



**Universidad Nacional Mayor de San Marcos**

**Universidad del Perú. Decana de América**

**Facultad de Ingeniería Electrónica y Eléctrica**

**Escuela Profesional de Ingeniería Electrónica**

**Diseño del sistema de seguridad perimetral basado en  
firewalls de nueva generación en una entidad del  
estado**

**TRABAJO DE SUFICIENCIA PROFESIONAL**

**Para optar el Título Profesional de Ingeniero Electrónico**

**AUTOR**

**Javier Gustavo NORIEGA QUIROGA**

**ASESOR**

**Mg. Carlos Alberto CHIRI HUANCA**

**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

---

Noriega, J. (2024). *Diseño del sistema de seguridad perimetral basado en firewalls de nueva generación en una entidad del estado*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

---

### Metadatos complementarios

|                                  |                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------|
| <b>Datos de autor</b>            |                                                                                           |
| Nombres y apellidos              | Javier Gustavo Noriega Quiroga                                                            |
| Tipo de documento de identidad   | DNI                                                                                       |
| Número de documento de identidad | 73216646                                                                                  |
| URL de ORCID                     | No Aplica                                                                                 |
| <b>Datos de asesor</b>           |                                                                                           |
| Nombres y apellidos              | Carlos Alberto Chiri Huanca                                                               |
| Tipo de documento de identidad   | DNI                                                                                       |
| Número de documento de identidad | 09293427                                                                                  |
| URL de ORCID                     | <a href="https://orcid.org/0000-0002-1203-2005">https://orcid.org/0000-0002-1203-2005</a> |
| <b>Datos del jurado</b>          |                                                                                           |
| <b>Presidente del jurado</b>     |                                                                                           |
| Nombres y apellidos              | Ana Milagros Coronel Chamorro                                                             |
| Tipo de documento                | DNI                                                                                       |
| Número de documento de identidad | 09752919                                                                                  |
| <b>Miembro del jurado 1</b>      |                                                                                           |
| Nombres y apellidos              | Nicanor Raúl Benites Saravia                                                              |
| Tipo de documento                | DNI                                                                                       |
| Número de documento de identidad | 10189914                                                                                  |
| <b>Miembro del jurado 2</b>      |                                                                                           |
| Nombres y apellidos              | Jorge Elías Moscoso Sánchez                                                               |
| Tipo de documento                | DNI                                                                                       |
| Número de documento de identidad | 07206008                                                                                  |
| <b>Datos de investigación</b>    |                                                                                           |
| 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<br>Departamento: Lima<br>Provincia: Lima<br>Distrito: Lince<br>Latitud: -12.08181<br>Longitud: -77.03360                                                                                                                                                                  |
| Año o rango de años en que se realizó la investigación | 2020                                                                                                                                                                                                                                                                                 |
| URL de disciplinas OCDE                                | Ingeniería eléctrica, Ingeniería Electrónica<br><a href="https://purl.org/pe-repo/ocde/ford#2.02.01">https://purl.org/pe-repo/ocde/ford#2.02.01</a><br><br>Telecomunicaciones<br><a href="https://purl.org/pe-repo/ocde/ford#2.02.05">https://purl.org/pe-repo/ocde/ford#2.02.05</a> |



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 I – Perú



## ACTA DE SUSTENTACIÓN TRABAJO DE SUFICIENCIA PROFESIONAL

### ACTA N°039/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 31 de mayo del 2024, como presidenta de Jurado la **MG. ANA MILAGROS CORONEL CHAMORRO**, integrado por el Miembro de Jurado el **DR. NICANOR RAÚL BENITES SARAVIA**, la Miembro de Jurado **MG. JORGE ELÍAS MOSCOSO SÁNCHEZ** y Miembro Asesor el **MG. CARLOS ALBERTO CHIRI HUANCA**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **JAVIER GUSTAVO NORIEGA QUIROGA** con código N° 13190155 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL BASADO EN FIREWALLS DE NUEVA GENERACIÓN EN UNA ENTIDAD DEL ESTADO**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de **16. (dieciséis)**.....

Ciudad Universitaria, 31 de mayo del 2024

MG. ANA MILAGROS CORONEL CHAMORRO  
Presidente Jurado

DR. NICANOR RAÚL BENITES SARAVIA  
Miembro Jurado

MG. JORGE ELÍAS MOSCOSO SÁNCHEZ  
Miembro Jurado

MG. CARLOS ALBERTO CHIRI HUANCA  
Miembro Asesor



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Vicerrectorado de Investigación y Posgrado



### CERTIFICADO DE SIMILITUD

Yo **MG. CARLOS ALBERTO CHIRI HUANCA** mi condición de asesor acreditado con el Acta de Sustentación de Trabajo de Suficiencia Profesional: **DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL BASADO EN FIREWALLS DE NUEVA GENERACIÓN EN UNA ENTIDAD DEL ESTADO**, presentado por el bachiller **JAVIER GUSTAVO NORIEGA QUIROGA** para optar al título profesional de Ingeniero Electronico. 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:

09293424

Nombres y apellidos del  
asesor:

Mg. Carlos Alberto Chiri Huanca



## **DEDICATORIA**

A mi padre que me acompaña cada día, a mi madre por su cuidado y dedicación, a mi abuelita que está en el cielo, a mis familiares y amigos que me han apoyado en este proceso.

## **AGRADECIMIENTOS**

A la empresa en donde crecí  
laboralmente.

## RESUMEN

El presente trabajo tiene como objetivo mostrar el diseño del sistema de seguridad perimetral basado en firewalls de nueva generación en una entidad del estado que permite la actualización de la infraestructura a nivel de hardware y software, diseño de un sistema que soporte alta disponibilidad, incorporar características como políticas avanzadas con IPS, perfiles antivirus, antispyware, detección de vulnerabilidades, protección por países, listas automatizadas de IP's maliciosas, bloqueo de ataques basados en puertos y aplicaciones, reconocimiento de navegación por usuarios y perfiles creados tanto de manera local como en el directorio activo, bloqueo de malware, acceso restringido a través de una red privada virtual (VPN) usando políticas de doble factor de autenticación para prevenir el uso de credenciales robadas, análisis de paquetes para tráfico encriptado y completa visualización con informes generados manualmente y autogenerados en la plataforma. Se dará a conocer también la propuesta de diseño y el valor agregado que se brindó con el fabricante Palo Alto Networks a través del proveedor Imperia Soluciones Tecnológicas.

Finalmente se expondrán los casos de uso, recomendaciones y conclusiones.

**Palabras clave:** Firewall de nueva generación, seguridad de la información, infraestructura tecnológica, alta disponibilidad, red privada virtual.

## ABSTRACT

The objective of this TSP is to show the design of the perimeter security system based on new generation firewalls in the state entity that allows the updating of the infrastructure at the hardware and software level, design of a system that high availability support, incorporate features such as advanced policies with IPS, antivirus profiles, antispyware, vulnerability detection, protection by country, dynamic lists of malicious IP's, blocking of attacks based on ports and applications, recognition of user browsing and profiles created by both local and active directory, malware blocking, restricted VPN access through two-factor authentication policies to prevent the use of stolen credentials, packet analysis for encrypted traffic, and complete visualization with manually generated and auto-generated reports on the platforms .

The design proposal and the added value that was provided with the maker Palo Alto Networks through the provider Imperia Technological Solutions will also be announced.

Finally, the use cases, recommendations and conclusions will be presented in this TSP.

**Keywords:** New generation firewall, information security, technological infrastructure, high availability, virtual private network.

## TABLA DE CONTENIDO

|                                                                                  |             |
|----------------------------------------------------------------------------------|-------------|
| <b>RESUMEN .....</b>                                                             | <b>iv</b>   |
| <b>ABSTRACT .....</b>                                                            | <b>v</b>    |
| <b>TABLA DE CONTENIDO .....</b>                                                  | <b>vi</b>   |
| <b>LISTA DE FIGURAS .....</b>                                                    | <b>viii</b> |
| <b>LISTA DE TABLAS .....</b>                                                     | <b>ix</b>   |
| <b>CAPITULO I: INTRODUCCIÓN.....</b>                                             | <b>1</b>    |
| <b>CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD .....</b> | <b>3</b>    |
| 2.1    Institución – Actividad que desarrolla .....                              | 3           |
| 2.2    Periodo de duración de la actividad.....                                  | 3           |
| 2.3    Finalidad y objetivos de la entidad.....                                  | 3           |
| 2.4    Razón social .....                                                        | 4           |
| 2.5    Dirección postal .....                                                    | 4           |
| 2.6    Correo electrónico del profesional a cargo. ....                          | 4           |
| <b>CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD .....</b>                           | <b>5</b>    |
| 3.1 Organización de la actividad.....                                            | 5           |
| 3.2 Finalidad y objetivos de la Actividad .....                                  | 5           |
| 3.2.1    Finalidad .....                                                         | 5           |
| 3.2.2    Objetivos .....                                                         | 6           |
| 3.3 Problemática.....                                                            | 6           |
| 3.3.1    Problema General.....                                                   | 6           |
| 3.3.2    Problemas Específicos .....                                             | 7           |
| 3.3.3    Justificación e importancia de la investigación .....                   | 7           |
| 3.4 Metodología.....                                                             | 8           |
| 3.4.1    Bases teóricas.....                                                     | 8           |
| 3.4.2    Marco conceptual .....                                                  | 10          |

|                                          |                                            |           |
|------------------------------------------|--------------------------------------------|-----------|
| 3.5                                      | Procedimiento.....                         | 14        |
| 3.6                                      | Resultado de la actividad.....             | 16        |
| 3.7                                      | Configuración de la Solución:.....         | 21        |
| 3.7.1                                    | Topología de Red Propuesta:.....           | 21        |
| 3.7.2                                    | Configuración Interna de los Equipos:..... | 22        |
| <b>CAPITULO IV: CONCLUSIONES .....</b>   |                                            | <b>33</b> |
| 4.1                                      | Justificación .....                        | 33        |
| 4.1.1                                    | Evaluación Económica.....                  | 33        |
| 4.2                                      | Descripción del diseño.....                | 33        |
| 4.3                                      | Conclusiones .....                         | 34        |
| <b>CAPITULO V: RECOMENDACIONES .....</b> |                                            | <b>36</b> |
| <b>CAPITULO VI: BIBLIOGRAFIA .....</b>   |                                            | <b>37</b> |
| <b>CAPITULO VII: ANEXOS .....</b>        |                                            | <b>40</b> |

## LISTA DE FIGURAS

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| Figura 1: Firewall Netgate Pfsense Modelo 7100-1U.....                                     | 15 |
| Figura 2: Firewalls PA-3250 en Alta Disponibilidad .....                                   | 16 |
| Figura 3: Firewall JunOS Modelo SRX 1500 .....                                             | 17 |
| Figura 4: Firewall Forcepoint Modelo N2201 .....                                           | 18 |
| Figura 5: Firewall Palo Alto Modelo PA-3250. ....                                          | 20 |
| Figura 6: Topología de Red Propuesta. ....                                                 | 22 |
| Figura 7: Servicios a habilitar para las interfaces de administración.....                 | 23 |
| Figura 8: Configuración de las Interfaces .....                                            | 24 |
| Figura 9: Configuración de enlaces WAN. ....                                               | 24 |
| Figura 10: Configuración de HA.....                                                        | 24 |
| Figura 11: Topología Final Sede Principal. ....                                            | 25 |
| Figura 12: Políticas de Seguridad.....                                                     | 26 |
| Figura 13: Actualizaciones automáticas de los equipos para los perfiles de seguridad. .... | 27 |
| Figura 14: Perfil de Seguridad de Antivirus.....                                           | 27 |
| Figura 15: Perfil de Seguridad de Antispyware. ....                                        | 28 |
| Figura 16: Perfil de Seguridad de Filtrado de URL .....                                    | 28 |
| Figura 17: Bloqueo Customizado por categoría de URL.....                                   | 29 |
| Figura 18: Perfil de Seguridad de DLP. ....                                                | 29 |
| Figura 19: Perfil de Seguridad de Sandboxing (Wildfire). ....                              | 30 |
| Figura 20: Suite de Aplicaciones.....                                                      | 30 |
| Figura 21: Running Configuration – Backup .....                                            | 31 |

## LISTA DE TABLAS

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Tabla 1: Especificaciones Técnicas de los Firewalls de Nueva Generación. | 16 |
| Tabla 2: Configuración Interna de los Equipos. ....                      | 23 |
| Tabla 3: Estimación de Costos .....                                      | 33 |

## **CAPITULO I: INTRODUCCIÓN**

En la actualidad, la seguridad de la información es un eje relevante en el mundo de las Tecnologías de la Información y Comunicaciones, en donde las corporaciones y empresas del sector privado y público ya le están dando mayor importancia dentro de la infraestructura de red; inclusive, en el actual contexto, los ciberdelincuentes y los ataques dirigidos a empresas y personas originadas durante la pandemia del covid-19 generó que se invirtieran en equipos más modernos y en más especialistas en el sector.

En este aspecto, una entidad del estado, en el año 2020 hizo la propuesta para poder desarrollar e implementar en sus sedes tecnología de nueva generación.

Es por ello que Imperia Soluciones Tecnológicas, empresa en la que laboré en los años 2020 y 2021, propuso implementar los firewalls fabricados por Palo Alto Networks con la serie PA-3200, los cuales brindaron la flexibilidad en el rendimiento y redundancia para poder cumplir con los requisitos de implementación.

En ese sentido, el presente informe de suficiencia profesional detalla el diseño que brindó las características de seguridad de próxima generación para ayudar a proteger a la organización a través de la visibilidad y el control avanzados de aplicaciones, usuarios y contenido.

El informe se desarrolló mediante los siguientes capítulos:

En el Capítulo I, se evidencia el origen y el motivo de la propuesta presentada a la organización.

En el Capítulo II, brindo detalle de la empresa en donde laboré, y también el detalle la organización en donde se propone el diseño.

En el Capítulo III, describo a modo de detalle los antecedentes, la problemática y se brinda la propuesta de solución para la organización.

En el Capítulo IV, se realizan las conclusiones. Finalmente, en el capítulo V, se realizan las recomendaciones del presente trabajo de suficiencia profesional.

## **CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD**

### **2.1 Institución – Actividad que desarrolla**

La institución donde se desarrollaron las actividades a detallarse para la entidad del estado, es la empresa Imperia Soluciones Tecnológicas el cual se dedica a brindar soluciones en tecnología que permitan optimizar y garantizar los procesos de negocios, permitiéndole una mayor productividad, alta calidad de los servicios y soporte e implementación de equipos basados en las Tecnologías de la Información.

### **2.2 Periodo de duración de la actividad.**

El desarrollo de la actividad se llevó a cabo entre los meses de octubre a diciembre del año 2020.

### **2.3 Finalidad y objetivos de la entidad**

Imperia Soluciones Tecnológicas tiene como finalidad brindar soluciones en redes y conectividad, seguridad informática, data center y servicios de soporte y post venta, respaldados por los fabricantes en los diferentes países del mundo.

## **2.4 Razón social**

La razón social de la empresa es IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.

## **2.5 Dirección postal**

Dirección Legal: Av. Abel Bergasse du Petit Thouars nro. 1775 of. 804.

Distrito/Ciudad: Lince.

Departamento: Lima, Perú.

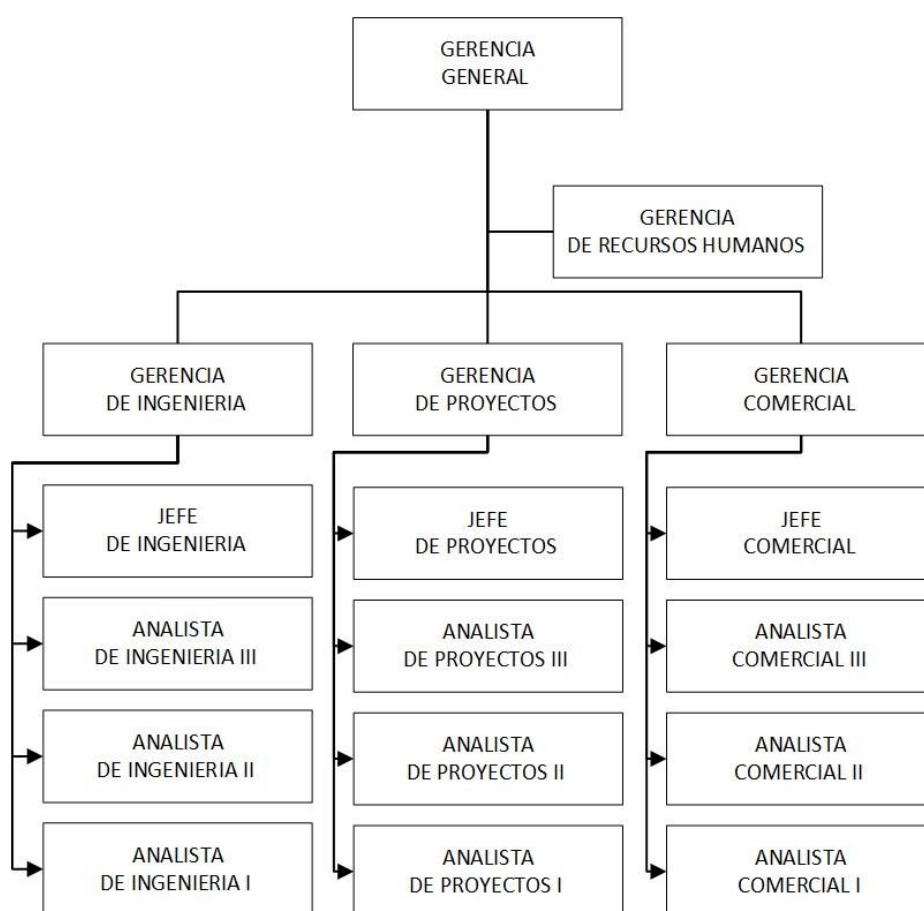
## **2.6 Correo electrónico del profesional a cargo.**

El jefe de proyecto a cargo fue el Ing. Héctor Pessolano.

