UNIVERSIDAD DE PIURA

FACULTAD DE INGENIERÍA

Proyecto de actualización de los sistemas Firewall para mejorar la ciberseguridad en la Marina de Guerra del Perú

Trabajo de Suficiencia Profesional para optar el Título de
Ingeniero Industrial con mención en Gestión Logística

Pedro César Montalván Grijalba

Revisor:
Dr. Ing. Ronald Alejandro Ruiz Robles

Piura, noviembre de 2020

UNIVERSITAS STUDIORUM PIURENSIS

Dedicatoria

A mi abuela, Aurea Luz por todas sus enseñanzas y cariño.

UNIVERSITAS STUDIORUM PIURENSIS

Resumen

En el año 2015 la Marina de Guerra del Perú renovó sus sistemas de seguridad tipo *firewall*, los cuales ya se empezaban a ver limitados en su capacidad tecnológica y traían problemas en cuanto al rendimiento y a las funcionalidades requeridas por los administradores y los usuarios.

Durante la etapa de evaluación se tuvo que hacer un levantamiento de información de la problemática total, la cual demandaba dar solución al tiempo de procesamiento para la aplicación de reglas, funcionalidades de seguridad avanzadas, conexiones VPN, proceso de aprendizaje de la nueva solución y uno de los factores más limitantes, el presupuesto.

Una vez definido el problema, se procedió a analizar las soluciones disponibles en el mercado, tomando como referencia un análisis de *benchmarking*, recomendación de expertos, precio, funcionalidades, dando como solución elegida un *firewall* de la marca *checkpoint*.

Posteriormente se procedió al proceso de configuración, pruebas, instalación física y puesta en producción al sistema, teniendo como resultado éxito en este proyecto y el sistema de seguridad tipo *firewall* fue implementado sin mayores complicaciones.

UNIVERSITAS STUDIORUM PIURENSIS

Tabla de contenido

Lista de tablas

UNIVERSITAS STUDIORUM PIURENSIS

Lista de figuras

UNIVERSITAS STUDIORUM PIURENSIS

Introducción

El presente Trabajo de Suficiencia Profesional, es producto del análisis y la solución a un problema que tenía la Marina de Guerra del Perú durante el año 2018. Debido al avance tecnológico, nuevas amenazas aparecían en Internet, la institución tenía la necesidad de publicar servicios en línea, pues el mundo interconectado lo demandaba.

Si bien es cierto existen diferentes soluciones de seguridad disponibles en el mercado, una de las más importantes es el sistema de seguridad tipo *firewall*, pues es la principal medida de seguridad frente a atacantes que intentan acceso a recursos no autorizados mediante el uso de protocolos o explotación de vulnerabilidades.

La Marina de Guerra del Perú, es una institución militar, por lo tanto, mantiene información relevante para la seguridad nacional, lo cual es bastante atractivo para ciberdelincuentes de diferentes partes del mundo que por simple reconocimiento pueden intentar vulnerar estos sistemas.

La elección de un sistema de seguridad tipo *firewall* es un proceso complejo, pues se debe buscar una alternativa que cumpla con los requerimientos de la institución, pues como se ha mencionado anteriormente, existen diferentes soluciones en el mercado.

El sistema elegido por la Marina de Guerra del Perú, cubre todos sus requisitos, lo cual asegura la confidencialidad, disponibilidad e integridad de la información de la institución.

UNIVERSITAS STUDIORUM PIURENSIS

Capítulo 1

Aspectos generales

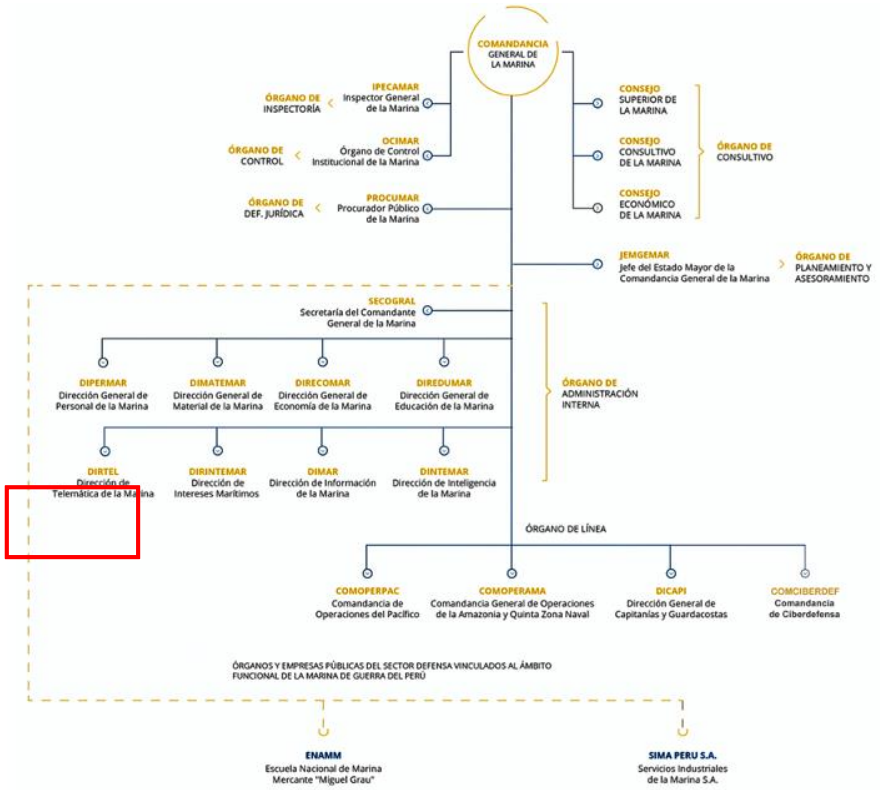
1.1. Descripción de la organización

1.1.1. Organigrama

Para cumplir con sus objetivos, la Marina de Guerra del Perú cuenta con diferentes unidades y dependencias organizadas jerárquica y funcionalmente. Dicha organización cuenta con órganos de apoyo, órganos de planeamiento y asesoramiento, órgano consultivo, órganos de administración interna y órganos de línea.

