UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIEROS ELECTRÓNICOS

TEMA:
SISTEMA DE SEGURIDAD PERIMETRAL PARA EL EDIFICIO ZEUS DE ARCOTEL BASADO EN TECNOLOGÍAS UTM DE CÓDIGO ABIERTO

AUTORES:
ANDRÉS MAURICIO PÉREZ LASSO
GABRIEL ELIAS PINTO GUTIÉRREZ

TUTOR:
JHONNY JAVIER BARRERA JARAMILLO

Quito, julio del 2019

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Andrés Mauricio Pérez Lasso con documento de identificación N° 1719716308 y Gabriel Elias Pinto Gutiérrez con documento de identificación N° 1722056767, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: "SISTEMA DE SEGURIDAD PERIMETRAL PARA EL EDIFICIO ZEUS DE ARCOTEL BASADO EN TECNOLOGÍAS UTM DE CÓDIGO ABIERTO", mismo que ha sido desarrollado para optar por el título de: Ingenieros Electrónicos, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la ley de propiedad intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Politécnica Salesiana.

Andrés Mauricio Pérez Lasso

Cédula: 1719716308

Gabriel Elias Pinto Gutiérrez

Cédula: 1722056767

Quito, julio del 2019

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo, Jhonny Javier Barrera Jaramillo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, "SISTEMA DE SEGURIDAD PERIMETRAL PARA EL EDIFICIO ZEUS DE ARCOTEL BASADO EN TECNOLOGÍAS UTM DE CÓDIGO ABIERTO", realizado por Andrés Mauricio Pérez Lasso y Gabriel Elias Pinto Gutiérrez, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, julio de 2019

Ing. Jhonny Javier Barrera Jaramillo

Cédula: 1400378475

DEDICATORIA

Existen caminos en la vida que van más allá del dolor y el temor, son aquellos caminos que liberan y nos arma de valor. Dedico el esfuerzo de este proyecto a Dios, leal amigo espiritual; por brindarme las bendiciones más grandes que poseo. A mi madre Cecilia, mujer innegable de amor sin condición que junto con mi padre Fausto, hombre de tesón; alcanzaron el máximo anhelo que pueden inculcar en los hijos como son el amor, dedicación y satisfacción del deber cumplido. Tía Fabiola Cartagena, mi segunda madre; por su aliento incondicional e inmenso desprendimiento, cumplo con una de las metas establecidas gracias a la confianza depositada. Mis hermanos Pablo, Daniel, Elizabeth y Sugey, ejemplo de compromiso, superación, entrega y humildad; precursores de este sueño que se convirtió en realidad. Mis sobrinas Pamela, Paula e Isabela; amores que me ha regalado Dios para motivarme, inspirarme y ser feliz. Finalmente, a los amigos de barrio que han sido como mis hermanos y los compañeros de cátedra por todas las travesías y consejos compartidos durante este ciclo de formación profesional.

ANDRÉS MAURICIO PÉREZ LASSO

Por la persistencia y esfuerzo, lo que parecía algo inalcanzable se convirtió en un éxito. Dedico el sacrificio de este proyecto al forjador de mi camino, mi padre celestial, que me acompaña y siempre me levanta de mi continuo tropiezo, a mis padres Rocío y Gabriel por haberme forjado como la persona que soy en la actualidad, ya que son el pilar fundamental en mi formación como persona, por proporcionarme valores, principios, perseverancia y empeño en todos mis logros obtenidos, ya que son las personas que me hay apoyado incondicionalmente para poder llegar a esta instancia de mi formación profesional; A mi hermana Melany por brindarme su alegría y amor incondicional; A mis compañeros ya que con ellos compartimos buenos y malos momentos aprendiendo día a día en la universidad como una familia y a cada persona que hizo posible este proyecto.

GABRIEL ELIAS PINTO GUTIÉRREZ

AGRADECIMIENTO

A Dios, por todas las bendiciones derramadas tanto en nuestra vida cotidiana como en la vida universitaria y profesional.

