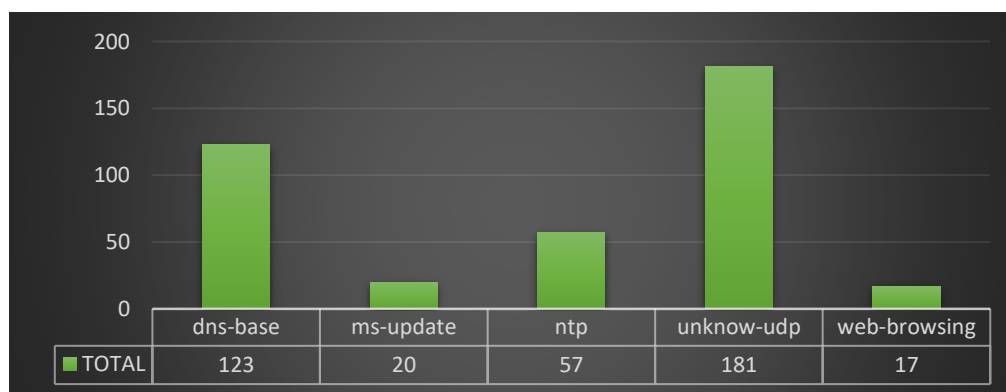
Nota: El gráfico muestra la cantidad de amenazas según el nivel de criticidad de todo el tráfico proveniente de Internet que han sido bloqueadas por el Firewall Palo Alto en la sede Lima.

Actividad de aplicación bloqueada

La presente figura nos detalla la cantidad de actividades de las aplicaciones que han bloqueado a partir de las políticas de configuradas.

Figura 30

Actividad de aplicación bloqueada.



Nota: El gráfico muestra las aplicaciones que han sido bloqueadas por el Firewall Palo Alto en la sede Parcoy.

Alta Disponibilidad

Se obtiene como resultado en caso de que se presente algún desperfecto o avería el tráfico conmutará hacia el otro firewall que conforma HA.

Figura 31

Log de Alta Disponibilidad.

RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION
05/02 11:22:21	ha	critical	connect-change	HA Group 10: HA heartbeat backup connection down
05/02 11:21:36	ha	informational	connect-change	HA Group 10: HA heartbeat backup connection up
05/02 11:21:29	ha	critical	connect-change	HA Group 10: HA heartbeat backup connection down
05/02 11:20:58	ha	informational	connect-change	HA Group 10: HA heartbeat backup connection up
05/02 11:20:55	ha	critical	connect-change	HA Group 10: HA heartbeat backup connection down
05/02 11:20:44	ha	informational	connect-change	HA Group 10: HA heartbeat backup connection up
05/02 11:20:42	ha	critical	connect-change	HA Group 10: HA heartbeat backup connection down
05/02 11:20:32	ha	informational	connect-change	HA Group 10: HA heartbeat backup connection up

Nota: El gráfico evidencia la conmutación y configuración de Alta disponibilidad. Tomado de *Firewall Palo Alto*.

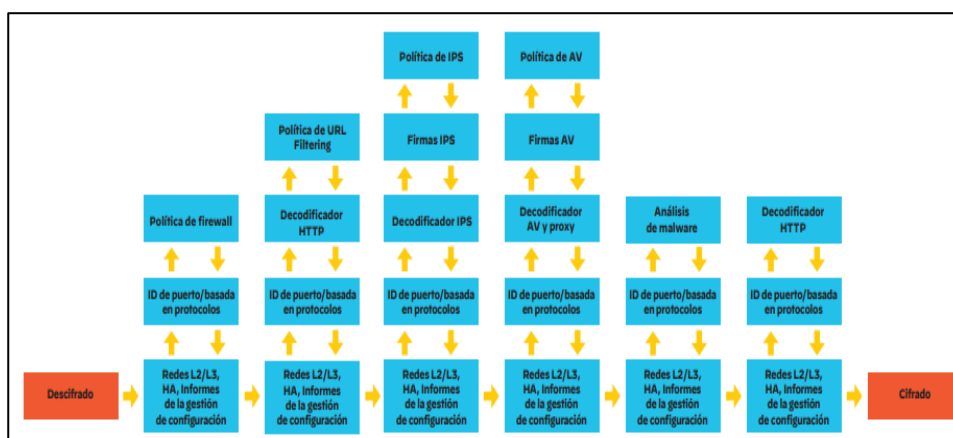
CAPITULO IV: DISCUSIÓN DE RESULTADOS

4.1 Descripción de la Implementación

Dado el aumento de los ataques cibernéticos, se hace indispensable proteger los activos e información. La seguridad con eficiencia operativa, el cumplimiento de las normativas de seguridad, la visibilidad, el control de los componentes de la red en conjunto se suman como una inversión estratégica de protección efectiva de los activos y datos críticos de la entidad.