Figura 1

Organigrama de la Marina de Guerra del Perú



Fuente Tomado y adaptado de "Portal Institucional de la Marina de Guerra del Perú"[1]

[1] Recuperado de: https://marina.mil.pe/es/nosotros/acerca-de/

Una de estas dependencias es la Dirección de Telemática de la Marina que actúa como área de soporte en materia de telecomunicaciones, informática y ciberseguridad, por lo tanto, es el ente técnico en materia tecnológica. Estas unidades y dependencias se pueden apreciar en la Figura 1.

1.1.2. Misión

La Marina de Guerra del Perú en su portal web, indica como su misión:

> Ejercer la vigilancia y protección de los intereses nacionales en el ámbito marítimo, fluvial y lacustre, y apoyar la política exterior del Estado a través del Poder Naval; asumir el control del orden interno, coadyuvar en el desarrollo económico y social del país y participar en la Defensa Civil de acuerdo a ley; con el fin de contribuir a garantizar la independencia, soberanía e integridad territorial de la República y el bienestar general de la población (Marina de Guerra del Perú, s.f.).

Como se puede apreciar, la misión de la Marina de Guerra del Perú es de índole nacional, poniendo especial énfasis, pero no limitado, al ámbito marítimo, fluvial y/o lacustre.

1.1.3. Visión

La Marina de Guerra del Perú en su portal web, indica como su visión: "Poder Naval capaz de actuar con éxito donde lo requieran los intereses nacionales" (Marina de Guerra del Perú, s.f.).

Para el cumplimiento de su visión, la Marina de Guerra del Perú, requiere un poder naval que debe actuar exitosamente para ayudar al cumplimiento de los intereses nacionales. Por esta razón y debido al avance tecnológico, es necesario adoptar nuevas tecnologías, implementadas de manera segura, que ayuden a cumplir con esta visión.

1.2. Descripción del cargo ocupado

En el año 2014, presté servicios como Jefe de la División de Comunicaciones y Navegación en el B.A.P. "Sánchez Carrión", donde realicé labores relacionadas al mantenimiento del estado operacional de los sistemas de comunicaciones, informática y de navegación de dicha unidad de combate. Uno de los mayores logros fue el cumplimiento al 85% de las políticas de ciberseguridad establecidas en la institución, así como la actualización de las cartas náuticas. Dicho cargo fue ocupado hasta enero del año 2015.

Durante el año 2015 realicé la especialización de ingeniería de sistemas y logré obtener dicha calificación por la Escuela Superior de Guerra Naval con el primer puesto. En el año 2016 fui destacado a la Dirección de Telemática de la Marina, donde desempeñé los siguientes cargos:

• Jefe de la División de Conectividad, este cargo fue desempeñado entre enero y marzo del 2016, las principales funciones en dicho cargo fueron garantizar la conectividad de la unidades

y dependencias de la Marina de Guerra del Perú, gestionar los recursos para el mantenimiento de torres y antenas de radio enlace en todo el territorio nacional. En este cargo se evaluó la posibilidad de integrar la red de la Marina de Guerra del Perú a la Red Dorsal de Fibra Óptica con la que cuenta el Estado Peruano.

• Jefe de la División de Operaciones en el Ciberespacio, este cargo fue desempeñado de marzo del 2016 a octubre del 2018 las principales funciones en este cargo estuvieron relacionadas al análisis de vulnerabilidades en los servidores y sistemas con los que contaba la Marina de Guerra del Perú. Uno de los principales logros obtenidos en el cargo fue la creación del *Computer Security Information and Response Team* (CSIRT-MGP) de la institución, donde logré firmar un convenio muy importante para colaboración y compartir información relacionada a la ciberseguridad con la Asociación Nacional de Bancos del Perú (ASBANC).

Posteriormente, de octubre del 2017 a marzo del 2018 fui enviado en misión de estudios a España para cursar la fase práctica de la Maestría en Ciberdefensa por la Universidad de Alcalá de Henares.

De marzo del 2018 a enero del 2020, ocupé el cargo de Jefe de la División de Ciberseguridad, mi principal función consistió en mantener actualizado el sistema de ciberseguridad de la Marina de Guerra del Perú a través de la implementación de políticas, procedimientos y lineamientos, así como gestionar la adquisición de software y hardware de ciberseguridad. Sobre este último punto, para el cumplimiento de las funciones asignadas debía considerar todos los requerimientos de ciberseguridad de la institución y la tecnología disponible en el mercado, poniendo énfasis en garantizar la confidencialidad, integridad y disponibilidad de la información. Posterior a ello, debía elaborar las especificaciones técnicas y después de ser aprobadas por el jefe inmediato, el Jefe del Departamento de Administración de Redes y Ciberseguridad, debía solicitar la conformación del comité especial a cargo del proceso de licitación público según lo estipulado por el Organismo Supervisor de las Contrataciones del Estado (OSCE). Finalmente, debía evaluar las propuestas técnicas y una vez obtenida la buena pro, iniciar el proyecto de implementación del nuevo sistema adquirido.

1.3. Descripción del problema

Los sistemas de seguridad tipo *Firewall* con los que contaba la Marina de Guerra habían sido renovados en el año 2015. Estos sistemas *firewall* requerían ser renovados pues sus características técnicas empezaban a verse limitadas, como por ejemplo existía un excesivo retraso al momento de aplicar reglas de seguridad, lo cual dificultaba las tareas de administración, solo permitía un número limitados de usuarios conectados de manera concurrente mediante VPN (hasta 30), soportaba hasta la versión del sistema operativo R77.30, lo cual no permitía contar con todas las bondades de la nueva versión R80.x, que permitía aplicar reglas de seguridad más complejas y simplificaba el análisis de eventos de seguridad, lo cual reducía el número de horas-hombre, además debido a la digitalización de

los procesos de la institución y a la mejora del parque informático hacía que más usuarios puedan conectarse a la red, navegar hacía Internet y acceder a los servicios publicados, lo cual hacía crítica esta actualización.