Correo electrónico: hector.pessolano@imperia.com.pe

## CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

### 3.1 Organización de la actividad



### 3.2 Finalidad y objetivos de la Actividad

#### 3.2.1 Finalidad

Se propone un diseño de un sistema de seguridad perimetral basado en firewalls de nueva generación para mejorar la infraestructura tecnológica de una entidad del estado de la República del Perú.

### **3.2.2 Objetivos**

#### **3.2.2.1 Objetivo General**

Diseñar un sistema de seguridad perimetral basado en firewalls de nueva generación que permitan mejorar el sistema de seguridad y la protección de la red de la infraestructura tecnológica en una entidad del estado de la República del Perú.

#### **3.2.2.2 Objetivos específicos**

Evaluar la situación actual de la seguridad informática de la entidad del estado de la República del Perú.

Mostrar las ventajas que se obtienen al introducir firewalls de nueva generación a la infraestructura tecnológica de la entidad del estado de la República del Perú.

Diseñar la topología de red y dimensionar los parámetros técnicos de los firewalls de nueva generación.

### **3.3 Problemática**

#### **3.3.1 Problema General**

¿De qué manera se realizará el diseño un sistema de seguridad perimetral basado en firewalls de nueva generación con las nuevas tecnológicas de

protección que permitan hacer frente a las nuevas amenazas cibernéticas y asegurar la operatividad y disponibilidad de la red?

### **3.3.2 Problemas Específicos**

¿Cómo obtener información sobre la seguridad informática de la entidad del estado de la República del Perú?

¿Cómo mejorar la seguridad informática de la entidad de la entidad del estado de la República del Perú?

¿Cómo cuantificar los parámetros de funcionamiento?

### **3.3.3 Justificación e importancia de la investigación**

En la actualidad, la presente entidad de la República del Perú es una importante entidad del estado y maneja data sensible como el presupuesto y tesoro público.

Por ejemplo, los trabajadores de la presente entidad necesitan realizar transacciones hacia las distintas entidades públicas y privadas a nivel nacional para solventar los diferentes programas sociales que existen, por lo que la pérdida de la información o del servicio por ataques cibernéticos podrían afectar de manera directa hacia los distintos procesos y generar conflictos sociales.

Además, esta data sensible también está relacionada con los datos personales que toda entidad posee y esta debe tener el nivel suficiente de protección de acuerdo a la actual Ley de Protección de Datos Personales (Ley Nro. 29733).

Es por ello que, sabiendo que la presente entidad necesita mantener constantemente actualizada su infraestructura tecnológica ya que maneja data sensible, es necesario evidenciar el diseño de un sistema de seguridad perimetral basado en firewalls de nueva generación que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos.

Finalmente, en conjunto al diseño propuesto, podemos mostrar sugerencias de las mejores prácticas basándonos en las recomendaciones de Palo Alto Networks para una mejora continua y así contribuir al aumento de la literatura respecto a temas relacionados con la Seguridad de la Información.

### **3.4 Metodología**

#### **3.4.1 Bases teóricas**

A continuación, se presentarán diferentes investigaciones desde el campo internacional y nacional, relacionadas con el presente trabajo de suficiencia profesional.

##### **Internacional:**

ESET en su informe “Eset Security Report Latinoamérica” realizado en el año 2022, se evidenció que el 87% de empresas implementan antivirus, el 79% firewalls y el 70% un sistema de backup, siendo así el Perú el país con la mayor cantidad de detecciones de malware (18%), seguido por México (17%), Colombia (12%), Argentina (11%) y Ecuador (9%).

En esta misma encuesta se señala que una de las mayores preocupaciones para los encuestados en materia de ciberseguridad es la infección con códigos maliciosos (ESET, 2022).

En ese sentido, Coy (2020) publicó una tesis que tiene como objetivo mencionar todas las características de adquisición un firewall nueva generación en las entidades bancarias de Colombia y resalta que la administración de acceso a los usuarios, los mecanismos de alertas en tiempo real para la identificación de amenazas, el filtrado de paquetes y protocolos en función del origen y destino y el control del número de conexiones registradas en la red permiten fortalecer el modelo de seguridad del sector financiero (Coy, 2020).

Finalmente, Moragas et al. (2019) en su tesis “Las tecnologías de Internet, un riesgo para empresas y ciudadanos”, tuvieron como objetivo analizar y clasificar los riesgos que el uso de Internet conlleva en donde se evidencia que en una empresa puede existir la suplantación de identidad y vulneración de la privacidad además de ciberataques a empresas reconocidas como Yahoo (2016) y Zara (2017) y las consecuencias de la ciberdelincuencia como poder afectar la energía eléctrica de un país o filtrar datos de tarjetas de crédito (Moragas et al., 2019).

### **Nacional:**

Campomanes (2021) en su tesis “Diseño e implementación de firewall palo alto para mejorar el control de seguridad y acceso a internet” se menciona que dentro de las soluciones tecnológicas que actualmente están disponibles para reforzar la seguridad de una red, el firewall palo alto permite aumentar la seguridad implementando políticas de seguridad granulares mediante identificación de usuarios, inspección de contenido e identificación de aplicaciones estableciendo a que servicios se pueden acceder o que pueden ser restringidos brindando nuevas características de un firewall de nueva generación (Campomanes, 2021).

Cossio (2021) en su artículo “La Ciberseguridad de la Información del empleador y la fiscalización del trabajo remoto: Alcances y Límites”, tuvo como objetivo analizar la implementación de mecanismos de ciberseguridad de la información de parte del empleador dado el incremento de la modalidad de trabajo remoto implementado en el Perú por el contexto de la pandemia del Covid 19, se menciona que los equipos utilizados para el teletrabajo se encuentran generalmente en mayor riesgo de ataques cibernéticos en ambientes fuera de la empresa que dentro de las misma, por lo que las compañías deben implementar superiores elementos de seguridad que permitan cautelar la información corporativa (NIST, 2016).

Es por ello que uno de los mecanismos de ciberseguridad asociados al trabajo remoto es la implementación de VPN's (redes privadas virtuales) solicitados

por el mismo empleador a los empleados para que puedan acceder a los recursos internos de la red de la empresa (Cossio, 2021).

Finalmente, Cajahuaringa (2020) en su tesis titulada “Implementación de firewall para el control de servicio de internet en la filial Chanchamayo de la Universidad Peruana Los Andes” se evidencia que la implementación del firewall en una arquitectura de red además de permitir mejoras a nivel de seguridad con el nivel de control de uso y acceso a internet, permitió solucionar un problema de lentitud en la sede (Cajahuaringa, 2020).

### **3.4.2 Marco conceptual**

#### **Seguridad de la Información:**

Brinda las medidas de protección que se le debe dar a un sistema físico o digital de la organización. Su principal aspecto fundamental es velar por la integridad, confidencialidad y disponibilidad de los sistemas de información.

#### **Seguridad Informática:**

Se basa en el conjunto medidas e implementaciones para prevenir ataques cibernéticos y así proteger la información de la organización.

#### **Ciberseguridad:**

Es el conjunto de procedimientos para la protección, detección y respuesta de la información digital, es decir, la información que puede ser procesada, almacenada y transmitida a través de la red.

#### **Cibercriminal:**

Es un delincuente que usa el internet para cometer delitos cibernéticos.

**Malware:**

Software malicioso diseñado para acceder a un dispositivo y generar daño. Tipos de malware: Virus, gusanos, troyanos, botnets, spyware, rootkits, ransomware, etc.

**Amenazas Persistentes Avanzadas:**

Son técnicas avanzadas de intentos de acceso no autorizado a un sistema informático el cual necesita un mayor nivel esfuerzo debido a que se puede obtener mayor información en un lapso mayor tiempo y tiene consecuencias destructivas hacia el sistema.

**Vulnerabilidad:**

Es una falla en la seguridad relacionada al software de un dispositivo digital y que puede ser explotado por un cibercriminal.

**Sistema de Detección de Intrusos:**

Sistema diseñado para monitorear detectar una amenaza en el perímetro de una red.

**Sistema de Protección de Intrusos:**

Sistema diseñado para identificar una amenaza y proteger el perímetro de una red.

**Firewall:**

Es un dispositivo que permite o bloquea el tráfico en la red. Por su función, existen dos tipos de firewall: Los firewalls de red los cuales se ejecutan en el hardware de un equipo fuera de la computadora y es un punto intermediario entre más subredes o hacia internet y los firewalls instalados en la propia computadora que permiten un filtrado dentro del mismo equipo.

### **Firewall Tradicional:**

Es un tipo de firewall de red que permite controlar el tráfico de red basándose en puerto de origen, destino, protocolo y dirección IP.

### **Firewall de Segunda Generación:**

Este tipo de firewall además de la mencionado anteriormente permite conocer si la conexión fue exitosa o son comunicaciones que no se llegan a completar como por ejemplo un intento de conexión por escritorio remoto a una computadora que tiene el puerto cerrado el cuál será fallido.

### **Firewall de Tercera Generación:**

Este tipo de firewalls reconoce ya las aplicaciones que están relacionadas a un puerto específico, por ejemplo, reconoce que el puerto 53 está relacionado al protocolo por nombre DNS. Esto permite que se creen políticas de seguridad en base a aplicaciones y no permitir crear políticas que den pase o bloqueen todos los puertos relacionados a la aplicación.

### **Firewall de Nueva Generación:**

Este tipo de firewall, además de brindar todas las funcionalidades mencionadas anteriormente para las antiguas generaciones de los firewalls, permite una inspección de paquetes más avanzada para identificar el tráfico malicioso, sistemas de prevención y detección de amenazas (IPS e IDS), implementación de redes privadas virtuales (VPN's) y filtrado web.

### **Red Privada Virtual:**

Una red privada virtual es una conexión que nos permite acceder a los recursos locales como servidores o computadoras que están dentro de la red de una empresa estando fuera de esta red, por ejemplo, desde nuestra casa. Este tipo de conexiones permiten el cifrado de la comunicación y la transferencia segura de los datos además de ser controlado por las políticas brindadas en el firewall.

### **Doble Factor de Autenticación:**

Este término va ligado al inicio de sesión en un determinado servicio y nos permite acceder de manera más segura. Generalmente va solicita una verificación de inicio de sesión a través de dispositivo móvil ya sea por una llamada, un mensaje de texto o generando un código único en una aplicación.

### **DLP:**

Es el acrónimo de Data Loss Prevention y está relacionado a la prevención de la pérdida de información tales como información almacenada dentro de nuestro ordenador o información relevante para la empresa ya sea por filtración de los mismos usuarios en sitios restringidos o por desconocimientos de los mismos.

### **CVE:**

Es el acrónimo de Common Vulnerabilities and Exposures y es un listado de vulnerabilidades categorizadas de menor a mayor impacto.

### **Wildfire:**

El módulo de wildfire es la solución de análisis de malware de Palo Alto para prevenir amenazas desconocidas ayudando a detectar comportamiento malicioso aún no identificado a nivel de CVE integrando la nube de la marca.

## **3.5 Procedimiento**

El presente trabajo ha sido estructurado en 3 etapas:

### **Etapas 1: Situación Actual**

- La presente entidad del estado posee firewalls pfSense open source basada en FreeBSD (software libre).
- No se tiene una arquitectura en HA que permita el cambio automático entre los firewalls ante una posible falla del firewall principal.
- No se tienen políticas basadas en detección de aplicaciones, las políticas existentes son basadas en detección de puertos.



**Figura 1: Firewall Netgate PfSense Modelo 7100-1U. Fuente: Anexo 1**

## **Etap 2: Arquitectura de Solución:**

Se evalúan las siguientes alternativas de solución:

Implementación de Firewalls de Nueva Generación en HA de los siguientes fabricantes:

- JunOS (Modelo SRX 1500)
- Forcepoint (Modelo N2201)
- Palo Alto (Modelo 3250)

Requisitos Mínimos para la implementación brindados por el Ministerio de Economía y Finanzas:

**Tabla 1:** Especificaciones Técnicas de los Firewalls de Nueva Generación

| Características vs Modelos             | Firewall de Nueva Generación                                                                                      | JunOS SRX 1500 | Forcepoint N2201        | Palo Alto 3250 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------|----------------|-------------------------|----------------|
| Características Generales de Seguridad | Control granular de permisos                                                                                      | Sí             | Sí                      | Sí             |
|                                        | Troughput > 6Gbps                                                                                                 | 9Gbps (Max)    | 5.5Gbps                 | 6.3Gbps        |
|                                        | Control de aplicaciones                                                                                           | Sí             | Sí                      | Sí             |
|                                        | IPS                                                                                                               | Sí             | Sí                      | Sí             |
|                                        | Antivirus                                                                                                         | Sí             | Sí                      | Sí             |
|                                        | Antispyware                                                                                                       | No             | No                      | Sí             |
|                                        | Sandboxing (DLP)                                                                                                  | No             | Sí                      | Sí             |
|                                        | Filtrado URL                                                                                                      | Sí             | Sí                      | Sí             |
|                                        | Filtrar ataques DoS                                                                                               | Sí             | Sí                      | Sí             |
|                                        | Sesiones simultáneas = 2 millones                                                                                 | 2 millones     | 17 millones             | 2 millones     |
|                                        | Sesiones nuevas por segundo = 70 mil                                                                              | 50 mil         | 90 mil                  | 94 mil         |
|                                        | Vlan soportadas > 1024                                                                                            | 3900           | No especifica           | 4094           |
|                                        | 8 Interfaces de fibra óptica = 10GB (SFP+)                                                                        | No             | No                      | Sí             |
|                                        | Interfaz dedicada de administración = 1                                                                           | Sí             | Sí                      | Sí             |
|                                        | Interfaz de tipo consola o similar = 1                                                                            | Sí             | Sí                      | Sí             |
|                                        | Almacenamiento interno > 200GB                                                                                    | 100GB          | 64GB                    | 240GB          |
| Características Funcionales            | Políticas con capacidad de seleccionar campos como direcciones y redes, identificador de usuarios y aplicaciones. | Sí             | Sí                      | Sí             |
|                                        | Políticas con vigencia de base a tiempo                                                                           | Sí             | Sí                      | Sí             |
|                                        | Filtro de políticas para VoIP y protocolo SIP                                                                     | Sí             | Sí                      | Sí             |
|                                        | Soporte IPv4 e IPv6                                                                                               | Sí             | Sí                      | Sí             |
|                                        | Políticas de Geolocalización                                                                                      | Sí             | Sí                      | Sí             |
|                                        | Alta Disponibilidad                                                                                               | Sí             | Necesita otro appliance | Sí             |
| Características de Red y Conectividad  | Interfaces en modalidad Capa 2 y Capa 3                                                                           | Sí             | Sí                      | Sí             |
|                                        | Soporte Ruteo Estático y Dinámico                                                                                 | Sí             | Sí                      | Sí             |
|                                        | Soporte Policy Based Routing                                                                                      | No             | Sí                      | Sí             |
|                                        | Soporte para la integración con AD                                                                                | Sí             | Sí                      | Sí             |
|                                        | Soporte NAT/PAT dinámico y estático                                                                               | Sí             | Sí                      | Sí             |
|                                        | Implementar políticas QoS                                                                                         | Sí             | Sí                      | Sí             |
|                                        | Soporte DHCP                                                                                                      | Sí             | Necesita otro appliance | Sí             |
|                                        | Soporte VPN AES 128, 192 e 256 (AES)                                                                              | Sí             | Sí                      | Sí             |

Fuente: Anexo 1

### Etapa 3: Diseño Propuesto (Práctico)

De lo visto en la etapa 1 y 2 se concluye que el diseño que cumple con todos los requisitos mínimos especificados por la entidad del estado es el de dos firewalls de nueva generación Palo Alto conectados en alta disponibilidad (Activo – Pasivo).

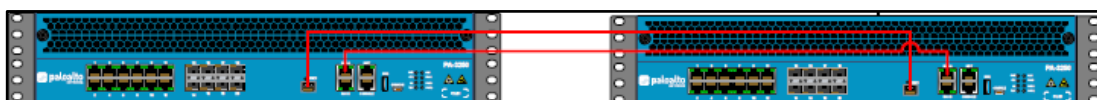


**Figura 2:** Firewalls PA-3250 en Alta Disponibilidad. Fuente: Elaboración propia

### 3.6 Resultado de la actividad

A continuación, se va a hacer un análisis de las alternativas propuestas:

### **Alternativa 1**

#### **Firewalls de Nueva Generación JunOS:**

Se maneja como primera alternativa la implementación de dos firewalls JunOS en HA.