La implementación del NGFW Palo Alto, contribuye al procesamiento de datos en un solo paso, en la siguiente imagen se muestra el procesamiento en diferentes pasos el cual no es óptimo, genera mayor tiempo y menos eficacia.

Figura 32
Procesos de un enfoque de múltiples pasos.



Nota: El gráfico los procesos del enfoque de múltiples pasos del Firewall Next Generation Palo Alto. Tomado de *la página web paloaltonetworks.lat*.

Además, la elección de un Firewall de nueva generación Palo Alto se justifica con base en los objetivos planteados. El Cuadrante Mágico de Gartner proporciona una comparativa detallada de los proveedores de Firewalls, clasificándolos en cuatro categorías: Nicho de Jugadores, Desafiadores, Visionarios y Líderes. Se observa que Fortinet, Palo Alto y Checkpoint son líderes.

Figura 33
Cuadrante mágico para Firewalls.



Nota: El gráfico muestra el cuadrante mágico de Gartner. Tomado de la página Tecnozero.

4.2 Presentación de Resultados y Evaluación económica

4.2.1 Seguridad

En cuanto a la implementación de Firewall de Nueva Generación Palo Alto en las sedes de Lima y Parcoy de Consorcio Minero Horizonte se muestran resultados que demuestra una mayor capacidad de visibilidad y mitigación de amenazas.

Tabla 1

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto sede Lima conexión hacia Internet.

Nivel de Criticidad	Antes de Implementar Firewall NGFW PA-450	Después de Implementar Firewall NGFW PA – 450
Crítica	23	72
Alta	37	147
Media	60	188
Baja	122	185
Informativa	0	0

Nota: Estos resultados se han obtenido por medio de monitorear 30 días antes de la implementación NGFW y el monitoreo 30 días posterior a la implementación de NGFW ha mejorado la capacidad de visibilidad y protección contra amenazas para la conectividad hacia Internet en la sede Lima.

Tabla 2

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto sede Parcoy conexión hacia Internet.

Nivel de Criticidad	Antes de Implementar Firewall NGFW PA-450	Después de Implementar Firewall NGFW PA - 450
Crítica	11	17
Alta	5	35
Media	6	75
Baja	16	58
Informativa	0	0

Nota: Estos resultados se han obtenido por medio del monitoreo 30 días antes de la implementación NGFW y el monitoreo 30 días posterior a la implementación de NGFW ha mejorado la capacidad de visibilidad y protección contra amenazas para la conectividad hacia Internet en la sede Parcoy.

Tabla 3

Cuadro comparativo de amenazas mitigadas por el NGFW Palo Alto en toda la red sede Parcoy.

Nivel de Criticidad	Antes de Implementar Firewall NGFW PA-450	Después de Implementar Firewall NGFW PA - 450
Crítica	18	29
Alta	13	63
Media	40	147
Baja	89	159
Informativa	0	0

Nota: Estos resultados se han obtenido por medio del monitoreo 30 días antes de la implementación NGFW y el monitoreo 30 días posterior a la implementación de NGFW ha mejorado la capacidad de visibilidad y protección contra amenazas para la conectividad en toda la red de la sede Parcoy.

4.2.2 Evaluación Económica

En la tabla 4 se muestra los costos obtenidos del desarrollo del proyecto, se tomó en consideración: Costo del producto, licencias, implementación y servicio gestionado por un periodo de 4 años.

Tabla 4

Costo de implementación de NGFW Palo Alto Networks.