Para tener una idea del problema, podemos tomar como referencia un reporte de la empresa Cisco, que, en su Reporte Anual de Ciberseguridad del año 2018, concluyó que:

> En el moderno panorama de las amenazas, los adversarios son expertos en evadir la detección. Tienen herramientas más efectivas, como encriptación, y tácticas más avanzadas e inteligentes, como el abuso de servicios legítimos de Internet, para ocultar su actividad y socavar las tecnologías de seguridad tradicionales. Y están desarrollando constantemente sus tácticas para mantener su *malware* fresco y efectivo. Incluso las amenazas conocidas por la comunidad de seguridad pueden tardar mucho tiempo en identificarse. (CISCO, 2018)

Como se puede apreciar, en el citado informe existe una necesidad para hacerle frente a estas amenazas, que cada vez son más frecuentes y avanzadas. Para poder hacerles frente es necesario contar con tecnología avanzada que pueda detectar cualquier ataque en su fase inicial y permita actuar al analista de manera preventiva y no reactiva, los sistemas *firewall* con los que contaba la Marina de Guerra del Perú en el año 2018 no contaban con la tecnología ni con las características técnicas necesarias para cumplir con todos los requerimientos.

Capítulo 2

Fundamentación del tema elegido

2.1. Riesgos del Ciberespacio

En la publicación MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método se describe a los riesgos como "Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización" (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Estos riesgos pueden afectar a los sistemas que la Marina de Guerra del Perú tiene implementados, pues como se ha mencionado antes las amenazas han aumentado su impacto y capacidades técnicas, como controles a estos riesgos existen tecnologías de ciberseguridad disponibles, siendo una de las más importantes los sistemas *firewall*.

La Norma Chilena NCh ISO 27032. Define a la ciberseguridad como:

> Condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable (Instituto Nacional de Normalización, 2015)

Para contar con niveles aceptables de ciberseguridad la Marina de Guerra del Perú necesita medidas de protección que garanticen los puntos antes señalados, los cuales formaban partes de las funciones de la División de Ciberseguridad de la Dirección de Telemática de la Marina.

2.1.1. Amenazas

En el ciberespacio existen diferentes tipos de amenazas, como por ejemplo el malware, que es código malicioso y generalmente lo conocemos como virus o gusanos, pero existen otros tipos como el adware, ransomware, troyano, spyware, entre otros. Se procederá a definir alguno de los tipos de malware más conocidos:

• Ransomware: Es un tipo de malware cuyo objetivo principal es cifrar la información de una estación de trabajo, servidor, celular u otro dispositivo de punto final. Para descifrar la información el atacante pide un depósito económico.

• Virus: Es un tipo de malware que generalmente es incrustado en archivos aparentemente inofensivos (documentos en formato word, pdf, excel, etc) y realizan actividades maliciosas en las computadoras de los usuarios. Para hacer daño necesita que el usuario ejecute el archivo infectado

• Gusano: Es un tipo de malware que realiza actividades maliciosas en las computadoras de los usuarios, por ejemplo eliminar archivos, alterar contenido, etc. No necesita la actividad del usuario para replicarse

• Spyware: Este tipo de malware, tiene por finalidad monitorear toda la actividad de los usuarios, por ejemplo, espiar a través de la cámara web, escuchar mediante el micrófono o visualizar la pantalla del usuario.

• Adware: Tipo de Malware que crean publicidad incómoda para los usuarios

Otra amenaza común en el ciberespacio son los denominados exploits, que son código que explotan una vulnerabilidad en el sistema. Estas vulnerabilidades pueden ser desactualizaciones en el sistema operativo, errores de los usuarios, ausencia de controles, etc.

Finalmente, otro tipo de amenaza común en el ciberespacio son las personas, que según la motivación o sus objetivos pueden ser catalogados como:

• Hacktivistas: Son personas que siguen una ideología en el ciberespacio y utilizan sus conocimientos informáticos para imponer esta ideología. Uno de los grupos de hacktivistas más conocidos son el grupo Anonymous, famosos por sus amenazas a los gobiernos.

• Ciberterroristas: Son personas que generan terror utilizando técnicas o herramientas cibernéticas, un ciberterrorista podría afectar a la banca, comunicaciones, red de hospitales, sistemas industriales, etc. Lo cual podría crear una preocupación grande en la población y problemas a los gobiernos.

• Script Kiddie: En Internet tenemos disponibles muchas herramientas, la información que podemos obtener en páginas como google, youtube, facebook, telegram o foros hacen que las técnicas de explotación de vulnerabilidades estén accesibles a personas que no cuentan con el conocimiento técnico avanzado, pero al tener la información pueden ejecutar diferentes tipos de ataques ocasionando daños a las diferentes organizaciones.

• Cibercomandos: Finalmente tenemos ejércitos que preparan a su personal para la protección de su soberanía y sus recursos informáticos.

La empresa Panda Security en su artículo denominado En la cabeza del cibercriminal: ¿qué busca y por qué quiere atacar tu empresa? Señala que:

> El 51% de los encuestados afirmaba que su principal motivación a la hora de emprender ciberataques era “la búsqueda de emociones”, mientras que sólo un 18% señalaba los beneficios económicos como razón. Según el estudio, esto viene a indicar que “los modernos hackers son curiosos, están aburridos o quieren poner a prueba sus habilidades” (Panda Security, s.f.).

Como podemos apreciar, la mayoría de ataques proviene de personas curiosas y debido a que el ciberespacio no tiene fronteras es una preocupación latente para la Marina de Guerra del Perú, además al ser una institución relevante a nivel nacional puede ser muy atractiva para un ciberdelincuente de cualquier parte del mundo.

Un caso bastante nuevo de ciberataques el ocurrido al Ministerio de Desarrollo e Inclusión social durante la pandemia del 2020 en el que el programa Bono Universal fue hackeado por ciberdelincuentes que se llevaron aproximadamente un millón de soles (Neyra, 2020). Esto demuestra que los ciberdelincuentes buscan cualquier vulnerabilidad para atacar y no tienen límites a la hora de realizar sus ataques.

2.1.2. Vulnerabilidades

El instituto Nacional de Ciberseguridad (INCIBE) en su publicación Glosario de Términos de Ciberseguridad, define a las vulnerabilidades como:

Fallos o deficiencias de un programa que pueden permitir que un usuario no legitimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas (Instituto Nacional de Ciberseguridad, 2017).