**Figura 3: Firewall JunOS Modelo SRX 1500. Fuente: Anexo 1**

#### **Ventajas:**

- El modelo SRX 1500 brinda seguridad y es uno de los productos más económicos en comparación con otros vendors.
- Permite la detección de amenazas avanzadas y filtrado de URL.
- Permite la protección ante ataques DoS y DDoS.
- Soporta Alta Disponibilidad.
- Permite la creación de políticas por aplicativo (App-ID).
- Permite el monitoreo por usuario a nivel de consumo de ancho de banda (App-QoS).

#### **Desventajas:**

- Interface gráfica poco amigable, por lo que la mayoría de las configuraciones y soluciones se realizan a través de CLI.
- La memoria flash se corrompe debido a fallas operativas a nivel de hardware por lo que hay que realizar el formateo de la memoria o solicitar el cambio de equipo.
- Para hacer uso de la VPN se tiene como limitante un máximo de 2 usuarios en simultáneo sin licencia.
- Vulnerabilidades asociadas a DoS (CVE-2020-1661, CVE-2020-1669, CVE-2020-1667).

## **Alternativa 2**

### **Firewalls de Nueva Generación Forcepoint:**

Se maneja como segunda alternativa la implementación de dos firewalls Forcepoint en HA.

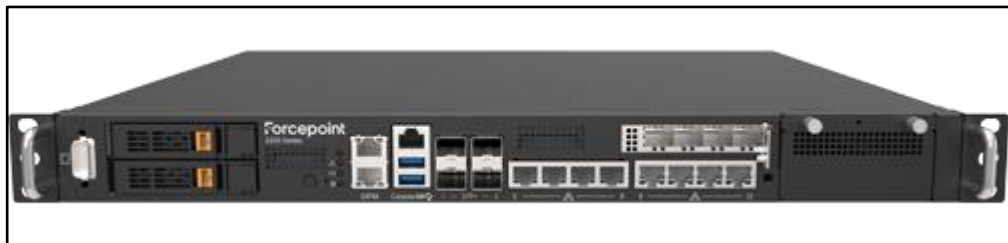


**Figura 4: Firewall Forcepoint Modelo N2201. Fuente: Anexo 1**

### **Ventajas:**

- El modelo N2201 permite la detección de amenazas avanzadas y filtrado de URL.
- Se puede implementar en un entorno Cloud (AWS y Azure).
- Enfocado a brindar solución a nivel de red.

**Desventajas:**

- La depuración de logs se puede hacer de manera automática solo a nivel de tiempo (días, semanas, meses, años, etc) mas no a nivel de cantidad de paquetes, por lo que no es eficiente en tanto la carga se incrementa, trayendo como consecuencia lentitud del equipo o inclusive perder gestión del equipo.
- Necesitan ser administrados por un Forcepoint Stonesoft Management Center (SMC), el cual centraliza la gestión de los mismos. Sin este equipo centralizador no pueden ser operados y tampoco se permite la operación en HA.
- No asignan un pool de IPs a los usuarios para conexión en Dynamic Host Configuration Protocol (DHCP), necesita un servidor exclusivo para realizar esta tarea.
- Para la comunicación del servidor Active Directory (AD) con el firewall necesita otro servidor donde se instala un agente el cual sirve de intermediario.
- Problemas con el reconocimiento de usuarios cuando se hace el cambio de contraseña o cuando se crea un nuevo usuario en el servidor AD.
- No permite utilizar un wildcard a nivel de dominio para el filtrado de URL.
- Carecen de compatibilidad con algunos vendors o marcas líderes en la región como es el caso de Solarwinds y Zabbix para sincronizar datos a nivel de syslog para que se puedan leer logs en el Security Information and Event Management (SIEM).
- La mayoría de configuraciones de preferencia se deben hacer por CLI como lo es el rollback, consulta de consumo de CPU, etc.
- Implementación compleja.
- Vulnerabilidades asociadas a Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832).

**Alternativa 3**

En función de la alternativa 1 y 2 se llega a la solución más apropiada.

### **Firewalls de Nueva Generación Palo Alto:**

Se maneja como tercera alternativa la implementación de dos firewalls Palo Alto en HA.



**Figura 5: Firewall Palo Alto Modelo PA-3250. Fuente: Anexo 1.**

### **Ventajas:**

- Es una marca reconocida caracterizada por ser uno de los líderes del sector en el Cuadrante Mágico de Gartner (Fuente: Anexo 2).
- Brinda flexibilidad en el rendimiento y redundancia (alta disponibilidad) y en el diseño de una arquitectura de red de seguridad que ayuda a proteger la organización a través de visibilidad de logs, controles avanzados de aplicaciones (App-ID), usuarios y contenido.
- Permite la detección de amenazas avanzadas y filtrado de URL.
- Permite la protección ante ataques DoS y DDoS.
- Permite la sincronización con el directorio activo de una empresa y asociar una política de seguridad en base al ID del usuario y ya no solamente a su dirección IP.
- Permite implementar políticas HIP VPN el cual identifica el terminal del usuario a través de sus características y permite aplicar políticas de seguridad de acceso y bloqueo a la entidad: Tipo de antivirus, tipo de

sistema operativo, dirección ip, firewall local, intervalo de tiempo de acceso. Además, se puede brindar un mensaje customizado al usuario.

- Permite un reporte detallado por usuario a nivel de consumo de ancho de banda (QoS).
- Tiene un módulo de detección de amenazas avanzadas a nivel de archivos (Wildfire).

### **3.7 Configuración de la Solución:**

#### **3.7.1 Topología de Red Propuesta:**

A continuación, observamos la siguiente topología de red propuesta dividida en las siguientes zonas de disponibilidad:

- Zona WAN: En esta zona encontramos los routers que permiten la conectividad hacia internet en modo activo – pasivo.
- Zona Perimetral: En esta zona encontramos los firewalls perimetrales activo y pasivo que son el nexo entre la zona wan y la zona lan.
- Zona LAN: En esta zona encontramos un switch capa 3 que permite disponer de varias subredes y ser el nexo entre la zona perimetral y las computadoras de los usuarios finales.
- Zona DMZ: También conocida como zona desmilitarizada, es aquella donde se encuentra el switch que permite la conexión entre la zona perimetral y los servidores de la organización.

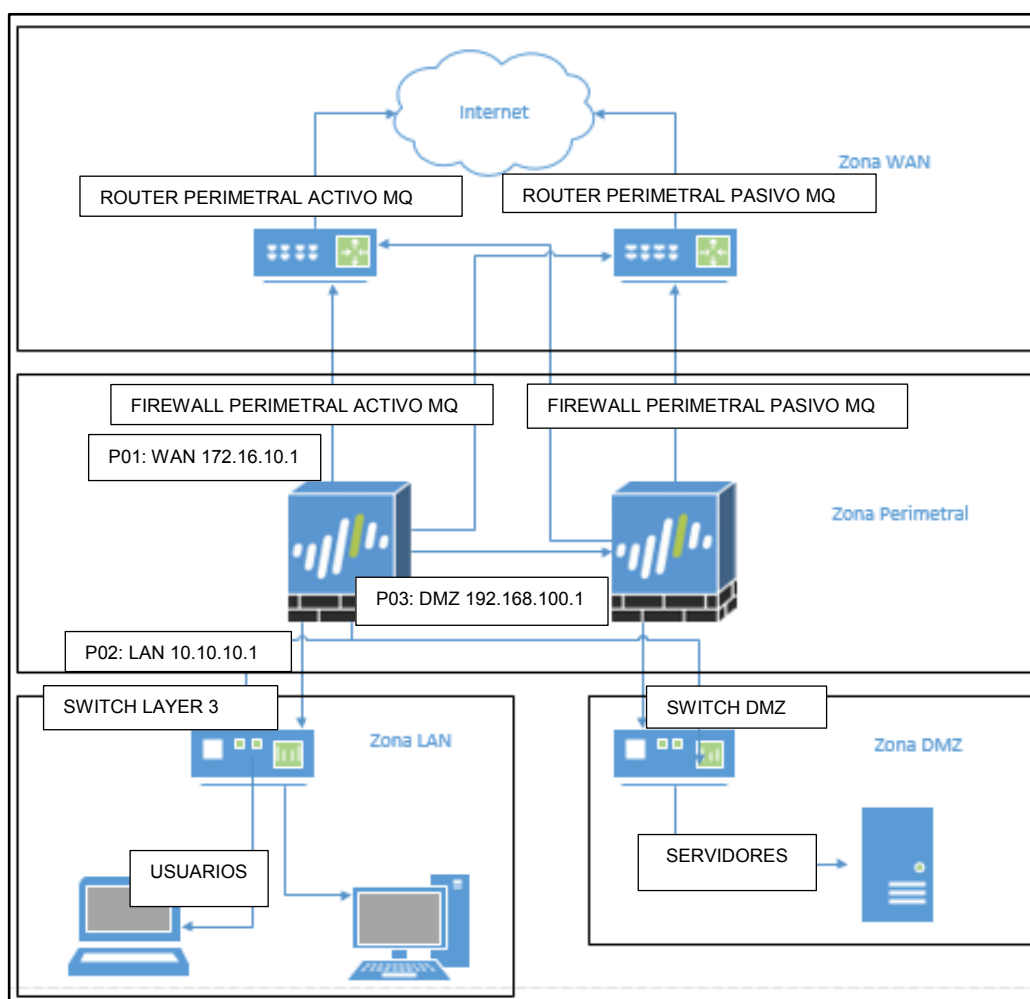


**Figura 6: Topología de Red Propuesta. Fuente: Elaboración Propia**

### 3.7.2 Configuración Interna de los Equipos:

A continuación, se describirán las configuraciones de los equipos de manera descriptiva y técnicas.

Configuración de las Interfaces de administración: Para poder administrar los firewalls perimetrales primario y secundario, se debe configurar una dirección IP de gestión las cuales se muestran en la siguiente tabla:

**Tabla 2: Configuración Interna de los Equipos**

| Firewall              | IP de Gestión |
|-----------------------|---------------|
| Perimetral Primario   | 192.168.10.10 |
| Perimetral Secundario | 192.168.10.20 |

Fuente: Elaboración Propia

Esto le servirá al administrador de tecnología de la información el acceso hacia los equipos.

Además se recomienda la habilitación de los siguientes servicios:

- Ping: Para validaciones a nivel de conectividad y disponibilidad de los equipos.
- Https: Para validaciones a nivel de acceso seguro a la interface gráfica de los equipos.
- Ssh: Para validaciones a nivel de acceso seguro a la interface de consola (cli) de los equipos.

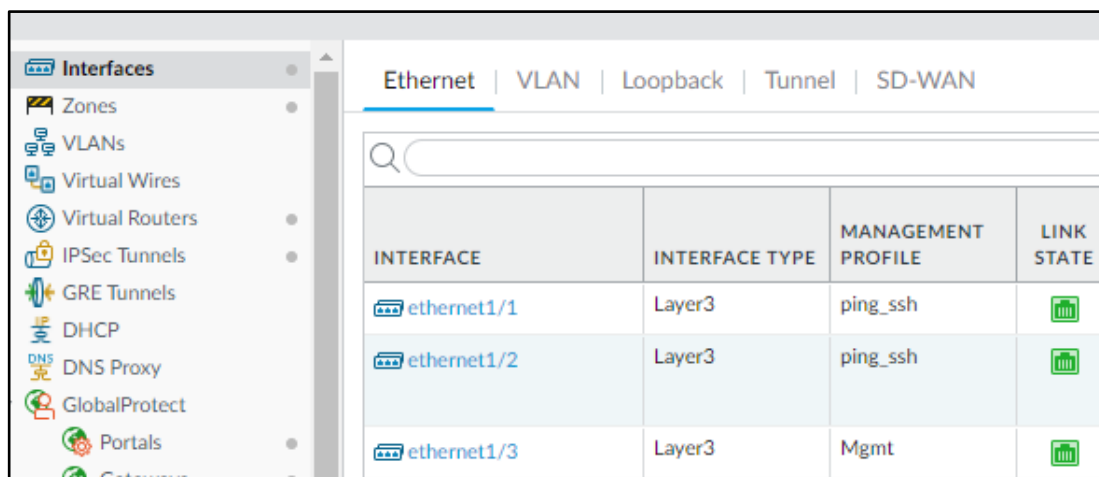
| Administrative Management Services |                                           |
|------------------------------------|-------------------------------------------|
| <input type="checkbox"/> HTTP      | <input checked="" type="checkbox"/> HTTPS |
| <input type="checkbox"/> Telnet    | <input checked="" type="checkbox"/> SSH   |

| Network Services                                     |                                                      |
|------------------------------------------------------|------------------------------------------------------|
| <input type="checkbox"/> HTTP OCSP                   | <input checked="" type="checkbox"/> Ping             |
| <input type="checkbox"/> SNMP                        | <input type="checkbox"/> User-ID                     |
| <input type="checkbox"/> User-ID Syslog Listener-SSL | <input type="checkbox"/> User-ID Syslog Listener-UDP |

**Figura 7: Servicios a habilitar para las interfaces de administración.**  
Fuente: Elaboración Propia

A continuación, se muestra la forma de visualización de la configuración de las interfaces desde la interface gráfica del equipo:



| Ethernet   VLAN   Loopback   Tunnel   SD-WAN |                |                    |            |
|----------------------------------------------|----------------|--------------------|------------|
| INTERFACE                                    | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE |
| ethernet1/1                                  | Layer3         | ping_ssh           |            |
| ethernet1/2                                  | Layer3         | ping_ssh           |            |
| ethernet1/3                                  | Layer3         | Mgmt               |            |

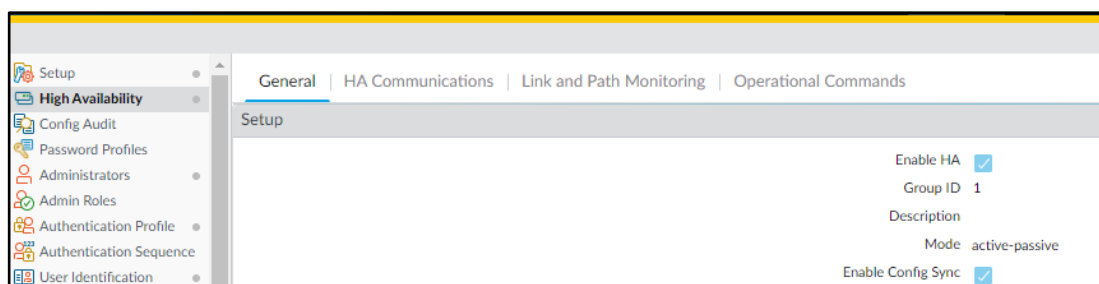
**Figura 8: Configuración de las Interfaces. Fuente: Elaboración propia**

Asimismo, se muestran los enlaces a configurar para el acceso a internet:

|                          | NAME           | TYPE   | INTERFACES / VIRTUAL SYSTEMS |
|--------------------------|----------------|--------|------------------------------|
| <input type="checkbox"/> | WAN-Claro      | layer3 | ethernet1/1                  |
| <input type="checkbox"/> | WAN_Telefonica | layer3 | ethernet1/2                  |

**Figura 9: Configuración de enlaces WAN. Fuente: Elaboración Propia**

Y también las configuraciones de Alta disponibilidad que deben poseer los firewalls perimetrales:



| General   HA Communications   Link and Path Monitoring   Operational Commands |                                     |
|-------------------------------------------------------------------------------|-------------------------------------|
| Setup                                                                         |                                     |
| Enable HA                                                                     | <input checked="" type="checkbox"/> |
| Group ID                                                                      | 1                                   |
| Description                                                                   |                                     |
| Mode                                                                          | active-passive                      |
| Enable Config Sync                                                            | <input checked="" type="checkbox"/> |

**Figura 10: Configuración de HA. Fuente: Elaboración Propia**

Arquitectura Final de Red:

Posterior a la configuración de los puertos, se evidencia la arquitectura de red sobre la cual la configuración anteriormente descrita soporta:

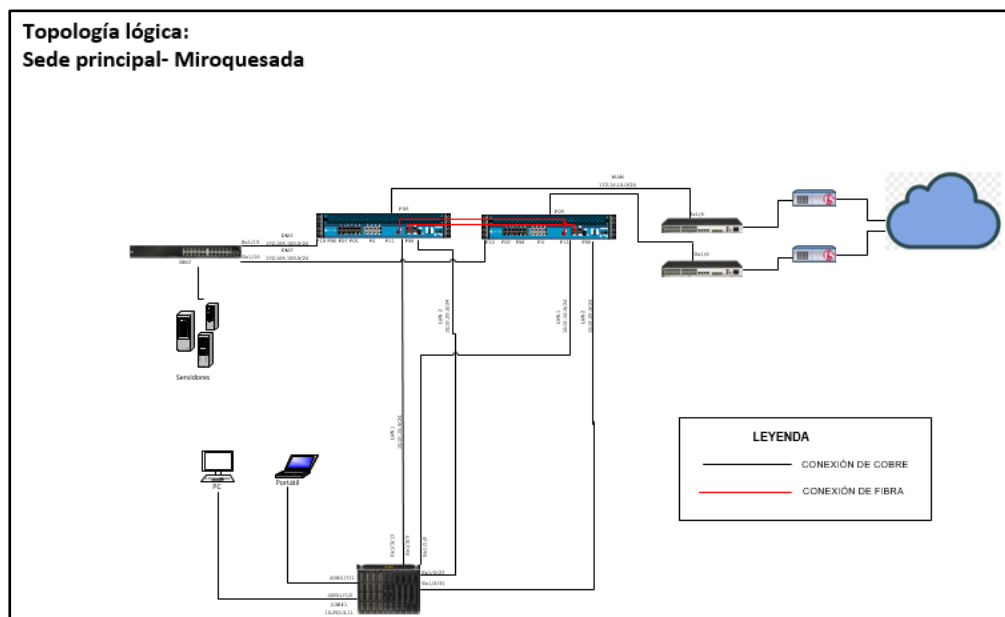


**Figura 11: Topología Final Sede Principal. Fuente: Elaboración Propia**

Configuración de las Políticas de Seguridad:

En el firewall Palo Alto también se integran listas dinámicas de direcciones IP's.