ITEM	DESCRIPCIÓN	COSTO
1	3 Firewalls Modelo PA – 450	\$ 9,849.00
2	Licencias	\$ 14,950.00
3	Bandejas	\$ 24.33
4	Conectores y cables	\$ 64.10
5	Costo de Implementación	\$ 3,250.00
6	Servicio Gestionado	\$14,350.00
	TOTAL	\$ 42,487.43

CAPÍTULO V: CONCLUSIONES

- En este trabajo se muestra cómo se redujeron los incidentes de seguridad para fortalecer la capacidad de la red frente a los ataques mediante el cumplimiento de las normativas de seguridad de datos y la garantía de que solo usuarios autorizados tengan acceso a la información crítica. A través de la elaboración de un plan de trabajo y diseño de red, se logró recolectar información que reveló las siguientes deficiencias: Las políticas de seguridad no tenían aplicados al 100% perfiles de seguridad, los eventos de seguridad del tráfico no reflejaron todas las amenazas hacia la red, no tenían configurado las políticas de seguridad para el control de acceso no autorizado a la información crítica. Se aprovechó las características del Firewall Palo Alto, uno de los líderes en Firewalls, por lo cual se configuró perfiles de seguridad que identifican y contienen las amenazas, se controló los accesos y se migró los puertos de servicios hacia identificadores de aplicaciones.
- Se implementó la alta disponibilidad en el Firewall de Nueva Generación, por lo que se configuró el Firewall de la sede Parcoy en modo A-P, en caso de una falla y/o avería del Firewall Primario el tráfico conmute hacia el Firewall Secundario para asegurar el funcionamiento de los servicios críticos.
- Se validó el rendimiento obtenido posterior a la implementación del Firewall de Nueva Generación en la red, se corrigió los posibles fallos mediante las pruebas de Alta disponibilidad, se ajustó las configuraciones del firewall en la etapa de monitoreo, se mejoró la capacidad de protección para la conexión hacia Internet en Parcoy y Lima y la capacidad de bloquear amenazas en toda la red en Parcoy.

CAPÍTULO VI: RECOMENDACIONES

- Se recomienda actualizar Firewalls regularmente, el firmware debe ser una versión recomendada por el fabricante y actualizar las capacidades de actualización dinámica de los firewalls para prevenir amenazas. Esto incluye aplicar parches y actualizaciones de seguridad tan pronto como estén disponibles.
- Supervisar los registros de tráfico y amenazas para detectar actividades sospechosas y tomar medidas preventivas.
- Realizar copias de seguridad periódicas, se debe programar y realizar copias de seguridad regulares de todos los datos críticos y almacenar en un lugar seguro y accesible en caso de un incidente de seguridad.
- Revisar cambios en la configuración del firewall, realizar auditorías periódicas de la configuración del sistema del firewall para asegurar que no se hayan hecho cambios no autorizados y que la configuración sigue las mejores prácticas de seguridad.
- Proteger los registros de auditoría, asegurar los registros de auditoría contra borrados y modificaciones no autorizadas. Guardar esta información de acuerdo con las regulaciones de seguridad y políticas internas para garantizar su integridad y disponibilidad.
- Mantener recursos de la red y energía eléctrica, asegurar que los recursos de la red interna y la alimentación eléctrica estén siempre disponibles. Implemente sistemas de respaldo de energía y soluciones de redundancia de red para minimizar el tiempo de inactividad.

CAPÍTULO VII: BIBLIOGRAFÍA

- Álvarez, J. y Caruzo, J. (2015). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD UTILIZANDO EL FIREWALL IPCOP PARA EL CONTROL DEL ACCESO A INTERNET Y A LA RED DE DATOS DE LA UNIVERSIDAD DE CÓRDOBA*. Universidad de Córdoba. Facultad de Ingenierías. Obtenido de <https://repositorio.unicordoba.edu.co/handle/ucordoba/495>
- Ardila, R. y García, S. (2013). *DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PARA REDES BASADAS EN EL PROTOCOLO MODBUS TCP POR MEDIO DE NETFPGA*. Universidad Pontificia Bolivariana. Escuela de Ingeniería. Obtenido de <http://hdl.handle.net/20.500.11912/5823>
- Caballa, E. y Torres, W. (2010). *Implementación de una solución de seguridad informática bajo la plataforma de gestión unificada de amenazas*. Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática. Obtenido de http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/15154/caballa_te.pdf?sequence=1&isAllowed=y
- Chicaiza, J. (2017). *IMPLEMENTACIÓN DE UN FIREWALL CONSTRUIDO A PARTIR DE SOFTWARE Y UNA PLACA DE CIRCUITOS COMPACTA O SBC (SINGLE BOARD COMPUTER) EN LA EMPRESA TAO SYSTEMS DE LA CIUDAD DE POPAYÁN*. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Obtenido de <https://repository.unad.edu.co/handle/10596/17389>
- Iturrigaza, M y Montes, J. (2015). *DISEÑO DE ARQUITECTURA DE SEGURIDAD PERIMETRAL PARA UNA EMPRESA DEDICADA A LA ACTIVIDAD INMOBILIARIA*. Universidad Ricardo Palma. Facultad de Ingeniería. Obtenido de