Debido al nivel de clasificación de la información que tiene la Marina de Guerra del Perú es necesario reducir la probabilidad que las amenazas exploten diferente tipo de vulnerabilidades propia de los sistemas. Entre las vulnerabilidades más comunes tenemos:

• Vulnerabilidad zero-day: Son vulnerabilidades para las que no existe un parche o solución de seguridad vigente, aprovechadas por un ciberdelincuente pueden ocasionar daños muy graves a las organizaciones, pues atentan contra la confidencialidad, integridad y disponibilidad de la información.

• Ausencia de actualizaciones: Para corregir las vulnerabilidades de los sistemas y/o protocolos, los fabricantes lanzan parches de seguridad, muchos usuarios no instalan estas actualizaciones dejando vulnerables a los sistemas. Uno de los ataques más conocidos debido a la ausencia de actualizaciones de seguridad fue el caso del ransomware WannaCry, este malware aprovechaba una vulnerabilidad conocida (MS17-10) para la que Windows ya había

lanzado un parche de seguridad en el mes de marzo del año 2017. El ataque sucedió en mayo del año 2017 y tuvo un alcance global, afectando a empresas muy grandes como telefónica.

• Vulnerabilidades físicas: Otro tipo de vulnerabilidades son las de tipo físico, como por ejemplo infraestructura deteriorada o en mal estado.

2.2. Next – Generation Firewall

David Cortes en su artículo titulado *Firewall*s de nueva generación: la seguridad informática vanguardista. Describe a los *firewalls* como:

Los *firewalls* son dispositivos que buscan proteger la información, por lo que son una de las herramientas principales de seguridad informática. Las organizaciones mantienen un flujo constante de información con su entorno y a través de este flujo puede entrar en riesgo el propio negocio por diversas amenazas, tanto internas (fuga de información) como externas (suplantación, estafas, malware) (Cortes)

Un *Next-Generation Firewall* (NGFW) es un dispositivo de seguridad informática que a diferencia de los *firewalls* tradicionales que generalmente inspeccionan las direcciones IP, los puertos, protocolo de comunicación o tienen implementada alguna regla de seguridad que evita cualquier conexión no autorizada o potencialmente inseguridad, posee una serie de ventajas, como, por ejemplo:

• Inspección del estado de la conexión, muchos ataques aprovechan las vulnerabilidades propias de los protocolos de comunicación, para evitar ello los NGFW tienen implementados un conjunto de reglas que permiten establecer cuál es el dispositivo que origina la comunicación y en base al análisis realizado permitir o denegar la conexión.

• Integración con otros dispositivos de seguridad como el sistema de prevención de instrucciones (IPS por sus siglas en inglés), antivirus de red, sistema de inspección de navegación web.

• Permiten el filtrado de páginas web potencialmente maliciosas para evitar que los usuarios de la institución ingresen a páginas web comprometidas que pudiesen afectar a la información institucional

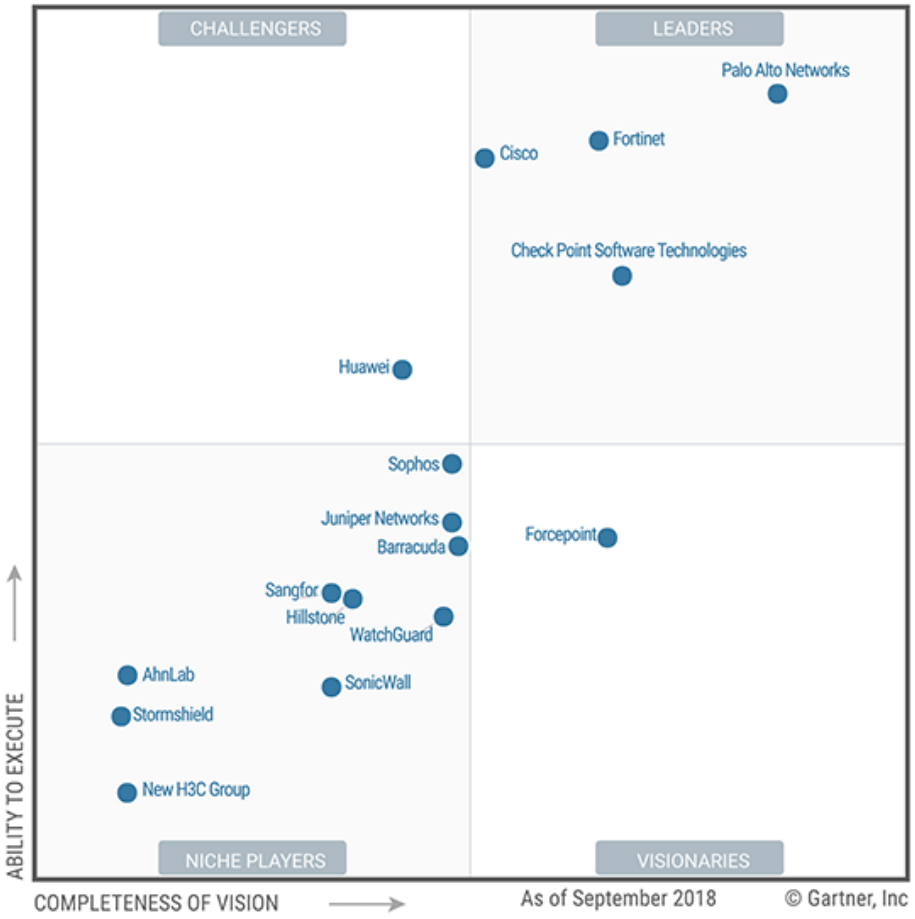
• Analizan el tráfico de correo electrónico para evitar cualquier tipo de malware distribuido por correo electrónico y/o cualquier tipo de estafa enviada a través del correo electrónico.

• Tienen integración con *Virtual Private Network* (VPN) ya sea entre clientes u organizaciones para realizar comunicación cifrada y más segura.

• Inteligencia avanzada para la detección de amenazas.

En la Figura 2 se muestra los mejores sistemas tipo *firewall* según el reporte de la empresa Gartner, que mide la eficiencia de las herramientas tecnológicas a diferentes niveles de estrés.