- Palo Alto Networks - Bulletproof IP addresses: Listas dinámicas de IP's que se relacionan a los servicios de infraestructura en donde se alojan servicios de internet tales como juegos de azar, spam, información errónea, etc.
- Palo Alto Networks - High risk IP addresses: Listas dinámicas de IP's que usan los ciberdelincuentes para la distribución de malware y campañas maliciosas.
- Palo Alto Networks - Known malicious IP addresses: Listas dinámicas de IP's que son consideradas maliciosas en internet.
- Estas deben ser configuradas de la siguiente forma:

- En el origen: Para que las aplicativos o servicios alojados en los servidores de la organización mateados para el acceso público sean protegidos por cibercriminales.
- En el destino: Para que el acceso de los usuarios internos a destinos maliciosos sean bloqueados.

| NAME                       | TAGS | TYPE      | ZONE      | ADDRESS     | USER | DEVI... | ZONE      | ADDRESS     |
|----------------------------|------|-----------|-----------|-------------|------|---------|-----------|-------------|
| 3 Block_Recommendation_PA  | Bloq | universal | WAN-Claro | Blac_List_1 | any  | any     | any       | any         |
| 4 Block_Recommendations_PA | Bloq | universal | any       | any         | any  | any     | WAN-Claro | Blac_List_1 |

**Figura 12: Políticas de Seguridad. Fuente: Elaboración Propia**

### Perfiles de Seguridad:

El firewall admite actualizaciones automáticas para todos los módulos de seguridad, para esto, el equipo debe seguir las siguientes recomendaciones:

- Antivirus: Se debe de actualizar cada hora como mínimo.
- Aplicaciones y amenazas: Se debe de actualizar cada 30 minutos como mínimo.
- Wildfire: Se debe de sincronizar en tiempo real.

| Antivirus                |                                 | Last checked: 2020/12/20 05:04:13 -05 | Schedule: Every hour at 4 minutes past the hour (Download and Install, sync-to-peer)        |        |                         |              |   |                 |               |   |
|--------------------------|---------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------|--------|-------------------------|--------------|---|-----------------|---------------|---|
| 3560-4071                | panupv2-all-antivirus-3560-4071 |                                       | Full                                                                                        | 94 MB  | 2020/12/12 07:01:22 -05 |              |   | Download        | Release Notes |   |
| 3561-4072                | panupv2-all-antivirus-3561-4072 |                                       | Full                                                                                        | 95 MB  | 2020/12/13 07:04:59 -05 |              |   | Download        | Release Notes |   |
| 3562-4073                | panupv2-all-antivirus-3562-4073 |                                       | Full                                                                                        | 95 MB  | 2020/12/14 07:01:27 -05 |              |   | Download        | Release Notes |   |
| 3563-4074                | panupv2-all-antivirus-3563-4074 |                                       | Full                                                                                        | 96 MB  | 2020/12/15 07:00:45 -05 |              |   | Download        | Release Notes |   |
| 3565-4076                | panupv2-all-antivirus-3565-4076 |                                       | Full                                                                                        | 100 MB | 2020/12/16 07:03:58 -05 |              |   | Download        | Release Notes |   |
| 3566-4077                | panupv2-all-antivirus-3566-4077 |                                       | Full                                                                                        | 105 MB | 2020/12/17 07:03:04 -05 |              |   | Download        | Release Notes |   |
| 3567-4078                | panupv2-all-antivirus-3567-4078 |                                       | Full                                                                                        | 105 MB | 2020/12/18 07:03:04 -05 | ✓ previously |   | Revert          | Release Notes | ✗ |
| 3568-4079                | panupv2-all-antivirus-3568-4079 |                                       | Full                                                                                        | 105 MB | 2020/12/19 07:01:03 -05 | ✓            | ✓ |                 | Release Notes | ✗ |
| Applications and Threats |                                 | Last checked: 2020/12/20 05:34:05 -05 | Schedule: Every 30 minutes at 4 minutes past half-hour (Download and Install, sync-to-peer) |        |                         |              |   |                 |               |   |
| 8347-6424                | panupv2-all-contents-8347-6424  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/11/20 13:23:53 -05 |              |   | Download        | Release Notes |   |
| 8348-6427                | panupv2-all-contents-8348-6427  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/11/24 20:11:39 -05 |              |   | Download        | Release Notes |   |
| 8349-6435                | panupv2-all-contents-8349-6435  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/01 19:27:03 -05 |              |   | Download        | Release Notes |   |
| 8350-6438                | panupv2-all-contents-8350-6438  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/03 19:20:20 -05 |              |   | Download        | Release Notes |   |
| 8351-6445                | panupv2-all-contents-8351-6445  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/08 14:17:41 -05 |              |   | Download        | Release Notes |   |
| 8352-6446                | panupv2-all-contents-8352-6446  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/09 14:59:35 -05 |              |   | Download        | Release Notes |   |
| 8353-6449                | panupv2-all-contents-8353-6449  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/10 20:34:54 -05 |              |   | Download        | Release Notes |   |
| 8354-6456                | panupv2-all-contents-8354-6456  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/14 21:31:49 -05 |              |   | Download        | Release Notes |   |
| 8355-6462                | panupv2-all-contents-8355-6462  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/17 17:32:21 -05 | ✓ previously |   | Revert          | Release Notes | ✗ |
| 8356-6464                | panupv2-all-contents-8356-6464  | Apps, Threats                         | Full                                                                                        | 57 MB  | 2020/12/17 21:25:18 -05 | ✓            | ✓ | Review Policies | Release Notes | ✗ |

**Figura 13: Actualizaciones automáticas de los equipos para los perfiles de seguridad. Fuente: Elaboración Propia**

Cada perfil de seguridad se debe configurar de la siguiente forma:

- Perfil de Seguridad de Antivirus: En este perfil podemos bloquear la ejecución de virus en la red. Se recomienda resetear la comunicación en los servicios críticos como http, ftp y smb.

External Dynamic Lists

Custom Objects

Data Patterns

Spyware

Vulnerability

URL Category

Security Profiles

Antivirus

Anti-Spyware

Vulnerability Protection

URL Filtering

File Blocking

WildFire Analysis

Data Filtering

DoS Protection

Security Profile Groups

Log Forwarding

Authentication

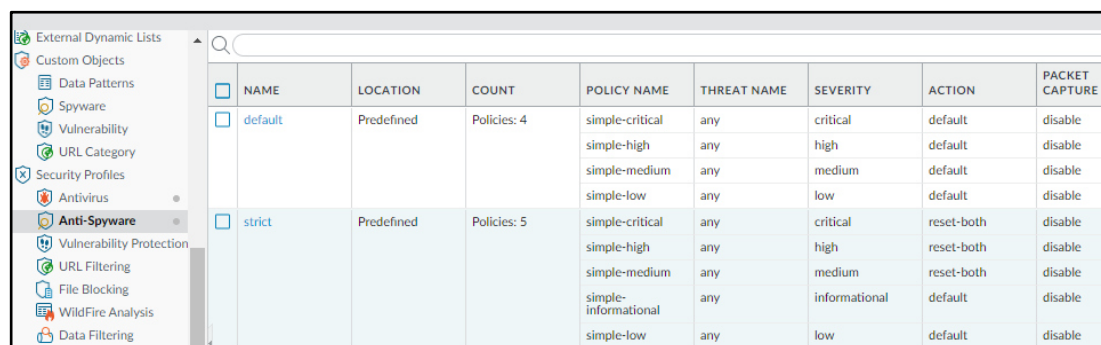
Decryption

Decryption Profile

|                          | NAME    | LOCATION   | PACKET CAPTURE           | Decoders |                      |                           |                           | Application Exceptions |        | WildFire Inline ML       |                                       |
|--------------------------|---------|------------|--------------------------|----------|----------------------|---------------------------|---------------------------|------------------------|--------|--------------------------|---------------------------------------|
|                          |         |            |                          | PROTOCOL | SIGNATURE ACTION     | WILDFIRE SIGNATURE ACTION | WILDFIRE INLINE ML ACTION | APPLICATION            | ACTION | MODEL                    | ACTION SETTING                        |
| <input type="checkbox"/> | default | Predefined | <input type="checkbox"/> | http     | default (reset-both) | default (reset-both)      | default (reset-both)      |                        |        | Windows Executables      | enable (inherit per-protocol actions) |
|                          |         |            |                          | http2    | default (reset-both) | default (reset-both)      | default (reset-both)      |                        |        | PowerShell Script 1      | enable (inherit per-protocol actions) |
|                          |         |            |                          | smtp     | default (alert)      | default (alert)           | default (alert)           |                        |        | PowerShell Script 2      | enable (inherit per-protocol actions) |
|                          |         |            |                          | imap     | default (alert)      | default (alert)           | default (alert)           |                        |        | Executable Linked Format | enable (inherit per-protocol actions) |
|                          |         |            |                          | pop3     | default (alert)      | default (alert)           | default (alert)           |                        |        | MSOffice                 | enable (inherit per-protocol actions) |
|                          |         |            |                          | ftp      | default (reset-both) | default (reset-both)      | default (reset-both)      |                        |        | Shell                    | enable (inherit per-protocol actions) |
|                          |         |            |                          | smb      | default (reset-both) | default (reset-both)      | default (reset-both)      |                        |        |                          |                                       |

**Figura 14: Perfil de Seguridad de Antivirus. Fuente: Elaboración Propia**

- Perfil de Seguridad de Antispyware: En este perfil podemos identificar la acción a realizar en la comunicación ante amenazas de tipo spyware. Se recomienda resetear la comunicación de los servicios críticos, altos y medios.



| NAME    | LOCATION   | COUNT       | POLICY NAME          | THREAT NAME | SEVERITY      | ACTION     | PACKET CAPTURE |
|---------|------------|-------------|----------------------|-------------|---------------|------------|----------------|
| default | Predefined | Policies: 4 | simple-critical      | any         | critical      | default    | disable        |
|         |            |             | simple-high          | any         | high          | default    | disable        |
|         |            |             | simple-medium        | any         | medium        | default    | disable        |
|         |            |             | simple-low           | any         | low           | default    | disable        |
| strict  | Predefined | Policies: 5 | simple-critical      | any         | critical      | reset-both | disable        |
|         |            |             | simple-high          | any         | high          | reset-both | disable        |
|         |            |             | simple-medium        | any         | medium        | reset-both | disable        |
|         |            |             | simple-informational | any         | informational | default    | disable        |
|         |            |             | simple-low           | any         | low           | default    | disable        |

**Figura 15: Perfil de Seguridad de Antispyware. Fuente: Elaboración Propia**

- Perfil de Seguridad de Filtrado de URL: En este perfil podemos verificar las categorías que existen para las url's o sitios web que existen en internet. Se recomienda realizar el bloqueo de aquellas categorías que no estén relacionadas con contenido malicioso u ofensivo.

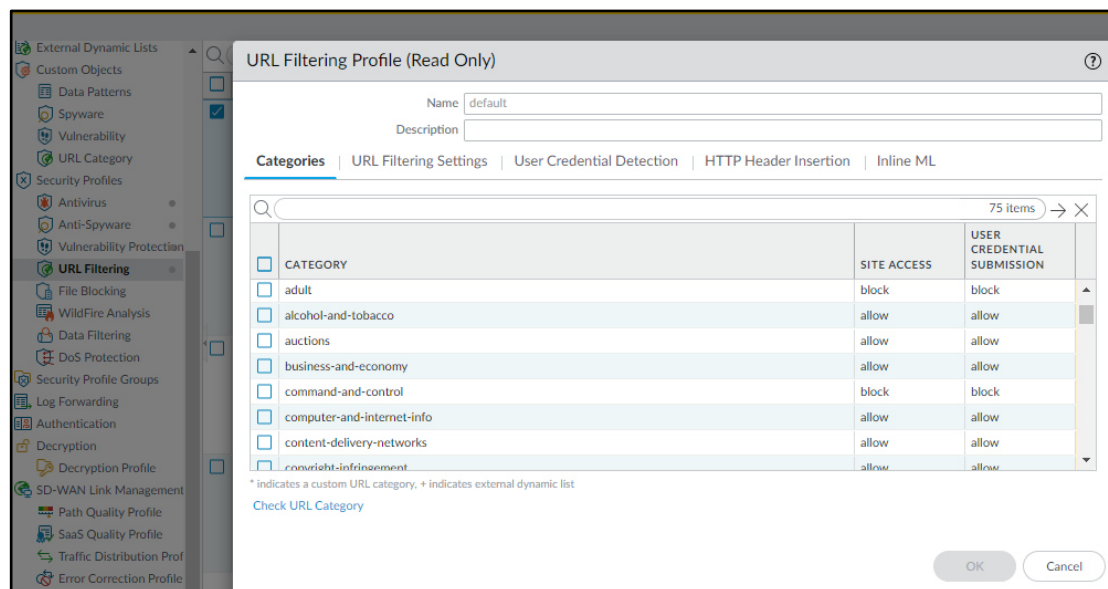


**Figura 16: Perfil de Seguridad de Filtrado de URL. Fuente: Elaboración Propia**

Además, el filtrado de URL también admite listas negras que se pueden customizar.

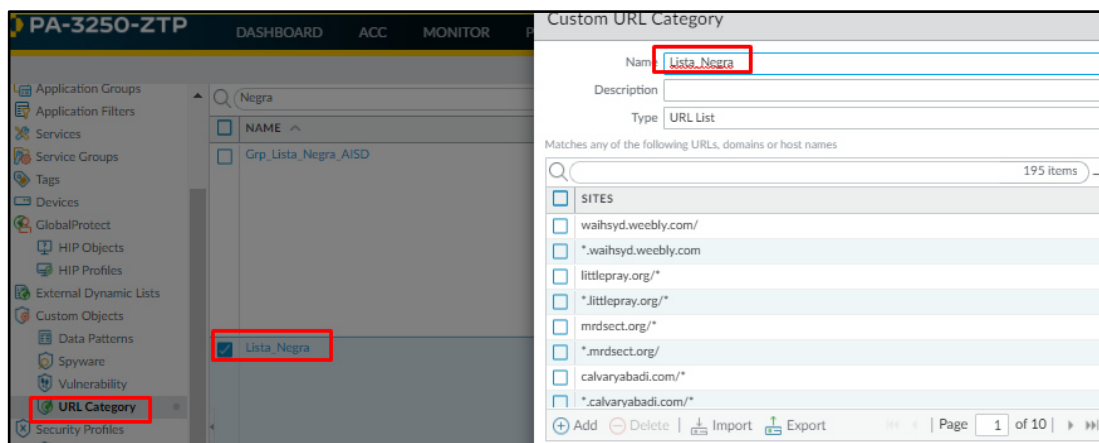


**Figura 17: Bloqueo Customizado por categoría de URL. Fuente: Elaboración Propia**

- Perfil de Seguridad de DLP: En este perfil podemos monitorear y proteger la carga y descarga de aquellos archivos que contienen software malicioso. Además de bloquear aquellos tipos de archivos encriptados. Se recomienda bloquear los siguientes tipos de archivos de manera bidireccional: 7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, multi level encoding, ocs, pe, pif, rar, scr, tar, torrent, vbe, wsf.

| NAME                                                     | LOCATION   | RULE NAME                       | APPLICATIONS | FILE TYPES                                                                                                                               | DIRECTION | ACTION   |
|----------------------------------------------------------|------------|---------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------|
| <input type="checkbox"/> basic file blocking             | Predefined | Block high risk file types      | any          | 7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocs, PE, pif, rar, scr, torrent, vbe, wsf                                             | both      | block    |
|                                                          |            | Continue prompt encrypted files | any          | encrypted-rar, encrypted-zip                                                                                                             | both      | continue |
|                                                          |            | Log all other file types        | any          | any                                                                                                                                      | both      | alert    |
| <input checked="" type="checkbox"/> strict file blocking | Predefined | Block all risky file types      | any          | 7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocs, PE, pif, rar, scr, tar, torrent, vbe, wsf | both      | block    |
|                                                          |            | Block encrypted files           | any          | encrypted-rar, encrypted-zip                                                                                                             | both      | block    |
|                                                          |            | Log all other file types        | any          | any                                                                                                                                      | both      | alert    |

**Figura 18: Perfil de Seguridad de DLP. Fuente: Elaboración Propia**

- Perfil de Seguridad de Sandboxing (Wildfire): En este perfil podemos bloquear de manera bidireccional el comportamiento malicioso en la red y usar la nube de Palo Alto para realizar el análisis en tiempo real.