https://repositorio.urp.edu.pe/bitstream/handle/20.500.14138/2136/iturrizaga_ma-montes_jm.pdf?sequence=1&isAllowed=y

Palo Alto Networks. (2016). *Descripción General del Firewall*. Obtenido de https://www.paloaltonetworks.com.mx/apps/pan/public/downloadResource?pagePath=/content/pan/es_MX/resources/datasheets/descripcion-del-firewall

Palo Alto Networks. (2021). *Arquitectura de paso único*. Obtenido de <https://www.paloaltonetworks.lat/resources/whitepapers/single-pass-parallel-processing-architecture>

PaloWard (S.F.). *Single Pass Parallel Processing (SP3) Architecture*. Obtenido de <https://www.paloguard.com/SP3-Architecture.asp>

Pascuas, J., Penagos, A. y Toconas, J. (2015). *IMPLEMENTACIÓN DE DISPOSITIVO FIREWALL CON REGLAS DE TRÁFICO EN LA CLÍNICA MEDILASER S.A. SEDE NEIVA*. Universidad Cooperativa de Colombia. Facultad de Ingenierías. Obtenido de <https://hdl.handle.net/20.500.12494/44651>

Pitancur, B. (2019). *Diseño e Implementación de una Red de datos y seguridad perimetral de la empresa Corporación Cayman S.A.C.* Universidad Tecnológica del Perú. Facultad de Ingeniería. Obtenido de <https://hdl.handle.net/20.500.12867/5933>

CAPÍTULO VIII: ANEXOS

ANEXO 1: Matriz de consistencia

Matriz de Consistencia				
Título: “DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PERIMETRAL DE NUEVA GENERACIÓN (NGFW) PARA LAS SEDES DE LIMA Y PARCOY DE UNA UNIDAD MINERA EN EL AÑO 2023.				
PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	MÉTODO Y DISEÑO
Problema General: ¿Cómo mejorar la seguridad de la red para dos sedes de una unidad minera mediante el diseño e implementación de un Firewall Perimetral de Nueva Generación (NGFW) en el año 2023?	Objetivo General: Implementar un firewall de nueva generación (NGFW) en dos sedes de una Unidad Minera en el año 2023 para fortalecer la seguridad de la red y proteger los activos críticos de la empresa.	Hipótesis General: El diseño y la implementación de un firewall perimetral de nueva generación (NGFW) en dos sedes de una unidad minera en el año 2023 reducirá significativamente el riesgo de intrusiones maliciosas, fortaleciendo así la protección de los datos y activos críticos de la empresa.	Variable Independiente Implementación de un firewall de nueva generación (NGFW). Implementación de alta disponibilidad en los Firewalls. Implementación del proceso de validación y corrección de posibles fallas en la configuración del Firewall.	Método Temporal. El estudio es del tipo transversal, su ejecución se inicia el febrero del año 2023 y mayo del 2023.
PROBLEMAS ESPECÍFICOS	OBJETIVOS ESPECÍFICOS	HIPÓTESIS ESPECÍFICAS	VARIABLES	MÉTODO Y DISEÑO
Problema Específico 1: ¿Cómo la identificación de amenazas en la red podría evitar la explotación de éstas y como detectar la presencia de tráfico no autorizado?	Objetivo Específico 1: Reducir incidentes de seguridad para fortalecer la capacidad de la red frente a los ataques mediante el cumplimiento de las normativas de seguridad de datos y la garantía de que solo usuarios autorizados tengan acceso a la información crítica.	Hipótesis Específica 1: El diseño e implementación de un firewall de Nueva Generación en la red permitirá identificar las vulnerabilidades en la red que podrían ser exploradas por amenazas externas y la identificación de tráfico autorizado, que posiblemente no se detecte por firewalls de generaciones anteriores.	Variable dependiente Nivel de seguridad, incidencia de intrusiones maliciosas, protección de datos activos y críticos. Continuidad del servicio en la red. Incidentes de seguridad relacionado a las configuraciones erróneas.	El proyecto se circunscribe en el distrito de Parcoy y la ciudad de Lima en el año 2023.
Problema Específico 2: ¿Qué consideraciones se debe realizar para asegurar la disponibilidad del dispositivo de seguridad que administra la red en caso de fallas y/o interrupciones?	Objetivo Específico 2: Implementar la alta disponibilidad en el dispositivo de seguridad que administra la red en caso de falla e interrupciones para asegurar el funcionamiento de los servicios críticos.	Hipótesis Específica 2: Si se implementa la alta disponibilidad en los Firewalls de Nueva Generación, los tiempos de inactividad no planificados se reducirá y mejorará la continuidad del servicio.		
Problema Específico 3: ¿En qué medida evaluar los resultados de la implementación de un NGFW en la red?	Objetivo Específico 3: Validar el rendimiento obtenido posterior a la implementación del Firewall de Nueva Generación en la red y corregir posibles fallos.	Hipótesis Específica 3: Será posible validar el funcionamiento y corregir fallos en la configuración del firewall NGFW.		