Figura 2
Reporte de Gartnet 2018



Fuente Tomado y adaptado de "Gartner"

Como se puede apreciar en la imagen existen diferentes soluciones de seguridad disponibles. En el caso de la Marina de Guerra del Perú se trabajó con la marca *Checkpoint.*

2.3. Herramientas de ingeniería utilizadas

2.3.1. Benchmarking

Roberto Espinoza en su sitio web señala que: "El *benchmarking* es un proceso continuo por el cual se toma como referencia los productos, servicios o procesos de trabajo de las empresas líderes, para compararlos con los de tu propia empresa y posteriormente realizar mejoras e implementarlas" (Espinoza, s.f.)

El *benchmarking*, por lo tanto, es una herramienta ampliamente utilizada por los ingenieros para comparar sus productos, servicios o procesos con los de otras organizaciones ya sea de un sector similar o totalmente diferente al suyo. Hoy en día gracias a la globalización es muy fácil acceder a diferentes productos de cualquier parte del mundo, con diferentes niveles de calidad y precio, por lo tanto, el *benchmarking* ayuda a encontrar el producto, servicio o proceso necesario para mejorar el que se tiene en la organización

Para el caso del presente proyecto, se utilizó *benchmark* para comparar los diferentes productos disponibles en el mercado y obtener el mejor para la realidad de la Marina de Guerra del Perú teniendo en cuenta los requerimientos estipulados.

2.3.2. Diagramas de flujo de procesos

Luis Miguel Manene, en su sitio web señala que un diagrama de flujo es:

> Un diagrama de flujo es la representación gráfica del flujo o secuencia de rutinas simples. Tiene la ventaja de indicar la secuencia del proceso en cuestión, las unidades involucradas y los responsables de su ejecución, es decir, viene a ser la representación simbólica o pictórica de un procedimiento administrativo (Manene, 2011).

En ese sentido, un diagrama de flujo ayuda a identificar todos los pasos involucrados en la realización de una tarea, permitiendo que los ingenieros puedan planificar todas las tareas y recursos necesarios. Para el caso del presente proyecto, se utilizó el diagrama de flujo para esquematizar el proceso de la instalación, configuración, pruebas y puesta en producción del sistema.

2.3.3. Pruebas de calidad

Las pruebas de calidad son aquellas que se realizan para identificar si el proyecto cumple con los requerimientos del usuario, en las pruebas se realizan comprobaciones de todos los requisitos del proyecto, en algunos casos se puede someter a cargas de estrés para identificar cuál es el rendimiento máximo del sistema, así como también se realizan pruebas de seguridad para identificar posibles vulnerabilidades que pudiesen afectar a los usuarios.

En el caso del presente proyecto, se realizaron las pruebas correspondientes antes de su puesta en producción, pues al ser un sistema crítico se debía tener certeza de que no existirían fallos.

Capítulo 3

Desarrollo de la experiencia

3.1. Evaluación de la necesidad y soluciones disponibles

Como se ha mencionado anteriormente, los sistemas de seguridad tipo *Firewall* con los que contaba la Marina de Guerra habían sido renovados en el año 2015, con una tecnología que estaba vigente en esos años y una capacidad suficiente para atender los requerimientos institucionales en la citada fecha.

Al llegar el año 2018, los sistemas ya contaban con un uso de tres años y su capacidad ya se veía limitada, por ejemplo al aplicar una regla de seguridad sencilla el tiempo de respuesta llegaba a ser de aproximadamente 45 minutos y de haber algún error no se detectaba hasta que la tarea culmine y muestre dicho error, esto provocaba estrés en el personal operador y retraso en las actividades pues muchas veces el equipo de desarrollo de la Dirección de Telemática de la Marina solicitaba aplicar una regla para colocar en producción un sistema, al aplicar reglas complejas, la demora podía llegar a ser de hasta dos horas.

Así mismo, el sistema solo permitía hasta 30 usuarios conectados de manera concurrente mediante VPN, para el año 2015 eso era suficiente, pero para el año 2018 teniendo en cuenta que un grupo oficiales tenían acceso VPN a diversos sistemas, las agregadurías navales acreditadas en otros países necesitaban acceder a sistemas institucionales mediante VPN y se requería integraciones para compartir información con otras organizaciones era necesario contar con un sistema que tuviese la capacidad de permitir la conexión de varios usuarios de manera concurrente y de una forma eficiente.

Otro aspecto a tener en cuenta era la versión del sistema operativo del *firewall* vigente. El dispositivo adquirido en el año 2015 solo soportaba hasta la versión R.77.30, la cual no contaba con todas las funcionalidades de la última versión R.80.X, la cual permitía aplicar reglas de seguridad más complejas y permitía a los analistas realizar un análisis más rápido y dinámico de cualquier brecha o incidente pues los filtros eran más sencillos y ya existía búsquedas predefinidas que la versión anterior no tenía.

Uno de los factores más importantes era la curva de aprendizaje que debía tener el personal de la Marina en el uso de un sistema de seguridad tipo *firewall*, con el anterior sistema ya tenían trabajando tres años y la topología de la red era bastante complejo, se

tenían aplicadas muchas configuraciones que no eran sencillas de configurar desde un inicio en un nuevo sistema, por lo cual la opción más viable era continuar con la marca adquirida en el año 2015 en su versión más actual.

Finalmente, muchos proyectos se ven limitados por el presupuesto, este también era el caso de la Marina de Guerra del Perú, teníamos un presupuesto fijo y se procedió a realizar cotizaciones con diferentes empresas y marcas. Se evaluaron marcas como:

- Palo Alto Networks
- Checkpoint
- Cisco
- Fortinet

La Tabla 1 muestra un cuadro comparativo entre las diferentes soluciones disponibles en el mercado.