A la Universidad Politécnica Salesiana y todos los docentes que han sido participes de la carrera Ingeniería Electrónica; protagonistas fundamentales del desarrollo, evolución y formación intelectual como humanística; impartiendo sus conocimientos y habilidades para convertirnos en seres de progreso y capaces de hacerle frente al campo laboral.

Al Ing. Jhonny Barrera, tutor del presente proyecto de titulación, que con su apoyo, compromiso, dedicación y trabajo supo encaminarnos tanto el transcurso de nuestra formación profesional como del presente proyecto, con esmero y desinterés; al punto de considerarlo no solamente como nuestro tutor, sino un gran amigo y colega con el que siempre podremos contar.

A la Agencia de Regularización y Control de las Telecomunicaciones – ARCOTEL y todos los que son participes del departamento "Dirección de Tecnologías de la Información y Comunicación" en especial a los que conforman el área de Infraestructura, con un particular agradecimiento a los Ing. Freddy Gallegos, Ing. Giovanny Males, Ing. Christian Zhamungui e Ing. Maribel Saraguro, precursores y facilitadores del proyecto implementado.

Agradecimiento especial al Ing. Giovanny Males por su enorme paciencia y predisposición al depositarnos toda su confianza para facilitarnos, capacitarnos y compartir sus conocimientos, experiencias y consejos de manera desinteresada para el desarrollo del proyecto establecido.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

De acuerdo a las afirmaciones realizadas por muchos expertos, la seguridad de la información constituye actualmente una de las principales preocupaciones de las organizaciones. Algo que es perfectamente lógico y comprensible si se considera el creciente número de incidentes reportados sobre ataques informáticos a los activos de las empresas, principalmente en contra de la información, mucha de ella de tipo confidencial y a veces perteneciente a terceros (proveedores, clientes, etc).

Las brechas de seguridad o vulnerabilidades como también se les conoce, permiten a los ciberdelincuentes acceder de forma fraudulenta a información muy crítica como datos médicos, personales y/o bancarios, quienes no dudan en aprovechar esta ventaja para obtener beneficios propios casi siempre a expensas de exponer de forma inescrupulosa la información privada.

En nuestro país, las instituciones públicas y privadas están conscientes de esta realidad, razón por la cual se sitúa a la seguridad informática como un asunto de alta prioridad que está motivando la implementación de mecanismos de prevención y defensa contra las diversas amenazas informáticas existentes, a fin de prevenir ataques que pongan en riesgo sus procesos y servicios.

El presente proyecto, contempla una solución tecnológica implementada en la ARCOTEL para la administración unificada de amenazas o UTM por sus siglas en inglés (Unified Threat Management) basada en la herramienta Open Source PFsense. Para su desarrollo se realizaron un conjunto de pruebas de hackeo ético y pentesting que permitieron caracterizar las vulnerabilidades existentes y definir una línea base en la seguridad de la institución y a partir de ello desplegar un conjunto de estrategias de control para evitar posibles incidentes que puedan causar algún daño en la red de la institución.

ABSTRACT

According to the statements made by many experts, information security is currently one of the main concerns of organizations. Something that is perfectly logical and understandable if one considers the increasing number of reported incidents of computer attacks on the assets of companies, mainly against information, much of confidential and sometimes belonging to third parties (suppliers, customers, etc.).

Security gaps or vulnerabilities, as they are also known to allow cybercriminals to fraudulently access very critical information such as medical data, personal or banking, who do not hesitate to take advantage of this advantage to obtain their own benefits almost always at the expense of exposing private information unscrupulously.

The reality, why IT security is considered a high priority issue that is motivating the implementation of prevention and defense mechanisms against the various computer threats that exist to prevent attacks that put your processes and services at risk.