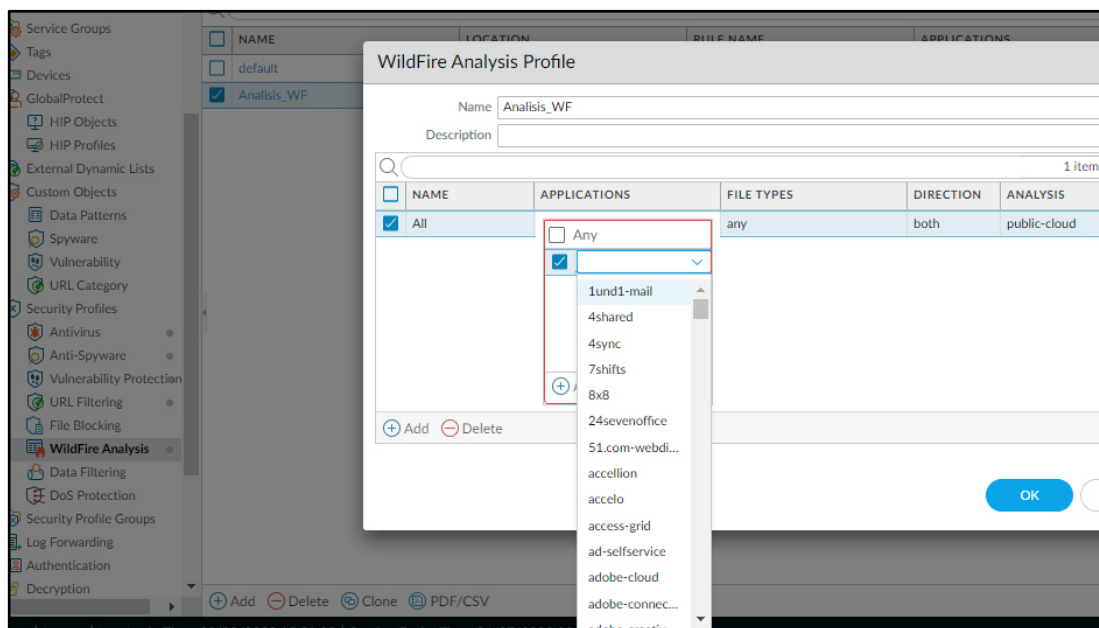


**Figura 19: Perfil de Seguridad de Sandboxing (Wildfire). Fuente: Elaboración Propia**

Módulo de aplicaciones:

En ese sentido, el firewall también tiene configurado un módulo de aplicaciones los cuales vienen de forma predeterminada, por ejemplo, podemos mencionar facebook, whatsapp, linkedin, etc; categorizados de acuerdo a su uso.

Addresses

Address Groups

Regions

Dynamic User Groups

Applications

Application Groups

Application Filters

Services

Service Groups

Tags

Devices

GlobalProtect

HIP Objects

HIP Profiles

External Dynamic Lists

Custom Objects

Data Patterns

Spyware

Vulnerability

URL Category

Security Profiles

Antivirus

Anti-Spyware

Vulnerability Protection

Search

Q

All

Clear Filters

| CATEGORY ^            | SUBCATEGORY ^          | RISK   | TAGS ^               | CHARACTERISTIC ^         |
|-----------------------|------------------------|--------|----------------------|--------------------------|
| 1682 business-systems | 54 audio-streaming     | 2069 1 | 2 Deleting           | 36 Data Breaches         |
| 452 collaboration     | 25 auth-service        | 1002 2 | 15 DLP App Exclusion | 645 Evasive              |
| 358 general-internet  | 5 content-management   | 572 3  | 77 Downloading       | 668 Excessive Bandwidth  |
| 332 media             | 3 customer-service     | 367 4  | 50 Editing           | 52 FEDRAMP               |
| 503 networking        | 41 database            | 143 5  | 27 eLearning         | 3 FINRA                  |
| 824 saas              | 2 design               |        |                      | 117 HIPAA                |
| 2 unknown             | 90 email               |        |                      | 87 IP Based Restrictions |
|                       | 74 encrypted-transport |        |                      | 73 Known IPs             |

| NAME                                                    | CATEGORY         | SUBCATEGORY   | RISK | TAGS | STANDARD PORTS      |
|---------------------------------------------------------|------------------|---------------|------|------|---------------------|
| <input type="checkbox"/> 100bao                         | general-internet | file-sharing  | 5    |      | tcp/3468,6346,11300 |
| <input type="checkbox"/> 1ec-60870-5-104                |                  |               |      |      |                     |
| <input type="checkbox"/> 104apci-supervisory            | business-systems | ics-protocols | 2    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered             | business-systems | ics-protocols | 2    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-startdt-act | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-startdt-con | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-stopdt-act  | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-stopdt-con  | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-test-act    | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104apci-unnumbered-test-con    | business-systems | ics-protocols | 1    |      | tcp/2404            |
| <input type="checkbox"/> 104asdu-file-transfer          | business-systems | management    | 3    |      | tcp/2404            |

**Figura 20: Suite de Aplicaciones. Fuente: Elaboración Propia**

### Proceso de Backup:

Se recomienda realizar el backup de los equipos y almacenar la información de manera segura.

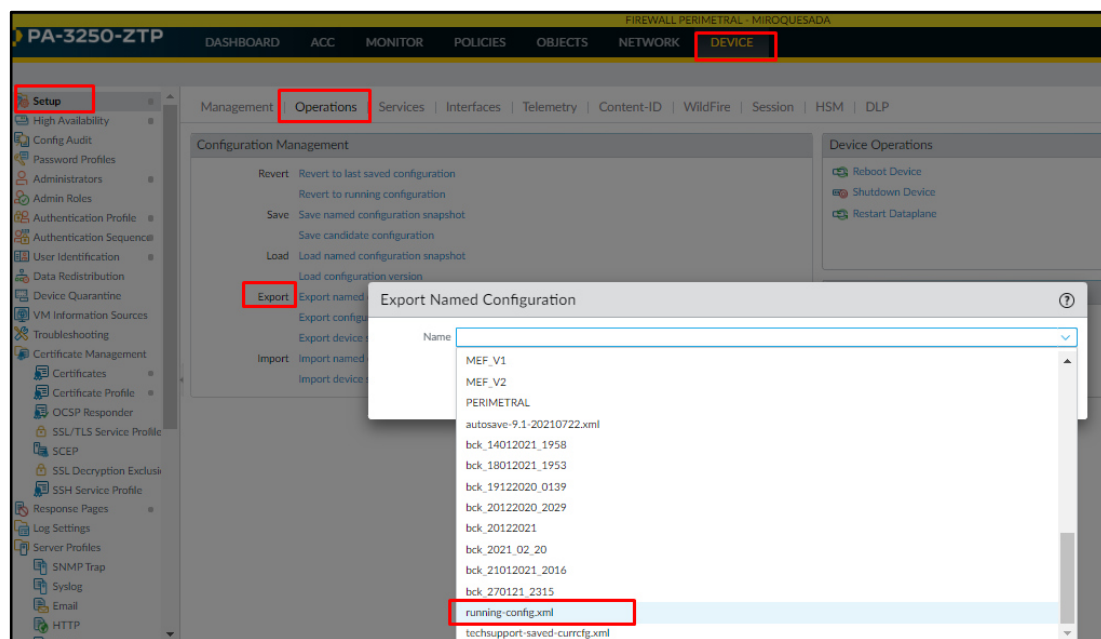


**Figura 21: Running Configuration – Backup. Fuente: Elaboración Propia**

### Generación de Informes:

Se puede generar informes para auditoría de ser necesario, por ejemplo: análisis de navegación de los usuarios en un determinado lapso de tiempo, cantidad de logs, uso de recursos, etc.

En la siguiente imagen podremos ver un ejemplo de generación de informe de tiempo de acceso VPN evidenciando el nombre del usuario, día, sistema operativo de la máquina y duración de la sesión.

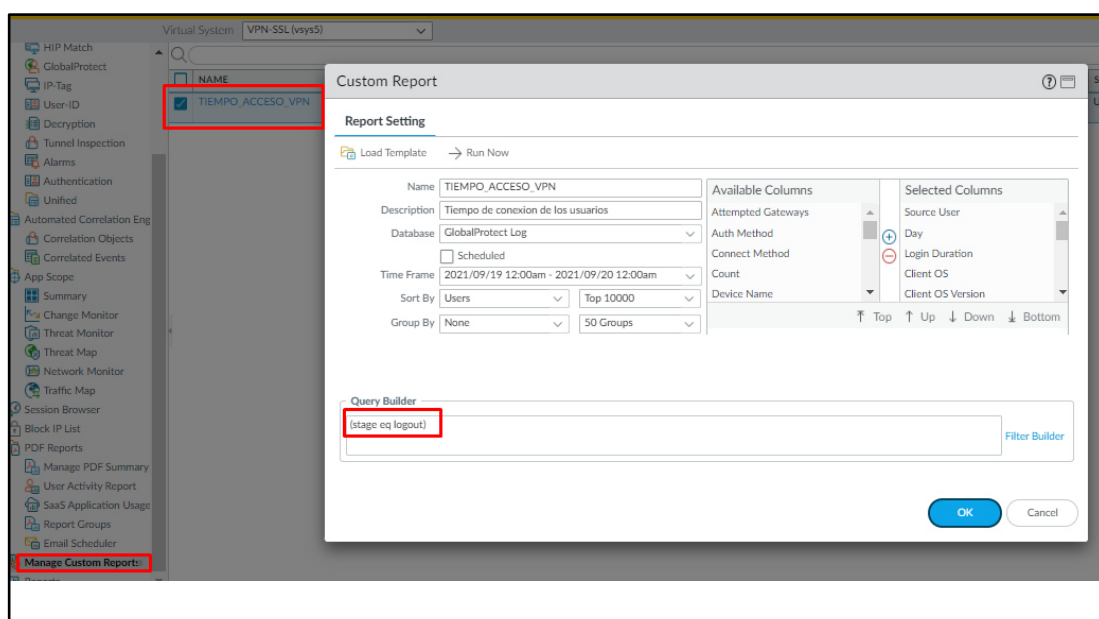


**Figura 22: Filtrado de Informes. Fuente: Elaboración Propia**

## CAPITULO IV: CONCLUSIONES

### 4.1 Justificación

El presente diseño de arquitectura en donde se ha contemplado el uso de un sistema de alta disponibilidad, permite la mejora en la seguridad de la información en la entidad del estado debido a que se cubre la continuidad del negocio en caso de emergencias, además trae consigo diversos módulos de protección que permiten resguardar los sistemas digitales de la entidad.

#### 4.1.1 Evaluación Económica

**Tabla 3: Estimación de Costos.**

| Código                    | Descripción                                                     | Cantidad | Costo Unitario | Subtotal      |
|---------------------------|-----------------------------------------------------------------|----------|----------------|---------------|
| PAN-PA-3250               | NGFW Palo Alto Networks PA-3250                                 | 2        | \$ 26,300.00   | \$ 52,600.00  |
| PAN-PA-3250-TP-3YR-HA2    | Subscripción Threat prevention NGFW PA-3250                     | 2        | \$ 9,300.00    | \$ 18,600.00  |
| PAN-PA-3250-URL4-3YR-HA2  | Subscripción PANDB URL filtering NGFW PA-3250                   | 2        | \$ 9,300.00    | \$ 18,600.00  |
| PAN-PA-3250-WF-3YR-HA2    | Subscripción WildFire NGFW PA-3250                              | 2        | \$ 9,300.00    | \$ 18,600.00  |
| PAN-PA-3250-SDWAN-3YR-HA2 | Subscripción SD-WAN NGFW PA-3250                                | 2        | \$ 9,300.00    | \$ 18,600.00  |
| PAN-SVC-PREM-3250-3YR     | Premium support NGFW PA-3250                                    | 2        | \$ 11,400.00   | \$ 22,800.00  |
| PAN-SFP-PLUS-SR           | 10Gb SFP+ optical transceiver                                   | 16       | \$ 1,500.00    | \$ 24,000.00  |
| PAN-SFP-PLUS-CU-5M        | 10Gb SFP+ cable de conexión directa + 2 transceiver ensamblados | 1        | \$ 500.00      | \$ 500.00     |
| PAN-PA-2RU-RACK4          | 4 post rack mount kit NGFW PA-3250                              | 2        | \$ 150.00      | \$ 300.00     |
|                           |                                                                 |          | <b>Total</b>   | \$ 174,600.00 |

Fuente: Anexo 3.

### 4.2 Descripción del diseño

El diseño se ha basado en las mejores prácticas para la configuración de los firewalls de nueva generación en donde hemos hablado de la alta

disponibilidad, políticas de seguridad, perfiles de antivirus, perfiles para aplicaciones, escaneo de amenazas, análisis en tiempo real, filtrado y categorización de sitios web que permiten la visibilidad de todo aquello que está pasando en la red de la organización.

Por ejemplo, el firewall de nueva generación teniendo los perfiles de IPS/IDS para bloquear firmas maliciosas reduce significativamente la exposición de los datos y permite la prevención de pérdidas y/o afectar directamente sobre el financiamiento de un proyecto en caso haya algún tipo de exposición de data a través de los servicios alojados en los distintos servidores de la entidad.

Además, se ha contemplado la gestión de los equipos a través de protocolos seguros y se ha brindado diversas sugerencias para la optimización de los recursos.

### **4.3 Conclusiones**

- Se logró hacer el diseño, mejorando los niveles de seguridad de la información de la entidad del estado al tener proponer un sistema de alta redundancia que permite la confidencialidad, disponibilidad e integridad de los datos, además de brindar las mejores prácticas recomendadas por el mismo fabricante para el uso correcto del firewall de nueva generación.
- Se evaluó la situación actual de la seguridad informática de la entidad tanto en el sustento teórico como en el sustento práctico dando a conocer los equipos implementados previo al diseño de la solución como los es el firewall con un sistema open source.
- Se mostró las ventajas de los firewalls de nueva generación y se hizo la evaluación comparativa de las principales marcas que existen en el mercado tales como Juniper, Forcepoint y Palo Alto.
- Se elaboró la topología de red diseñada para el presente trabajo, además se brindó el detalle técnico clasificándose en: Características Generales de Seguridad, Características Funcionales, Características de Red y Conectividad. Finalmente, se brindó la fuente de cada una de las

capacidades de las soluciones, asimismo se tiene el sustento económico que se evidencia en la bibliografía del presente trabajo.

## **CAPITULO V: RECOMENDACIONES**

- Concientizar al personal de Tecnologías de la Información de la entidad sobre las mejoras que trae consigo la implementación de firewalls de nueva generación.
- Tomar en consideración el presente trabajo para aprovechar las características técnicas y/o económicas en la implementación de firewalls de nueva generación.
- Tener un proceso de backup constante de los firewalls de nueva generación y de los activos que almacenan información sensible de la organización.
- Realizar actualizaciones de software y parches de seguridad sobre la plataforma que permiten el buen desempeño de los equipos.
- Aprovechar la generación de los informes que te brindan los firewalls de nueva generación mostrados para la corrección sobre los activos de la entidad y realizar medidas mitigadoras.
- Evaluar el uso de firewalls de nueva generación internos para la visibilidad de la comunicación entre activos en una misma red.

## CAPITULO VI: BIBLIOGRAFIA

Berta de Moragas J. y Pascual C. (2019). Las tecnologías de Internet, un riesgo para empresas y ciudadanos. Obtenido de <https://upcommons.upc.edu/bitstream/handle/2117/167007/memoria.pdf?sequence=1&isAllowed=y>

Cajahuaringa J. (2020). Implementación de firewall para el control de servicio de internet en la filial Chanchamayo de la Universidad Peruana Los Andes. Obtenido de [https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1711/T\\_03770061687.pdf?sequence=1&isAllowed=y](https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1711/T_03770061687.pdf?sequence=1&isAllowed=y)

Campomanes (2021). Diseño e implementación de firewall palo alto para mejorar el control de seguridad y acceso a internet. Obtenido de [https://alicia.concytec.gob.pe/vufind/Record/UUPN\\_685d1009d4c4e9f2777e1dbb5e777cb6](https://alicia.concytec.gob.pe/vufind/Record/UUPN_685d1009d4c4e9f2777e1dbb5e777cb6)

Congreso de la República (2011) Ley de Protección de Datos Personales Nro 29733. Obtenido de <https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779>

Cossio A. (2021) La Ciberseguridad de la Información del empleador y la fiscalización del trabajo remoto: Alcances y Límites. Obtenido de <https://rubio.pe/wp-content/uploads/2021/04/12-1.pdf>

Coy (2020) Guía rápida para la adquisición de firewall de nueva generación en entidad bancaria estatal. Obtenido de

<https://repository.ucatolica.edu.co/entities/publication/a64cc5cc-85e4-4cc6-b68f-1c718faafc97>

ESET (2022) ESET Security Report: Latinoamérica. Obtenido de <https://www.welivesecurity.com/wp-content/uploads/2022/10/ESET-security-report-LATAM2022.pdf>

Forcepoint (2023) NGFW Models. Obtenido de <https://www.forcepoint.com/appliance/forcepoint-ngfw-appliances>

Forcepoint (2022) Apache log4j2.x multiple vulnerabilities for Forcepoint NGFW Security Management Center. Obtenido de <https://support.forcepoint.com/s/article/CVE-2021-44228-Java-log4j-vulnerability-mitigation-with-NGFW-Security-Management-Center>

ISACA (2017) Guía de Estudio de Fundamentos de Ciberseguridad (Segunda Edición). Obtenido de <https://engage.isaca.org/home>

Juniper Networks (2020) How to block Telnet and SSH Brute Force log-in attacks. Obtenido de [https://supportportal.juniper.net/s/article/SRX-How-to-block-Telnet-and-SSH-Brute-Force-log-in-attacks?language=en\\_US](https://supportportal.juniper.net/s/article/SRX-How-to-block-Telnet-and-SSH-Brute-Force-log-in-attacks?language=en_US)

Palo Alto (2023) PA-3200 Series Datasheet. Obtenido de <https://www.paloaltonetworks.com/resources/datasheets/pa-3200-series>

Palo Alto (2019) Uso de Listas Dinámicas. Obtenido de <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PM0pCAG>

Palo Alto (2016) Descripción General del Firewall: Obtenido de [https://www.paloaltonetworks.lat/apps/pan/public/downloadResource?pagePath=/content/pan/es\\_LA/resources/datasheets/descripcion-del-firewall](https://www.paloaltonetworks.lat/apps/pan/public/downloadResource?pagePath=/content/pan/es_LA/resources/datasheets/descripcion-del-firewall)

Palo Alto Price List (2023). Consultado el 06 de octubre del 2020.  
<https://itprice.com/paloalto-price-list/.html>

Pfsense (2016) Security Appliances. Obtenido de <https://www.telenet.ba/datasheets/products/prod217ds1.pdf>

## CAPITULO VII: ANEXOS

### Anexo 1: Ficha de Datos (Datasheet)

- Datasheet del Netgate Pfsense Modelo 7100-1U.