Tabla 1

Cuadro comparativo de productos tipo Firewall

Característica	Palo Alto Networks	CheckPoint	Cisco	Fortinet
Capacidad NGFW	Si	Si	Si	Si
Capacidad conexión VPN	Si	Si	Si	Si
Conocimiento previo por personal naval	No	Si	No	No
Cuadrante de Gartner	Si	Si	Si	Si
Precio	Alto	Alto	Medio	Bajo
Dificultad en la implementación	Medio	Sencilla	Medio	Medio
Dificultad en la administración	Medio	Sencilla	Alta	Sencilla

Fuente Elaboración propia

También se consideró la experiencia de personas referentes y recomendaciones de especialistas con amplio conocimiento en la materia, como por ejemplo el personal de la Fuerza Área del Perú, Comando Conjunto, Asesores de la Marina de Guerra del Perú, Oficiales de seguridad de compañías para que este análisis tipo benchmarking sea más completo. La recomendación de estos expertos apuntaba a dos soluciones, *Checkpoint* y Palo Alto.

Debido a lo anteriormente descrito, evaluamos que la mejor opción era un *firewall* de la marca *checkpoint* modelo 5800, en alta disponibilidad y con la consola de gestión respectiva.

Figura 3

Firewall Checkpoint 5800

Fuente Tomado de "Checkpoint"

El modelo elegido, brindaba una solución completa a los problemas señalados anteriormente:

• Reducía el tiempo de aplicación de reglas sencillas a segundos y de reglas complejas hasta un par de minutos, pues su capacidad de procesamiento y memoria era mucho mayor.

• Debido a los requerimientos de los usuarios para el uso de VPN se determinó el número total en 300 licencias concurrentes, lo cual era cubierto por este nuevo modelo de firewall.

• Se podía instalar la nueva versión del fabricante, R.80.X con todas las nuevas funcionalidades y ventajas que ésta ofrecía y hacía más sencillo el análisis, así como un mejor nivel de ciberseguridad con reglas predefinidas y protección avanzada.

• Al ser una continuidad del producto anterior, el tiempo de aprendizaje era mínimo pues se trabaja del mismo sistema con mejoras en su funcionalidad, pero no eran grandes cambios y el personal encargado podría adaptarse rápidamente.

• El presupuesto de este modelo se adaptaba a lo planificado en el proceso de renovación por lo cual la adquisición fue sencilla.

Además, el modelo elegido tenía otras funcionalidades que mejoraban la ciberseguridad de la Marina de Guerra del Perú, pues permitía:

• Proteger contra vulnerabilidades *zero-day*, mediante su tecnología s*andblas* que tiene la capacidad de defensiva contra amenazas desconocidas.

• Poseía un *throughput* de 4 Gb lo cual era suficiente para las comunicaciones de la Marina de Guerra del Perú.

• Poseía diferentes interfaces para comunicar los segmentos de red con los que contaba la institución.

• Permitía el monitoreo de tráfico cifrado del protocolo SSL.

• La tecnología utilizada era la misma que la versión adquirida en el 2015, con mejoras funcionales y tiempo de respuesta más rápido.

3.2. Planificación e implementación

Después de haber obtenido la buena pro en el proceso de selección, me correspondía como Jefe de la División de Ciberseguridad llevar a cabo la planificación y coordinar todo lo necesario para la nueva implementación. El siguiente diagrama de flujo muestra el proceso seguido:

• Después de haber obtenido la buena pro del proceso, como primera medida se tenía que considerar el espacio físico donde se colocaría el nuevo equipo adquirido que constaba de tres equipos:

- ✓ 02 *Firewalls Checkpoint* modelo 5800
- ✓ 01 consola de gestión *Checkpoint*

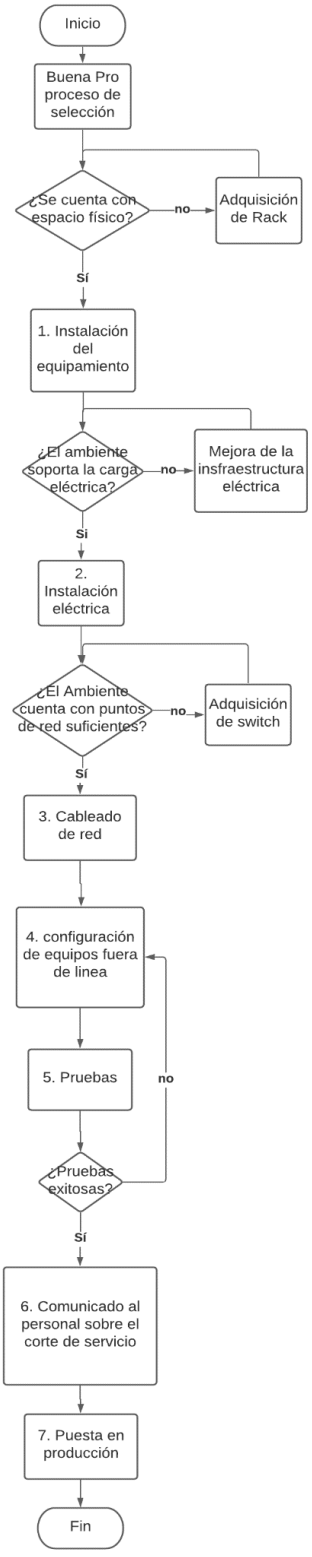
Esto demandaba 6 RU que debían estar disponibles en el rack asignado a los equipos de seguridad. El equipamiento anterior solo ocupaba 2 RU por lo que se necesitaba solo 4 RU disponibles y se contaba con el espacio suficiente. Fueron colocados en un rack de 42 RU. En caso no se hubiera contado con el espacio suficiente habría sido necesario adquirir un nuevo rack.

• Posteriormente se tenía que considerar el consumo eléctrico para no sobre cargar el UPS y la energía térmica generada para no tener problemas con el aire acondicionado. Referente al consumo de energía, según las especificaciones del fabricante no sobrepasaría los 330W y el calor generado no superaría los 1128 BTU/hora. El data center de la Dirección de Telemática estaba preparado para soportar esta carga sin mayores complicaciones. En caso no hubiera sido factible la instalación debía coordinarse con el área de logística para que mejore la infraestructura eléctrica

• Finalmente, para culminar con los aspectos físicos se debía tener en consideración la conexión al *switch core* de la dirección de telemática, la conexión al *router* de Internet y la conexión a la zona desmilitarizada (DMZ). Esto fue factible ya que el nuevo equipamiento adquirido contaba con las interfaces de red necesarias y el cableado de red era muy sencillo de realizar ya que se utilizaría parte del cableado anterior (UTP cat. 6a), la nueva configuración no demandaba puertos disponibles en el *switch core*, lo cual no generaba gastos adicionales por temas de licenciamiento.