ANEXO 2: Especificaciones Técnicas Firewall Modelo PA-450

Feature	PA-450
Performance <i>*1. Firewall throughput measured with App-ID and User-ID features enabled utilizing AppMix transactions. 2. Threat prevention throughput measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled utilizing AppMix transactions. 3. New sessions per second measured with 1 byte HTTP transactions. Additionally, for VM models, please refer to hypervisor, cloud specific data sheet for associated performance.</i>	
App-ID firewall throughput	3.3 Gbps
Threat prevention throughput	2.1 Gbps
IPSec VPN throughput	1.7 Gbps
Connections per second	48,000
Sessions	
Max sessions (IPv4 or IPv6)	300,000
Policies	
Security rules	2,500
Security rule schedules	256
NAT rules	3,000
Decryption rules	500
App override rules	500
Tunnel content inspection rules	500
SD-WAN rules	250
Policy based forwarding rules	500
Captive portal rules	500
DoS protection rules	500
Security Zones	
Max security zones	75
Objects (addresses and services)	
Address objects	15,000
Address groups	500

Members per address group	2,500
Service objects	2,000
Service groups	1,000
Members per service group	1,000
FQDN address objects	2,000
Max DAG IP addresses	100,000
<i>*System wide capacity</i>	
Tags per IP address	64
Security Profiles	
Security profiles	150
App-ID	
Custom App-ID signatures	6,000
Shared custom App-IDs	512
Custom App-IDs (virtual system specific)	6,416
User-ID	
IP-User mappings (management plane)	512,000
IP-User mappings (data plane)	128,000
Active and unique groups used in policy	1,000
<i>*Aggregate of LDAP groups, XML API Groups and Dynamic User Groups</i>	
Number of User-ID agents	100
Monitored servers for User-ID	100
Terminal server agents	1,000
Tags per User	64
<i>*Only valid for PAN-OS 9.1 and above</i>	
SSL Decryption	
Max SSL inbound certificates	100
SSL certificate cache (forward proxy)	2,000
SSL Port Mirror	Yes
SSL Decryption Broker	No
<i>*Change this to network packet broker</i>	
HSM Supported	No

URL Filtering	
Total entries for allow list, block list and custom categories	25,000
Max custom categories	2,849
Max custom categories (virtual system specific)	500
Dataplane cache size for URL filtering	150,000
Management plane dynamic cache size	600,000
EDL	
Max number of custom lists	30
Max number of IPs per system	50,000
Max number of DNS Domains per system	1,000,000
Max number of URL per system	100,000
Shortest check interval (min)	5
Interfaces	
Mgmt - out-of-band	10/100/1000, RJ45/ Micro USB console
Mgmt - 10/100/1000 high availability	NA
Mgmt - 40Gbps high availability	NA
Mgmt - 10Gbps high availability	NA
Traffic - 10/100/1000	8
Traffic - 10M/100M/1G/2.5G/5G <i>*10M/100M/...</i>	NA
Traffic - 100/1000/10000	NA
Traffic - 1Gbps SFP	NA
Traffic - 10Gbps SFP+	NA
Traffic - 25Gbps SFP28	NA
Traffic - 40/100Gbps QSFP+/QSFP28	NA
802.1q tags per device	4,094
802.1q tags per physical interface	4,094
Max interfaces (logical and physical)	3,000
Maximum aggregate interfaces	4
Maximum SD-WAN virtual interfaces	840