Netgate XG-7100 1U pfSense® Security Gateway Appliance

#### TECHNICAL SPECIFICATIONS

|              |                                                                                                                                                                                                                           |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU          | Intel Denverton C3558, 2.2 GHz                                                                                                                                                                                            |
| CPU Cores    | Four Cores                                                                                                                                                                                                                |
| Networking   | 2x 10GbE Intel x553 SFP+ Ports<br>8-port 1Gbps Marvell 88E6190 switch, uplinked at 5 Gbps (2x 2.5 Gbps) to Intel SoC for LAN<br>Virtual Machine Device Queues reduce I/O overhead<br>Note: Copper SFP/SFP+ not supported. |
| Storage      | 32GB eMMC onboard<br>Additional storage via M.2 SSD or SATA3                                                                                                                                                              |
| Memory       | 8 GB DDR4 (expandable to 24GB via SODIMM)                                                                                                                                                                                 |
| Expansion    | 1x PCI-E 3.0 x4 slot<br>1x M.2 M-Key 2280 supported<br>4x SATA3                                                                                                                                                           |
| Console Port | 1x mini-USB Console                                                                                                                                                                                                       |
| USB Ports    | 1x USB 3.0 ports<br>2x USB 2.0 ports                                                                                                                                                                                      |
| LED          | Power/Status/SATA Activity                                                                                                                                                                                                |
| Enclosure    | 19" 1U Rack Mount                                                                                                                                                                                                         |
| Form Factor  | 1U 1.75" x 19" x 8.5" 1U Rack Mount                                                                                                                                                                                       |
| Cooling      | 2x Low-noise active control chassis fans                                                                                                                                                                                  |

|                       |                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------|
| Environmental         | 0°C to 60°C Operating Temp<br>8% to 90% Operating Relative Humidity (non-condensing)                      |
| Power Consumption     | TBD                                                                                                       |
| Certifications        | FCC, CE, RoHS, REACH, IEC 60950,<br>EN55022, EN 61000-3-3, EN 61000-3-2, EN55024, CISPR 22                |
| SoC                   | Marvell Armada 3720LP (88F3720) dual core ARM Cortex A53 processor @ 1.2GHz                               |
| System Memory         | 1 GB DDR4 RAM on board                                                                                    |
| Storage               | 8 GB EMMC                                                                                                 |
| Network Interfaces    | 1x Marvell 88E6141 networking switch<br>3x GbE Ethernet (WAN/LAN/OPT)<br>1x Mini PCIe slot <sup>(a)</sup> |
| USB                   | 1x USB 3.0<br>1x USB 2.0<br>1x Micro USB port (console)                                                   |
| Misc                  | Reset button, heatsink, 3 Status LED                                                                      |
| Power                 | 12V 2A DC 5.5mm x 2.1mm x 10mm jack, center pin positive (power over USB not supported)                   |
| Power Consumption     | 3.48W (idle)                                                                                              |
| Operating Temperature | 0°C (32°F) to 45°C (113°F)                                                                                |
| Enclosure             | Plastic 110 x 84.6 x 31.75 mm (4.33" x 3.33" x 1.25")                                                     |
| Hardware Warranty     | 1-year standard. Second year available only at time of purchase.                                          |

## COMMON USE CASES

- Medium to Large Sized Networks with 1U rack mount cabinets
- Medium to Large Sized Branch Office
- Managed Service Providers (MSP) / Managed Security Service Provider (MSSP) On-Premises Appliance
- High-Speed 10 Gigabit Connections
- Multiple VPN Connections
- High speed connections with IDS/IPS functionality

## SOFTWARE FEATURES

pfSense software is a free, open source firewall and router platform that is functionally competitive with expensive, proprietary commercial firewalls. The pfSense platform can be configured as a stateful packet filtering firewall, a LAN or WAN router, VPN appliance, DHCP server, DNS server, or can be configured for other applications and special purpose appliances. This next generation pfSense security appliance features include:

- Stateful packet filtering firewall or pure router
- Routing policy per gateway and per-rule for multiple WAN, failover, load balancing
- Transparent layer 2 firewall
- Support for IPV6, NAT, BGP
- Captive portal with MAC filtering, RADIUS support, etc
- VPN: IPsec, OpenVPN, PPTP
- Dynamic DNS client
- DHCP Server and Relay functions
- PPPoE Server
- Reporting and monitoring features with real time information
- IoT gateway / security endpoint
- Network tap
- IPMI / BMC firewall
- [Learn more about the features of pfsense software](#)

- Datasheet del Firewall de Nueva Generación - JunOS Modelo SRX1500.



Driven by  
Experience

Data Sheet 



### Product Overview

The SRX1500 is a next-generation firewall and security services gateway offering outstanding protection, performance, scalability, availability, and security service integration. Designed for port density, a high-performance security services architecture, and seamless integration of networking and security in a single platform, the SRX1500 is best suited for client protection in enterprise campus, regional headquarters, or cloud-based security solutions with a focus on application visibility and control, intrusion prevention, and advanced threat protection. The SRX1500 is powered by Junos OS, the industry-leading operating system that keeps the world's largest and most mission-critical enterprise networks secure.

## SRX1500 FIREWALL DATASHEET

Next-Generation Firewall For The Distributed Enterprise

---

### Product Description

The Juniper Networks® SRX1500 is a high-performance next-generation firewall and security services gateway that protects mission-critical networks at campuses and regional headquarters. The SRX1500 provides best-in-class security and threat detection and mitigation capabilities, integrating carrier-class routing and feature-rich switching in a single platform.

The SRX1500 delivers a next-generation security solution that supports the changing needs of cloud-enabled enterprise networks. Whether rolling out new services in an enterprise campus, connecting to the cloud, complying with industry standards, or achieving operational efficiency, the SRX1500 helps organizations realize their business objectives while providing scalable, easy-to-manage, secure connectivity and advanced threat detection and mitigation capabilities. The SRX1500 protects critical corporate assets as a next-generation firewall, acts as an enforcement point for cloud-based security solutions, and provides application visibility and control to improve the user and application experience.

A combination of hardware and software architectures on the SRX1500 add significant performance improvements to a small 1 U form factor. The key to the SRX1500 hardware is the security flow accelerator, a programmable high-speed Layer 4 firewall chip, and a robust x86-based security compute engine for advanced security services like application visibility, intrusion prevention, and threat mitigation capabilities. The SRX1500 software architecture leverages these programmable hardware components and virtualization to deliver high-speed firewall performance, application visibility, and intrusion prevention while lowering total cost of ownership (TCO).

The SRX1500 is purpose-built to protect 10GbE network environments, consolidating multiple security services and networking functions in a highly available appliance. It supports up to 9.2 Gbps of firewall performance, 3.3 Gbps of intrusion prevention, and 4.5 Gbps of IPsec VPN in enterprise campus, regional headquarters, and data center deployments.

### SRX1500 Highlights

The SRX1500 delivers a full complement of next-generation firewall capabilities that use advanced application identification and classification to enable greater visibility, enforcement, control, and protection over the network. It provides a detailed analysis of application volume and usage, fine-grained application control policies to allow or deny traffic based on dynamic application name or group names, and prioritization of traffic based on application information and context.

## SRX1500 Firewall Datasheet

The SRX1500 recognizes more than 4,275 applications and nested applications in plain-text or SSL encrypted transactions. The SRX1500 also integrates with Microsoft Active Directory and combines user information with application data to provide network-wide application and user visibility and control.

For the perimeter, the SRX1500 Firewall offers a comprehensive suite of application security services, threat defenses, and intelligence services to protect networks from the latest content-borne threats. Integrated threat intelligence via Juniper Networks ATP Cloud offers adaptive threat protection against command and control (C&C)-related botnets and policy enforcement based on GeolIP. Integrating the Juniper Networks Advanced Threat Prevention Cloud solution, or working with the Juniper Networks ATP Appliance, the SRX1500 detects and enforces automated protection against known malware and zero-day threats with an extremely high degree of accuracy.

The SRX1500 enables agile SecOps through automation capabilities that support Zero Touch Deployment, Python scripts for orchestration, and event scripting for operational management.

The SRX1500 delivers fully automated SD-WAN to both enterprises and service providers. A Zero-Touch Provisioning (ZTP) capability simplifies branch network connectivity for initial deployment and ongoing management. Due to its high performance and scale, the SRX1500 acts as a VPN hub and terminates VPN/secure overlay connections in the various SD-WAN topologies.

The SRX1500 Firewall runs Juniper Networks Junos® operating system, a proven, carrier-hardened network OS that powers the top 100 service provider networks worldwide. These rigorously tested carrier-class routing features of IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments.

## Features and Benefits

| Business Requirement                          | Feature/Solution                                                                                                                                                              | SRX1500 Advantages                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>High performance</b>                       | Up to 9 Gbps of firewall performance                                                                                                                                          | <ul style="list-style-type: none"> <li>Best suited for enterprise campus and data center edge deployments</li> <li>Addresses future needs for scale and feature capacity</li> </ul>                                                                                                                                                                                                                                                          |
| <b>High quality end-user experience</b>       | Application visibility and control                                                                                                                                            | <ul style="list-style-type: none"> <li>Detects 4,275 Layer 3-7 applications, including Web 2.0</li> <li>Controls and prioritizes traffic based on application and user role</li> <li>Inspects and detects applications inside the SSL encrypted traffic</li> </ul>                                                                                                                                                                           |
| <b>Threat protection</b>                      | IPS, antivirus, anti-spam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, Threat Intelligence Feeds, and Juniper ATP Appliance | <ul style="list-style-type: none"> <li>Provides real-time updates to IPS signatures and protects against exploits</li> <li>Implements industry-leading antivirus and URL filtering</li> <li>Delivers open threat intelligence platform that integrates with third-party feeds</li> <li>Protects against zero-day attacks</li> <li>Restores visibility lost due to encryption, without the heavy burden of full TLS/SSL decryption</li> </ul> |
| <b>Professional-grade networking services</b> | Routing, switching, and secure wire                                                                                                                                           | <ul style="list-style-type: none"> <li>Supports carrier-class advanced routing, quality of service (QoS), and services</li> <li>Offers flexible deployment modes (L1/L2/L3)</li> </ul>                                                                                                                                                                                                                                                       |
| <b>Highly secure</b>                          | IPsec VPN, remote access/SSL VPN, secure boot                                                                                                                                 | <ul style="list-style-type: none"> <li>Provides high-performance IPsec VPN with dedicated crypto engine</li> <li>Simplifies large VPN deployments with auto VPN and group VPN</li> <li>Offers secure and flexible remote access SSL VPN with Juniper Secure Connect</li> <li>Verifies binaries that execute on the hardware with secure boot</li> </ul>                                                                                      |
| <b>High reliability</b>                       | Chassis cluster, redundant power supply                                                                                                                                       | <ul style="list-style-type: none"> <li>Provides stateful configuration and session synchronization</li> <li>Supports active/active and active/backup deployment scenarios</li> <li>Offers highly available hardware with dual PSU, redundant fans</li> </ul>                                                                                                                                                                                 |
| <b>Easy to manage and scale</b>               | On-box GUI, Security Director                                                                                                                                                 | <ul style="list-style-type: none"> <li>Enables centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments</li> <li>Includes simple easy-to-use on-box GUI for local management</li> </ul>                                                                                                                                                                        |
| <b>Lower TCO</b>                              | Junos OS                                                                                                                                                                      | <ul style="list-style-type: none"> <li>Integrates routing, switching, and security in a single device</li> <li>Reduces OpEx with Junos OS automation capabilities</li> </ul>                                                                                                                                                                                                                                                                 |



SRX1500

## SRX1500 Firewall Specifications

### Software Specifications

#### Firewall Services

- Stateful and stateless firewall
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomalies
- Integration with Pulse Unified Access Control (UAC)
- Integration with Aruba Clear Pass Policy Manager
- User role-based firewall
- SSL Inspection

#### Network Address Translation (NAT)

- Source NAT with Port Address Translation (PAT)
- Bidirectional 1:1 static NAT
- Destination NAT with PAT
- Persistent NAT
- IPv6 address translation

#### VPN Features

- Tunnels: Site-to-Site, Hub and Spoke, Dynamic Endpoint, AutoVPN, ADVPN, Group VPN (IPv4/IPv6/Dual Stack)
- Juniper Secure Connect: Remote access/SSL VPN
- Configuration payload: Yes
- IKE Encryption algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB
- IKE authentication algorithms: MD5, SHA-1, SHA-128, SHA-256, SHA-384
- Authentication: Pre-shared key and public key infrastructure (PKI) (X.509)
- IPsec (Internet Protocol Security): Authentication Header (AH)/ Encapsulating Security Payload (ESP) protocol
- IPsec Authentication Algorithms: hmac-md5, hmac-sha-196
- IPsec Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB
- Perfect forward secrecy, anti-reply
- Internet Key Exchange: IKEv1, IKEv2
- Monitoring: Standard-based dead peer detection (DPD) support, VPN monitoring
- VPNs GRE, IP-in-IP, and MPLS

### High Availability Features

- Virtual Router Redundancy Protocol (VRRP)
- Stateful high availability
  - Dual box clustering
  - Active/passive
  - Active/active
  - Configuration synchronization
  - Firewall session synchronization
  - Device/link detection
  - In-Service Software Upgrade (ISSU)
- IP monitoring with route and interface failover

### Application Security Services<sup>1</sup>

- Application visibility and control
- Application-based firewall
- Application QoS
- Advanced/application policy-based routing (APBR)
- Application Quality of Experience (AppQoE)
- Application-based multipath routing

### Threat Defense and Intelligence Services<sup>1</sup>

- Intrusion prevention
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- Protection from botnets (command and control)
- Adaptive enforcement based on GeolP
- Juniper Advanced Threat Prevention, a cloud-based SaaS offering, to detect and block zero-day attacks
- Juniper ATP Appliance, a distributed, on-premises advanced threat prevention solution to detect and block zero-day attacks
- Adaptive Threat Profiling
- Encrypted Traffic Insights
- SecIntel to provide threat intelligence

<sup>1</sup>Offered as advanced security subscription license

**Routing Protocols**

- IPv4, IPv6
- Static routes
- RIP v1/v2
- OSPF/OSPF v3
- BGP with Route Reflector
- IS-IS
- Multicast: Internet Group Management Protocol (IGMP) v1/v2; Protocol Independent Multicast (PIM) sparse mode (SM)/dense mode (DM)/source-specific multicast (SSM); Session Description Protocol (SDP); Distance Vector Multicast Routing Protocol (DVMRP); Multicast Source Discovery Protocol (MSDP); Reverse Path Forwarding (RPF)
- Encapsulation: VLAN, Point-to-Point Protocol over Ethernet (PPPoE)
- Virtual routers
- Policy-based routing, source-based routing
- Equal-cost multipath (ECMP)

**QoS Features**

- Support for 802.1p, DiffServ code point (DSCP), EXP
- Classification based on VLAN, data-link connection identifier (DLCI), interface, bundles, or multifield filters
- Marking, policing, and shaping
- Classification and scheduling
- Weighted random early detection (WRED)
- Guaranteed and maximum bandwidth
- Ingress traffic policing
- Virtual channels
- Hierarchical shaping and policing

**Switching Features**

- ASIC-based Layer 2 forwarding
- MAC address learning
- VLAN addressing and integrated routing and bridging (IRB) support
- Link aggregation and LACP
- LLDP and LLDP-MED
- STP, RSTP, MSTP
- MVRP
- 802.1X authentication

**Network Services**

- Dynamic Host Configuration Protocol (DHCP) client/server/relay
- Domain Name System (DNS) proxy, dynamic DNS (DDNS)
- Juniper real-time performance monitoring (RPM) and IP monitoring
- Juniper flow monitoring (J-Flow)
- Bidirectional Forwarding Detection (BFD)
- Two-Way Active Measurement Protocol (TWAMP)
- IEEE 802.3ah Link Fault Management (LFM)
- IEEE 802.1ag Connectivity Fault Management (CFM)