Figura 4

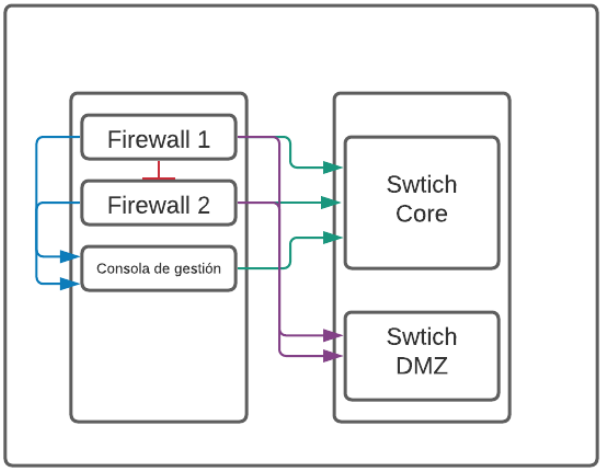
Diagrama de flujo del trabajo realizado



Fuente Elaboración propia

Figura 5

Diagrama físico del sistema tipo firewall



Fuente Elaboración propia

• Posteriormente se tenían que configurar los equipos, se estableció que los equipos serían configurados fuera de la data center en las oficinas de la División de Ciberseguridad para la facilidad del trabajo, pues el acceso a la data center es restringido y no se puede permanecer muchas horas dentro.

✓ Como primer paso se debía instalar el sistema operativo, configurar direcciones IP, DNS, NTP, generar accesos por SSH, creación de usuarios, realizar pruebas y dejar el equipo listo para la instalación de reglas de seguridad.

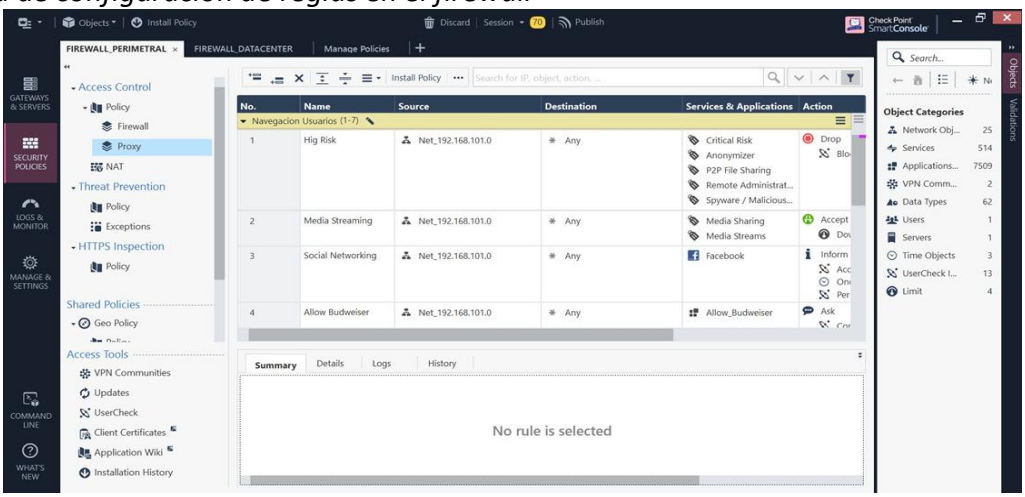
✓ Al ser de la misma marca, se podían exportar las reglas instaladas y de una manera sencilla el archivo generado se podía importar en el nuevo equipo, por lo que la parte de configuración de reglas era relativamente sencilla.

✓ Luego se tenía que instalar certificados de navegación (autogenerados por el nuevo *firewall*) para el análisis de tráfico cifrado SSL, lo cual fue factible gracias al directorio activo que media una política de grupo permitía el despliegue de una manera automatizada a todos los equipos registrados en el dominio.

✓ Posteriormente se tenían que crear los usuarios para la edición de reglas, modo lectura y acceso VPN. El personal de la División de Ciberseguridad, encargados de la administración del *firewall* (titular y alternos), tenían acceso a la edición de reglas, el técnico de cargo de la división tenía acceso de modo lectura al igual que el jefe de la división, los usuarios con acceso VPN, debían ser autorizados por el director de telemática de la Marina.

Figura 6

Consola de configuración de reglas en el firewall



Fuente Elaboración propia

Con la parte física coordinada y la parte lógica configurada se debía proceder a la instalación del nuevo firewall en los ambientes señalados, debido a que el trabajo tomaría aproximadamente 6 horas, se debía realizar fuera del horario de oficina y se optó por un fin de semana.

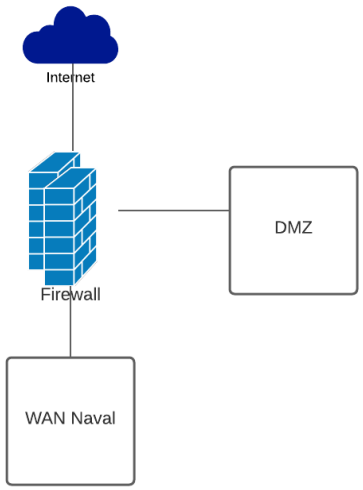
• Una vez instalado todo el equipamiento se procedían a las pruebas, la etapa de pruebas se detalla en el punto 3.3.

• Con la conformidad de las pruebas, se procedía a comunicar a los usuarios sobre el corte de servicio, que como ya se mencionó anteriormente, tomarían aproximadamente 6 horas.

• Finalmente se podía colocar el sistema en producción y empezar a utilizar el *firewall*.

Figura 7

Diagrama lógico del sistema tipo firewall



Fuente Elaboración propia

3.3. Pruebas

Las pruebas fueron una de las partes más importantes dentro del proyecto, ya que si algún servicio no funcionaba correctamente no se podía mantener el sistema activo. En ese sentido, las pruebas fueron muy exhaustivas y consistieron en lo siguiente:

- Usuarios de la WAN Naval:

  ✓ Acceso a Internet (con filtrado de páginas), para lo cual se verificó que los usuarios puedan navegar a páginas confiables y el tráfico a páginas potencialmente maliciosas se encuentre bloqueado.