Power Over Ethernet	
PoE Enabled Interfaces	NA
PoE Interface Speed	NA
Total Power Budget	NA
Max Power per single port	NA
Cellular Interface	
5G	NA
Virtual Routers	
Virtual routers	5
Virtual Wires	
Virtual wires	1,024
Virtual Systems	
Base virtual systems	1
Max virtual systems	5
<i>*Additional licenses are required for virtual system capacities above the base virtual systems capacity</i>	
Routing	
IPv4 forwarding table size	7,500
<i>*Entries shared across virtual routers</i>	
IPv6 forwarding table size	7,500
<i>*Entries shared across virtual routers</i>	
System total forwarding table size	7,500
Max route maps per virtual router	null
Max routing peers (protocol dependent)	1,000
Static entries - DNS proxy	1,024
Bidirectional Forwarding Detection (BFD) Sessions	Yes
L2 Forwarding	
ARP table size per device	6,000
IPv6 neighbor table size	6,000
MAC table size per device	6,000
Max ARP entries per broadcast domain	6,000
Max MAC entries per broadcast domain	6,000

NAT	
Total NAT rule capacity	3,000
Max NAT rules (static) <i>*Configuring static NAT rules to full capacity requires that no other NAT rule types are used.</i>	3,000
Max NAT rules (DIP) <i>*Configuring DIP NAT rules to full capacity requires that no other NAT rule types are used.</i>	2,000
Max NAT rules (DIPP)	1,500
Max translated IPs (DIP)	128,000
Max translated IPs (DIPP) <i>*DIPP translated IP capacity is proportional to the DIPP pool oversubscription value. The capacity shown here is based on an oversubscription value of 1x.</i>	1,500
Default DIPP pool oversubscription <i>*Source IP and source port reuse across concurrent sessions</i>	2
Address Assignment	
DHCP servers	5
DHCP relays <i>*Maximum capacity represents total DHCP servers and DHCP relays combined</i>	500
Max number of assigned addresses	64,000
High Availability	
Devices supported	2
Max virtual addresses	48
QoS	
Number of QoS policies	2,000
Physical interfaces supporting QoS	8
Clear text nodes per physical interface	31
DSCP marking by policy	Yes
Subinterfaces supported	System Limit
IPSec VPN	
Max IKE Peers	2,800
Site to site (with proxy id)	2,800
SD-WAN IPSec tunnels	2,800
GlobalProtect Client VPN	
Max tunnels (SSL, IPSec, and IKE with XAUTH)	1,500
GlobalProtect Clientless VPN	
Max SSL tunnels	200
Multicast	
Replication (egress interfaces)	300
Routes	1,500
Product Notes	
End-of-sale	NA

Alimentación del sistema (consumo de energía medio/máx.)*
PA-410: 17/18 W PA-415, PA-440, PA-445: 29/34 W PA-450, PA-460: 33/41 W PA-415-5G: 39/44 W PA-455: 50/60 W
BTU/h máximo
PA-410: 78 PA-415, PA-440, PA-445: 117 PA-450, PA-460: 141 PA-415-5G: 150 PA-455: 205
Tensión de entrada (frecuencia de entrada)
100-240 V CA (50-60 Hz)
Consumo máximo de corriente
PA-410: 1,5 A a 12 V CC PA-415, PA-440, PA-445: 2,9 A a 12 V CC PA-450, PA-460: 3,4 A a 12 V CC PA-415-5G: 3,7 A a 12 V CC PA-455: 5 A a 12 V CC
Corriente máxima de entrada
PA-410: 2,1 A PA-415, PA-440, PA-445: 3,3 A PA-450, PA-460: 4,2 A PA-415-5G: 3,5 A PA-455: 4,4 A

ANEXO 3: Imágenes de la implementación de Firewall

Firewall rackeado e Instalado.