**Advanced Routing Services**

- Packet mode
- MPLS (RSVP, LDP)
- Circuit cross-connect (CCC), translational cross-connect (TCC)
- L2/L2 MPLS VPN, pseudo-wires
- Virtual private LAN service (VPLS), next-generation multicast VPN (NG-MVPN)
- MPLS traffic engineering and MPLS fast reroute

**Management, Automation, Logging, and Reporting**

- SSH, Telnet, SNMP
- Smart image download
- Juniper CLI and Web UI
- Juniper Networks Junos Space and Security Director
- Python
- Junos OS event, commit and OP scripts
- Application and bandwidth usage reporting
- Auto installation
- Debug and troubleshooting tools

## Hardware Specifications

| Specification                                               | SRX1500                                         |
|-------------------------------------------------------------|-------------------------------------------------|
| <b>Connectivity</b>                                         |                                                 |
| Total onboard ports                                         | 16x1GbE and 4x10GbE                             |
| Onboard RJ-45 ports                                         | 12x1GbE                                         |
| Onboard small form-factor pluggable (SFP) transceiver ports | 4x1GbE                                          |
| Onboard SFP+ ports                                          | 4x10GbE                                         |
| Out-of-Band (OOB) management ports                          | 1x1GbE                                          |
| Dedicated high availability (HA) ports                      | 1x1GbE (SFP)                                    |
| PIM slots                                                   | 2                                               |
| Console (RJ-45 + miniUSB)                                   | 1                                               |
| USB 2.0 ports (type A)                                      | 1                                               |
| <b>Memory and Storage</b>                                   |                                                 |
| System memory (RAM)                                         | 16 GB                                           |
| Primary boot storage (mSATA)                                | 16 GB                                           |
| Secondary storage (SSD)                                     | 100 GB                                          |
| <b>Dimensions and Power</b>                                 |                                                 |
| Form factor                                                 | 1 U                                             |
| Size (WxDxH)                                                | 17.28 x 1.75 x 18.2 in (43.9 x 4.44 x 46.22 cm) |
| Weight (device and PSU)                                     | 16.1 lb (7.30 kg)                               |
| Redundant PSU                                               | 1+1                                             |
| Power supply                                                | AC/DC (external)                                |
| Average power consumption                                   | 150 W                                           |
| Average heat dissipation                                    | 512 BTU / hour                                  |
| Maximum current consumption                                 | 2.5A (for AC PSU);<br>6.2A (for DC PSU)         |
| Maximum inrush current                                      | 50A by 1 AC cycle                               |
| Acoustic noise level                                        | 66.5dBA                                         |
| Airflow/cooling                                             | Front to back                                   |
| Operating temperature                                       | 32° to 104° F (0° to 40° C)                     |
| Nonoperating temperature                                    | 4° to 158° F (-20° to 70° C)                    |
| Operating humidity                                          | 10% to 90% noncondensing                        |
| Nonoperating humidity                                       | 5% to 95% noncondensing                         |
| Mean time between failures (MTBF)                           | 9.78 years (85,787 hours)                       |
| FCC classification                                          | Class A                                         |
| RoHS compliance                                             | RoHS 2                                          |
| FIPS 140-2                                                  | Level 2 (FIPS 19.2)                             |
| <b>Performance and Scale</b>                                |                                                 |
| Routing/firewall (1Mx packet size) Gbps <sup>a</sup>        | 4.8                                             |
| Routing/firewall (1,518 B packet size) Gbps <sup>a</sup>    | 9.2                                             |
| IPsec VPN (1Mx packet size) Gbps <sup>a</sup>               | 1.3                                             |
| IPsec VPN (1400 B packet size) in Gbps <sup>a</sup>         | 4.5                                             |
| Application visibility and control in Gbps <sup>a</sup>     | 7.9                                             |
| Recommended IPS in Gbps <sup>a</sup>                        | 3.3                                             |
| Next-generation firewall in Gbps <sup>a</sup>               | 2.1                                             |
| Secure Web Access firewall in Gbps <sup>a</sup>             | 1.6                                             |
| Route table size (RIB/FIB) (IPv4)                           | 2 million / 1 million                           |
| Maximum concurrent sessions (IPv4 or IPv6)                  | 2,000,000                                       |
| Maximum security policies                                   | 16,000                                          |
| Connections per second                                      | 90,000                                          |
| NAT rules                                                   | 8,000                                           |

| Specification                                      | SRX1500                  |
|----------------------------------------------------|--------------------------|
| Media access control (MAC) table size              | 64,000 (standalone mode) |
| IPsec VPN tunnels                                  | 2,000                    |
| Number of remote access/SSL VPN (concurrent) users | 2,000                    |
| GRE tunnels                                        | 2,048                    |
| Maximum security zones                             | 512                      |
| Maximum virtual router                             | 512                      |
| Maximum VLANs                                      | 3,900                    |

<sup>a</sup>Performance numbers based on UDP packets and RFC2544 test methodology.

<sup>b</sup>Performance numbers based on HTTP traffic with 4K transaction size.

<sup>c</sup>Next-Generation Firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions.

<sup>d</sup>Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions.

## Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit <https://www.juniper.net/us/en/products.html>.

## Ordering Information

To order Juniper Networks SRX Series Firewalls, and to access software licensing information, please visit the How to Buy page at <https://www.juniper.net/us/en/how-to-buy/form.html>.

- Datasheet del Firewall de Nueva Generación - Forcepoint Modelo N2201.

## Next Generation Firewall

# 2200 Series

For mid-size and large offices, next-generation firewall throughput up to 13.5 Gbps



### Key Benefits

- › 1U rack-mounted design
- › Modular interfaces for customized expansion
- › Multi-ISP SD-WAN and site-to-site Multi-Link™ VPN connectivity
- › Industry's most secure NGFW with anti-evasion IPS
- › High-availability clustering
- › Accelerated inspection of encrypted traffic
- › Zero-touch deployment
- › Access and security policy updates with just a few clicks
- › Centralized management of 6,000 appliances on one pane of glass
- › Integration with Forcepoint Remote Browser Isolation (RBI) and Advanced Malware Detection (AMD) Sandboxing
- › Optional URL Filtering powered by Forcepoint ThreatSeeker

Mid-size and large offices requiring enhanced performance and scalability can connect directly to the cloud with the Forcepoint NGFW 2200 Series. It integrates full SD-WAN connectivity and strong security in a compact, 1U rack-mounted appliance that's managed at enterprise scale from Forcepoint's renowned Security Management Center (SMC).

### Direct-to-cloud connectivity and security for digital transformation

Digital transformation is all about connecting distributed workforces to the resources they need, no matter where they are. With applications and data moving to the cloud, organizations are increasingly finding that old "hub-and-spoke" networking technologies such as MPLS can no longer handle the load.

The Forcepoint NGFW 2200 Series provides the networking and security needed to safely connect mid-size and large offices or small data centers directly to the Internet for maximum performance and productivity using the cloud. The 2200 Series' modular interfaces offer up to sixteen 10 Gb Ethernet ports, up to two 25 Gb Ethernet ports, or allowing organizations to tailor the appliance to their exact connectivity needs.

### Reduced costs and footprint with integrated SD-WAN and NGFW

The Forcepoint NGFW 2200 Series unites networking and security in a modular and space efficient 1U rackmount appliance. It integrates multi-ISP SD-WAN connectivity, site-to-site Multi-Link™ VPN and high-availability clustering with the industry's strongest next-generation firewall (NGFW)\* and intrusion prevention (IPS) security.

It is centrally administered using the same Forcepoint Security Management Center (SMC) that controls up to a 6,000 physical, virtual and cloud appliances from a single console of glass. With zero-touch deployment, Forcepoint NGFW devices throughout the world can be deployed quickly, without an on-site technician, and SMC enables access to devices so that security policies can be updated remotely with just a few clicks.

### Advanced clustering for high availability

Downtime is not an option for many organizations. That's why the Forcepoint NGFW 2200 Series offers advanced clustering that allows multiple appliances (including other Forcepoint NGFW models) to be used together to keep branch networks running even in the middle of firmware updates or hardware failure. Built-in SD-WAN traffic management enables links from more than one ISP to be used at the same time to further reduce the chance of outages.

| PERFORMANCE <sup>1</sup>                            | N2201      | N2205      | N2210      |
|-----------------------------------------------------|------------|------------|------------|
| NGFW/NGIPS throughput (HTTP 64kB payload)           | 5.5 Gbps   | 10.5 Gbps  | 13.5 Gbps  |
| Max firewall throughput (UDP 1518 byte)             | 80 Gbps    | 120 Gbps   | 120 Gbps   |
| Threat Prevention throughput                        | 3 Gbps     | 9 Gbps     | 12 Gbps    |
| TLS 1.2 inspection performance (44kB payload)       | 1.6 Gbps   | 2.7 Gbps   | 4.5 Gbps   |
| IPsec VPN throughput AES-GCM-256                    | 22 Gbps    | 40 Gbps    | 60 Gbps    |
| Concurrent IPsec VPN tunnels                        | 90,000     | 95,000     | 100,000    |
| Mobile VPN clients                                  | Unlimited  | Unlimited  | Unlimited  |
| Max number of concurrent inspected HTTP connections | 300,000    | 650,000    | 700,000    |
| Max number of concurrent connections                | 17 million | 35 million | 35 million |
| New TCP connections/sec.                            | 350,000    | 550,000    | 610,000    |
| VLAN tagging                                        | Unlimited  | Unlimited  | Unlimited  |
| Virtual contexts default/maximum                    | 10 / 100   | 10 / 100   | 10 / 100   |

<sup>1</sup> Performance values reflect maximums measured under test conditions and may vary based on configuration and features enabled.

| PHYSICAL                         | N2201                                     | N2205         | N2210         |
|----------------------------------|-------------------------------------------|---------------|---------------|
| Form factor                      | 1RU                                       |               |               |
| Dimensions (W x H x D)           | 438 x 44 x 420 mm (17.2" x 1.7" x 16.5")  |               |               |
| Net weight without modules       | 8.23Kg (18.14lb)                          |               |               |
| AC power supply                  | 100 - 240 VAC 50 - 60 Hz<br>300 W + 300 W |               |               |
| DC power supply option           | -72 ~ -36 VDC,<br>850 W + 850 W           |               |               |
| Redundant power supply           | Option                                    |               | Standard      |
| Typical power consumption        | 80                                        | 100           | 115           |
| Max power consumption            | 94                                        | 116           | 140           |
| Max BTU/hour                     | 291                                       | 360           | 434           |
| MTBF                             | 100,000 hours                             | 100,000 hours | 100,000 hours |
| Operating temperature            | 0 - 40 °C (32 - 104 °F)                   |               |               |
| Storage temperature              | -20 - 70 °C (-4 - 158 °F)                 |               |               |
| Relative humidity non-condensing | 40 °C @ 95% RH Non-Condensing             |               |               |
| Safety certifications            | CE, UL/EN60950, NOM                       |               |               |
| EMI certifications               | FCC Part 15, CE, EN55022, EN55024         |               |               |

| NETWORK INTERFACES              | N2201                                 | N2205                         | N2210 |
|---------------------------------|---------------------------------------|-------------------------------|-------|
| Fixed Ethernet interfaces       | 8x GE RJ45<br>4x 10 Gbps SFP+         | 8x GE RJ45<br>8x 10 Gbps SFP+ |       |
| Gigabit Ethernet - copper ports | 8 to 16                               |                               |       |
| 10 Gigabit Ethernet slots       | 4 to 12                               | 8 to 16                       |       |
| 25 Gigabit Ethernet slots       | 0 to 2                                |                               |       |
| 40 Gigabit Ethernet slots       | 0 to 2                                |                               |       |
| Network I/O slots               | 1                                     |                               |       |
| Connectors                      | 2x USB, 1x serial, VGA, IPMI Ethernet |                               |       |

| ORDERING                                       | N2201   | N2205             | N2210   |
|------------------------------------------------|---------|-------------------|---------|
| Forcepoint NGFW 220X Appliance                 | N2201   | N2205             | N2210   |
| URL Filtering for NGFW 220X                    | FPURL6X | FPURLBX           | FPURL9X |
| Advanced Malware Detection for 2200 Series     | FPAMD6X | FPAMD6X           | FPAMD6X |
| Virtual context upgrade for 220X               |         | FPVC25<br>FPVC100 |         |
| 8 Port Gb Ethernet RJ45                        |         | MODGB             |         |
| 8 Port Gb Ethernet SFP                         |         | MODGB8            |         |
| 4 Port 10Gb Ethernet SFP+                      |         | MOD10F4           |         |
| 8 Port 10Gb Ethernet SFP+                      |         | MOD10F8           |         |
| 2 Port 25Gb Ethernet SFP2B                     |         | MOD25F2           |         |
| 2 Port 40Gb Ethernet QSFP                      |         | MOD40F2           |         |
| 8 Port Gb Ethernet RJ45 Bypass Module          |         | MODGBB            |         |
| 4 Port 10Gb Ethernet Long Reach Bypass Module  |         | MOD10LAB          |         |
| 4 Port 10Gb Ethernet Short Reach Bypass Module |         | MOD10SAB          |         |
| 2 Port 40 G Ethernet MPO Bypass                |         | MOD40F2B          |         |
| 2200 Series rack mounting kit                  |         | ACR2200           |         |
| 2200 Series AC power supply                    |         | ACRA2200          |         |
| 2200 Series DC power supply                    |         | ACPD3400          |         |
| 2200 Series spare part SSD                     |         | ACD2200           |         |

- Datasheet del Firewall de Nueva Generación - Palo Alto Modelo PA-3250.



### Aspectos destacados

- El primer NGFW con tecnología ML del mundo
- Nueve veces líder en el Cuadrante mágico de Gartner® para firewalls de red
- Líder en The Forrester Wave™: Enterprise Firewalls, tercer trimestre de 2020
- Máxima puntuación de eficacia de seguridad en el informe sobre pruebas de NGFW de 2019 de NSS Labs con el 100 % de las evasiones bloqueadas
- Aumenta la visibilidad y la seguridad de todos los dispositivos, incluidos los dispositivos de IoT no gestionados, sin la necesidad de implementar sensores adicionales
- Admite la alta disponibilidad con los modos activo/activo y activo/pasivo
- Ofrece un rendimiento predecible con servicios de seguridad
- Simplifica la implementación de grandes cantidades de firewalls con aprovisionamiento cero fácil (ZTP) opcional
- Admite administración centralizada con la gestión de seguridad de redes de Panorama™

## PA-3200 Series

Los NGFW PA-3200 Series con tecnología ML de Palo Alto Networks (que incluyen PA-3260, PA-3250 y PA-3220) se dirigen a implementaciones de gateways de Internet de alta velocidad. Los dispositivos PA-3200 Series protegen todo el tráfico, incluso el tráfico cifrado, a través de procesamiento y memoria dedicados para el funcionamiento de la red, la seguridad, la prevención y la gestión de amenazas.



PA-3260



PA-3250



PA-3220

El elemento de control de PA-3200 Series es PAN-OS®, el mismo software que ejecuta todos los firewalls de nueva generación (NGFW) de Palo Alto Networks. PAN-OS clasifica de forma nativa todo el tráfico, incluso de las aplicaciones, las amenazas y el contenido, y lo vincula con el usuario sin importar la ubicación o el tipo de dispositivo. La aplicación, el contenido y el usuario (los elementos que hacen funcionar a su empresa) sirven como base de sus políticas de seguridad, lo que se traduce en una mejor postura de seguridad y una reducción en el tiempo de respuesta ante incidentes.

## Funciones clave de seguridad y conectividad

### Firewall de nueva generación con tecnología ML

- Integra aprendizaje automático (ML) en el núcleo del firewall a fin de proporcionar una prevención de ataques sin firma internos para los ataques basados en archivos, mientras identifica y detiene de inmediato los intentos de phishing nunca antes vistos.
- Aprovecha los procesos de ML basados en la nube para enviar instrucciones y firmas sin demora al NGFW.
- Usa el análisis de comportamiento para detectar dispositivos de Internet de las cosas (IoT) y ofrecer recomendaciones de políticas; un servicio integrado de forma nativa y entregado en la nube en el NGFW.
- Automatiza las recomendaciones de políticas que ahorran tiempo y reducen los errores humanos.

### Identificación y categorización de todas las aplicaciones en todos los puertos, en todo momento, con inspección completa de la Capa 7

- Identifica las aplicaciones que atraviesan su red, independientemente del puerto, el protocolo, las técnicas de evasión o el cifrado (TLS/SSL).
- Usa la aplicación, no el puerto, como base para todas las decisiones de políticas de habilitación segura: permitir, denegar, programar, inspeccionar y aplicar el control de tráfico.
- Proporciona la capacidad de crear etiquetas de App-ID™ personalizadas para las aplicaciones exclusivas o solicita el desarrollo de App-ID para las nuevas aplicaciones de Palo Alto Networks.
- Identifica todos los datos de la carga útil dentro de una aplicación, (por ejemplo, los patrones de datos y archivos) para bloquear los archivos maliciosos y frustrar los ataques de exfiltración de datos.
- Crea informes de uso de aplicaciones estándar y personalizados, incluidos informes de Software as a Service (Software como servicio - SaaS) que proporcionan información sobre todo el tráfico SaaS autorizado y no autorizado en su red.
- Habilita la migración segura de conjuntos de reglas de Capa 4 heredados para las reglas basadas en App-ID con un optimizador de políticas incorporado que ofrece un conjunto de reglas más seguro y fácil de administrar.