  ✓ Acceso a correo electrónico (dentro y fuera de la red), para lo cual se verificó que los usuarios puedan enviar y recibir correos electrónicos con datos adjuntos.

  ✓ Acceso a servicios operacionales, acceso a los servicios operacionales con los que contaba la Marina de Guerra del Perú.

  ✓ Acceso a servicios administrativos (página personal, sistema de control patrimonial, etc.), estos servicios son de uso interno y se verificó que los usuarios de la WAN Naval puedan acceder a ellos.

  ✓ Bloqueo de conexiones maliciosas, tanto de salida como de entrada (pruebas simuladas de ataques), se verificó el tráfico hacia servicios maliciosos, el firewall debía bloquear esos intentos de conexiones.

  ✓ Revisión de logs generados, para lo cual se procedió a verificar y analizar los logs generados mediante el uso de filtros por protocolo, dirección IP de origen, destino, puertos, etc.

  ✓ Creación y aplicación de reglas, para lo cual se aplicaron reglas de seguridad y se verificó su correcto funcionamiento, por ejemplo, el bloqueo de verificación a sitios web maliciosos.

- Usuarios VPN:

  ✓ Acceso según el perfil asignado, ya que por seguridad no todos los usuarios podían acceder a todos los servicios

  ✓ Concurrencia de usuarios en simultaneo

  ✓ Revisión de logs generados

  ✓ Creación y aplicación de reglas

Con las pruebas realizadas y el sistema listo para su funcionamiento, se podía dar por concluido el Proyecto de actualización de los sistemas Firewall para mejorar la ciberseguridad en la Marina de Guerra del Perú.

Conclusiones

Vivimos en un mundo cada vez más interconectado, las organizaciones, independientemente de su sector se ven en la necesidad de mantener sus sistemas interconectados y de fácil acceso a los usuarios, esto hace que los ciberdelincuentes encuentren muchos sistemas vulnerables sobre los cuales realizar ataques.

Los ataques cibernéticos son cada vez más avanzados y menos complejos en su realización, hoy en día existen muchos tutoriales disponibles en Internet en portales como YouTube, Facebook, LinkedIn, entre otros, lo cual permite a cualquier persona iniciarse en el mundo del hacking y de esa manera, en algunos casos, intentar vulnerar sistemas de diferentes organizaciones.

La Marina de Guerra del Perú posee información muy crítica para la seguridad nacional, motivo por el cual debe contar con personas capaces de defender los intereses institucionales y nacionales, sistemas de última generación para evitar que ciberdelincuentes accedan a la información clasificada y procesos diseñados para poder mantener toda la información segura.

El mercado hoy en día ofrece una alta variedad de soluciones tecnológicas, tanto *opensource* (código abierto) como licenciadas, que cuentan con el soporte de una marca reconocida y facilita su administración. Las organizaciones independientemente de su sector deben contar con herramientas tecnológicas que permitan proteger sus activos de información. Una buena fuente de referencia es *Gartnert*, quien anualmente evalúa a las soluciones tecnológicas.

Implementar una solución del tipo firewall es un paso obligatorio para toda organización que publique servicios en Internet. Estos firewalls cuentan con diferentes tecnologías que no solo permiten el filtrado de paquetes, cada funcionalidad eleva su costo por lo que las organizaciones deben evaluar qué es lo que realmente necesitan y adquirir un producto de acuerdo a sus necesidades.

La tecnología avanza y las soluciones de seguridad deben ser renovadas constantemente, es una buena práctica ir evaluando soluciones de seguridad disponibles en el mercado y compararlas frente a lo que se tiene actualmente implementado y a las técnicas de los ciberdelincuentes.

UNIVERSITAS STUDIORUM PIURENSIS

Lista de referencias

CISCO. (2018). *Reporte Anual de Ciberseguridad de Cisco 2018.*

Cortes, D. G. (s.f.). *Firewalls de nueva generación: La seguridad informática vanguardista.* Recuperado el 10 de octubre de 2020, de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00003329.pdf

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid. Recuperado el noviembre de 2020

Espinoza, R. (s.f.). *Benchmarking: qué es, tipos, etapas y ejemplos*. Recuperado el 24 de octubre de 2020, de robertoespinoza.es: https://robertoespinosa.es/2017/05/13/benchmarking-que-es-tipos-ejemplos

Instituto Nacional de Ciberseguridad. (20 de febrero de 2017). *Glosario de Términos de Ciberseguridad: una aproximación para el empresario*. Obtenido de Instituto Nacional de Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Instituto Nacional de Normalización. (2015). *Norma Chilena NCh ISO 27032. Tecnología de la información — Técnicas de seguridad — Directrices para la ciberprotección.* Instituto Nacional de Normalización. Recuperado el octubre de 2020

Manene, L. M. (28 de julio de 2011). *Diagramas de flujo: su definición, objetivo, ventajas, elaboración, fases, reglas y ejemplos de aplicaciones*. Obtenido de luismiguelmanene.com: http://www.luismiguelmanene.com/2011/07/28/los-diagramas-de-flujo-su-definicion-objetivo-ventajas-elaboracion-fases-reglas-y-ejemplos-de-aplicaciones/

Marina de Guerra del Perú. (s.f.). *Marina de Guerra del Perú*. Recuperado el 3 de octubre de 2020, de Portal Institucional de la Marina de Guerra del Perú: https://marina.mil.pe/es/nosotros/acerca-de/

Neyra, C. (30 de mayo de 2020). *Hackers vulneraron plataforma del Bono Familiar Universal para apropiarse de dinero*. (C. Neyra, Editor) Recuperado el octubre de 2020, de Diario

El Comercio: https://elcomercio.pe/lima/sucesos/coronavirus-en-peru-hackers-vulneraron-plataforma-del-bono-familiar-para-apropiarse-de-dinero-noticia/?ref=ecr

Panda Security. (s.f.). *En la cabeza del cibercriminal: ¿qué busca y por qué quiere atacar tu empresa?* Recuperado el 3 de octubre de 2020, de Panda Security.