### Refuerzo de la seguridad de los usuarios en cualquier ubicación, en cualquier dispositivo, y adaptación de políticas basada en la actividad de los usuarios

- Habilita la visibilidad, las políticas de seguridad, los informes y las investigaciones forenses en función de los usuarios y los grupos, no solo las direcciones IP.
- Se integra fácilmente en una amplia gama de repositorios para aprovechar la información de los usuarios: controladores de LAN inalámbricos, VPN, servidores de directorios, SIEM, proxies, etc.

- Permite definir grupos de usuarios dinámicos (DUG) en el firewall para adoptar medidas de seguridad con plazos determinados sin esperar a que los cambios se apliquen en los directorios de usuarios.
- Aplica políticas consistentes independientemente de las ubicaciones (oficina, hogar, viaje, etc.) y los dispositivos (dispositivos móviles iOS y Android®, macOS®, Windows®, computadoras de escritorio Linux, computadoras portátiles; servidores de terminales, y VDI Citrix y Microsoft) de los usuarios.
- Evita la filtración de credenciales corporativas a sitios web de terceros y la reutilización de credenciales sustraídas mediante la habilitación de la autenticación de varios factores (MFA) en la capa de la red para cualquier aplicación sin cambios.
- Proporciona acciones de seguridad dinámicas basadas en el comportamiento del usuario para restringir a los usuarios sospechosos o malintencionados.

### Prevención de actividades maliciosas ocultas en el tráfico cifrado

- Inspecciona y aplica políticas al tráfico cifrado con TLS/SSL, tanto entrante como saliente, incluido el tráfico que usa TLS 1.3 y HTTP/2.
- Ofrece visibilidad enriquecida del tráfico TLS, por ejemplo, la cantidad de tráfico cifrado, las versiones de TLS/SSL, los conjuntos de cifrado y mucho más, sin descifrado.
- Permite el control sobre el uso de protocolos TLS heredados, cifrados inseguros y certificados configurados incorrectamente para mitigar los riesgos.
- Facilita la implementación del descifrado y permite usar registros incorporados para solucionar problemas, como aplicaciones con certificados bloqueados.
- Permite habilitar o deshabilitar la flexibilidad del descifrado en función de la categoría de URL y la zona de origen y destino, la dirección, el usuario, el grupo de usuarios, el dispositivo y el puerto con fines de privacidad y cumplimiento normativo.
- Permite crear una copia del tráfico descifrado del firewall (reflejo de descifrado) y la envía a las herramientas de recopilación de tráfico para investigaciones forenses, fines históricos o data loss prevention (prevención de pérdida de datos - DLP).

### Ofrece visibilidad y gestión centralizadas

- Se beneficia de la gestión, la configuración y la visibilidad centralizadas para múltiples NGFW de Palo Alto Networks distribuidos (independientemente de la ubicación o la escala) a través de la gestión de seguridad de redes de Panorama™, en una interfaz de usuario unificada.
- Agiliza el uso compartido de la configuración a través de Panorama con plantillas y grupos de dispositivos, y escala la recopilación de registros a medida que aumentan las necesidades de registro.
- Permite a los usuarios obtener una visibilidad profunda e información integral del tráfico de red y las amenazas, gracias al Application Command Center (Centro de comando de aplicación - ACC).

### Detecta y previene amenazas avanzadas con servicios de seguridad en la nube

Los sofisticados ciberataques de la actualidad pueden generar 45.000 variantes en 30 minutos con múltiples vectores de amenaza y técnicas avanzadas para entregar cargas útiles maliciosas. La seguridad aislada tradicional plantea problemas a las organizaciones, ya que introduce brechas de seguridad, aumenta la sobrecarga de los equipos de seguridad y obstaculiza la productividad de la empresa con un acceso y una visibilidad inconsistentes.

Nuestros servicios de seguridad en la nube, que están perfectamente integrados con nuestros NGFW líderes del sector, utilizan el efecto de la red de 80.000 clientes para coordinar instantáneamente la información y proporcionar protección contra todas las amenazas en todos los vectores. Elimine las brechas de cobertura en todas sus ubicaciones y aproveche la seguridad de la más alta calidad suministrada de forma consistente en una plataforma, para poder estar a salvo incluso de las amenazas más avanzadas y evasivas. Los servicios incluyen:

- **Threat Prevention:** vaya más allá de un sistema de Intrusion Prevention (IPS) tradicional para prevenir todas las amenazas conocidas en todo el tráfico en un solo paso, sin sacrificar el rendimiento.
- **URL Filtering avanzado:** ofrece protección web de la más alta calidad y maximiza la eficiencia operativa con el primer motor de protección web en tiempo real del sector y una protección contra el phishing líder en el sector.
- **WildFire®:** garantiza la seguridad de los archivos con la detección y prevención automáticas de malware desconocido, gracias al análisis basado en la nube líder en el sector y a la inteligencia de origen colectivo de más de 42.000 clientes.
- **Seguridad de DNS:** aprovecha el poder de ML para detectar y prevenir las amenazas a través de DNS en tiempo real y proporciona al personal de seguridad la inteligencia y el contexto necesarios para elaborar políticas y responder a las amenazas de forma rápida y eficaz.
- **Seguridad de IoT:** proporciona la solución de seguridad de IoT más completa del sector, ya que ofrece visibilidad, prevención y cumplimiento con tecnología ML en una única plataforma.
- **DLP empresarial:** la primera DLP empresarial en la nube del

sector que protege sistemáticamente los datos confidenciales en todas las redes, nubes y usuarios.

- **Seguridad de SaaS:** ofrece una seguridad SaaS integrada que le permite ver y proteger las nuevas aplicaciones SaaS, proteger los datos y evitar las amenazas de día cero con el menor costo total de propiedad (TCO).

#### Entrega de un enfoque exclusivo para el procesamiento de paquetes con arquitectura de paso único

- Lleva a cabo la conexión de redes, la búsqueda de políticas, la aplicación, la decodificación y la comparación de firmas para todas las amenazas y el contenido en un solo paso. Esto reduce en gran medida la sobrecarga de procesamiento necesaria para realizar varias funciones en un solo dispositivo de seguridad.
- Evita la introducción de la latencia mediante el escaneo del tráfico para todas las firmas en un único paso con la comparación de firmas uniforme basada en flujos.
- Permite un rendimiento predecible y consistente cuando se habilitan las suscripciones de seguridad. (En la Tabla 1, "Rendimiento de Threat Prevention", se mide con varias suscripciones habilitadas.)

#### Habilitación de la funcionalidad SD-WAN

- Permite la adopción simple de SD-WAN mediante su habilitación en los firewalls existentes.
- Permite la implementación de SD-WAN de manera segura, la integración de forma nativa con nuestra seguridad líder en el sector.
- Ofrece una experiencia excepcional para el usuario final al minimizar la latencia, la fluctuación y la pérdida de paquetes.

**Tabla 1: Rendimiento y capacidad de PA-3200 Series**

|                                                 | PA-3260      | PA-3250      | PA-3220      |
|-------------------------------------------------|--------------|--------------|--------------|
| Rendimiento del firewall (HTTP/Appmix)*         | 7,8/8,7 Gbps | 5,3/5,8 Gbps | 4,3/4,8 Gbps |
| Rendimiento de Threat Prevention (HTTP/Appmix)† | 3,9/4,7 Gbps | 2,6/3,1 Gbps | 2,1/2,6 Gbps |
| Rendimiento de VPN IPSec‡                       | 4,7 Gbps     | 2,9 Gbps     | 2,6 Gbps     |
| Sesiones máximas                                | 2,2 millones | 2 millones   | 1 millón     |
| Sesiones nuevas por segundo§                    | 94.400       | 63.700       | 52.800       |
| Sistemas virtuales (base/máx.)                  | 1/6          | 1/6          | 1/6          |

Nota: Los resultados se midieron en PAN-OS 10.1.

\* El rendimiento del firewall se mide con App-ID y registros habilitados, mediante el uso de transacciones HTTP/AppMix de 64 KB.

† El rendimiento de Threat Prevention se mide con App-ID, IPS, antivirus, antispam, WildFire, Seguridad de DNS, bloqueo de archivos y registros habilitados mediante el uso de transacciones HTTP/appmix de 64 KB.

‡ El rendimiento de VPN IPSec se mide mediante el uso de transacciones HTTP de 64 KB y registros habilitados.

§ Las nuevas sesiones por segundo se miden mediante la cancelación de la aplicación que utiliza transacciones HTTP de 1 byte.

|| La incorporación de sistemas virtuales por encima de la cantidad base requiere una licencia adquirida por separado.

**Tabla 2: Funciones de red de PA-3200 Series**

| Modos de interfaz                                                                        |
|------------------------------------------------------------------------------------------|
| L2, L3, tap, virtual wire (modo transparente)                                            |
| Enrutamiento                                                                             |
| OSPFv2/v3 con reinicio cuidadoso, BGP con reinicio cuidadoso, RIP, enrutamiento estático |
| Policy-based forwarding (reenvío basado en políticas - PBF)                              |
| Point-to-point protocol over Ethernet (protocolo punto a punto sobre Ethernet - PPPoE)   |
| Multidifusión: PIM-SM, PIM-SSM, IGMP v1, v2 y v3                                         |

**Tabla 2: Funciones de red de PA-3200 Series (continuación)**

| SD-WAN                                                                      |
|-----------------------------------------------------------------------------|
| Medición de la calidad de ruta (fluctuación, pérdida de paquetes, latencia) |
| Selección de ruta inicial (PBF)                                             |
| Cambio dinámico de ruta                                                     |
| IPv6                                                                        |
| L2, L3, tap, virtual wire (modo transparente)                               |
| Funciones: App-ID, User-ID, Content-ID, WildFire                            |

**Tabla 2: Funciones de red de PA-3200 Series (continuación)**

| IPSec VPN                                                                                                      |
|----------------------------------------------------------------------------------------------------------------|
| Intercambio de claves: clave manual, IKEv1 e IKEv2 (clave precompartida, autenticación basada en certificados) |
| Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)                                                              |
| Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512                                                           |
| VLAN                                                                                                           |
| Etiquetas VLAN 802.1Q por dispositivo/por interfaz: 4094/4094                                                  |
| Interfaces agregadas (802.3ad), LACP                                                                           |
| Network address translation (traducción de dirección de red - NAT)                                             |
| Modos NAT (IPv4): IP estática, IP dinámica, IP y puerto dinámicos (traducción de direcciones de puertos)       |
| NAT64, NPTv6                                                                                                   |
| Funciones adicionales de la NAT: reserva de IP dinámica, IP y puerto dinámicos con túnel y sobresuscripción    |
| Alta disponibilidad                                                                                            |
| Modos: activo/activo, activo/pasivo, clúster de HA                                                             |
| Detección de fallas: monitoreo de rutas, supervisión de interfaz                                               |
| Aprovisionamiento cero táctil (ZTP)                                                                            |
| Disponible con SKU ZTP (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP)                                                 |
| Requiere Panorama 9.1.3 o posterior                                                                            |

**Tabla 3: Especificaciones del hardware de PA-3200 Series**

| E/S                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)                                                                                                                |
| PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)                                                                                                                               |
| PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)                                                                                                                   |
| E/S de gestión                                                                                                                                                               |
| Puerto de gestión fuera de banda de 10/100/1000 (1), alta disponibilidad de 10/100/1000 (2), alta disponibilidad de 10G SFP+ (1), puerto de consola RJ-45 (1), micro USB (1) |
| Capacidad de almacenamiento                                                                                                                                                  |
| SSD de 240 GB                                                                                                                                                                |
| Fuente de alimentación (consumo de energía promedio/máximo)                                                                                                                  |
| 650 W redundantes de CA o CC (180/240)                                                                                                                                       |
| BTU/h máximo                                                                                                                                                                 |
| 819                                                                                                                                                                          |
| Tensión de entrada (frecuencia de entrada)                                                                                                                                   |
| CA: 100–240 V CA (50/60 Hz)                                                                                                                                                  |
| CC: -48 V a 4,7 A, -60 V a 3,8 A                                                                                                                                             |

**Tabla 3: Especificaciones del hardware de PA-3200 Series (continuación)**

| Consumo de corriente máximo                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------|
| CA: 2,3 A a 100 V CA, 1,0 A a 240 V CA                                                                                                           |
| CC: -48 V a 4,7 A, -60 V a 3,8 A                                                                                                                 |
| Mean time between failures (tiempo medio entre fallos - MTBF)                                                                                    |
| 14 años                                                                                                                                          |
| Montaje en rack (dimensiones)                                                                                                                    |
| 2U, rack estándar de 19" (48,26 cm) (3,5" de alto x 20,53" de prof. x 17,34" de ancho [8,89 cm de alto x 52,15 cm de prof. x 44,04 cm de ancho]) |
| Peso (solo dispositivo/dispositivo preparado para envío)                                                                                         |
| 29 libras/41,5 libras (13,15 kg/18,82 kg)                                                                                                        |
| Seguridad                                                                                                                                        |
| cTUVus, CB                                                                                                                                       |
| EMI                                                                                                                                              |
| Clase A FCC, Clase A CE, Clase A VCCI                                                                                                            |
| Certificaciones                                                                                                                                  |
| Consulte <a href="https://paloaltonetworks.com/company/certifications.html">paloaltonetworks.com/company/certifications.html</a>                 |
| Entorno                                                                                                                                          |
| Temperatura operativa: 32 °F a 122 °F, 0 °C a 50 °C                                                                                              |
| Temperatura no operativa: -4 °F a 158 °F, -20 °C a 70 °C                                                                                         |
| Tolerancia a la humedad: Entre 10 % y 90 %                                                                                                       |
| Altitud máxima: 10.000 ft/3048 m                                                                                                                 |
| Flujo de aire: de adelante hacia atrás                                                                                                           |

Para consultar información adicional sobre las funciones y las capacidades asociadas de PA-3200 Series, consulte [paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series](https://paloaltonetworks.com/network-security/next-generation-firewall/pa-3200-series).

## Anexo 2: Cuadrante Mágico de Gartner:

Se evidencia en el estudio realizado por la empresa Gartner (2022) que, a nivel de firewalls, Palo Alto Networks se posiciona como uno de los líderes en el sector, asimismo se caracteriza por ser el que tiene mayor capacidad integral en su ejecución y mayor visión.

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

### Anexo 3: Propuesta Económica:

Se evidencia la propuesta económica realizada a la entidad del estado.



Propuesta Económica



Partner: IMPERIA  
Contacto:  
Fecha: 6/10/2020  
Forma de Pago: según créditos

Cliente  
Final: Ministerio de Economía y Finanzas  
País: Peru  
Vigencia: 15 días  
Fabricante: Palo Alto Networks  
Entrega: HW 45 días/ SW 10 días

| Part Number               | Term (M) | Descripción                                                                                                                                                             | Cant.    | Precio Socio de Negocio |
|---------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------------------|
| <b>PANW-ZFIN-002</b>      |          |                                                                                                                                                                         | <b>1</b> |                         |
| <b>FW de Perimetro</b>    |          |                                                                                                                                                                         |          |                         |
| <b>Sede Principal</b>     |          |                                                                                                                                                                         |          |                         |
| PAN-PA-3250               | -        | Palo Alto Networks PA-3250 with redundant AC power supplies                                                                                                             | 2        |                         |
| PAN-PA-3250-TP-3YR-HA2    | 39       | Threat prevention subscription 3 year prepaid for device in an HA pair, PA-3250                                                                                         | 2        |                         |
| PAN-PA-3250-URL4-3YR-HA2  | 39       | PANDB URL filtering subscription 3 year prepaid for device in an HA pair, PA-3250                                                                                       | 2        |                         |
| PAN-PA-3250-WF-3YR-HA2    | 39       | WildFire subscription 3 year prepaid for device in an HA pair, PA-3250                                                                                                  | 2        |                         |
| PAN-PA-3250-SDWAN-3YR-HA2 | 39       | SD-WAN subscription 3 year prepaid for device in an HA pair, PA-3250                                                                                                    | 2        |                         |
| PAN-SVC-PREM-3250-3YR     | 39       | Premium support 3-year prepaid, PA-3250                                                                                                                                 | 2        |                         |
| PAN-SFP-PLUS-SR           | -        | SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant                                                  | 16       |                         |
| PAN-SFP-PLUS-CU-5M        | -        | SFP+ form factor, 10Gb direct attach twin-ax passive cable with 2 transceiver ends and 5m of cable permanently bonded as an assembly, IEEE 802.3ae 10GBASE-CR compliant | 1        |                         |
| PAN-PA-2RU-RACK4          | -        | Palo Alto Networks PA-3220, PA-3250, and PA-3260 4 post rack mount kit                                                                                                  | 2        |                         |

**Condiciones Comerciales:**

La presente propuesta está expresada en Dólares Americanos.

La aceptación de la OC dependerá de la evaluación crediticia que Ingram Micro realice.

Vigencia de la oferta: 15 días calendario.

Tiempo de entrega: HW 45 días/ SW 15 días

Las OC serán procesadas de acuerdo a nuestros tiempos internos (+/- 48 horas)