The present project contemplates a technological solution implemented in the ARCOTEL for the unified administration of threats or UTM by its acronym (Unified Threat Management) based on the Open Source PFsense tool. For its development, a set of ethical hacking and pentesting tests were carried out that allowed to characterize the existent vulnerabilities and to define a baseline in the security of the Institution and starting that deploy a set of control strategies to avoid possible incidents that could cause some damage in the network of the institution.

INTRODUCCIÓN

El presente proyecto técnico fue desarrollado en la Agencia de Regularización y Control de las Telecomunicaciones (ARCOTEL), y su principal objetivo fue contribuir con una solución tecnológica de código abierto para implementar un sistema de seguridad perimetral y asegurar los activos de información más importantes de la institución señalada. De igual forma, esta solución se alinea con el decreto gubernamental en relación al uso de software libre para el desarrollo de las actividades de nivel gerencial, administrativo y servicios en empresas públicas.

El edificio Zeus, donde funcionan los principales departamentos de ARCOTEL, se considera como el punto de concentración de la información más importante de esta secretaria de estado; debido a ello es considerado como un objetivo de alto riesgo ante cualquier intento de ataque cibernético. Esta realidad impulsó a sus autoridades a definir un plan de acción preventivo para proteger la información, evitar pérdidas u alteración de los datos y reducir riesgos a los servicios de red utilizados por la institución.

Uno de los componentes del proyecto, se centra en la evaluación de los servidores institucionales con el fin de detectar posibles riesgos, para lo cual se procedió a analizar el desempeño del sistema actual que se basa en el fabricante PaloAlto analizando las brechas de seguridad que pudieran comprometer la red. Como resultado de esta evaluación, se generó un reporte con las vulnerabilidades encontradas para gestionar y prevenir posibles amenazas que puedan explotar la red.

Posteriormente se analizaron varias alternativas de solución de nueva generación que permitan prevenir, detectar y actuar ante amenazas informáticas que atenten contra la confidencialidad, integridad y disponibilidad de la información, mediante un sistema UTM convergente.

Finalmente, se realizó la implementación del sistema PFsense de código abierto, el cual posee un amplio repositorio de herramientas orientadas a atender diferentes aspectos de la seguridad informática y que además permite integrar múltiples servicios como antivirus, IPS e IDS, filtrado de contenido entre otros; a través de una plataforma de virtualización VMware vSphere 5.5, como solución alternativa a PaloAlto implementada en la ARCOTEL.

CAPÍTULO 1

ANTECEDENTES

1.1 Planteamiento del problema

Actualmente la seguridad informática constituye uno de los puntos estratégicos que aseguran el normal desenvolvimiento de las instituciones ya sean públicas o privadas. Durante los últimos años, este campo ha tomado vital importancia en nuestro país debido principalmente a los ataques masivos a los que se han enfrentado varias Instituciones gubernamentales como la Presidencia de la República, Cancillería del Ecuador, Banco Central del Ecuador, Ministerios y varios Municipios los cuales se han visto seriamente comprometidos.

La ARCOTEL es considerada una de las Instituciones más importantes que se encuentra al servicio del estado ecuatoriano, lo cual la convierte en un objetivo susceptible y de alto riesgo a cualquier tipo de amenaza u ataque orientado a violentar la seguridad de la red de la entidad.

La delicada situación que experimenta esta organización frente a los posibles ataques, la ha obligado a optar por una solución tecnológica que garantice el desempeño normal de su infraestructura de red; y que unifique los servicios de seguridad, manteniendo la independencia tecnológica y contribuyendo con el decreto gubernamental.

1.2 Justificación

Considerando las funciones que desempeña y los objetivos estratégicos de la ARCOTEL, la seguridad de la información debe atenderse como una situación de alta prioridad, y que coadyuve a la integración de diversas estrategias encaminadas a minimizar los riesgos y optimizar la protección de sus activos frente a las vulnerabilidades que presente en esta entidad.

Una de las estrategias más utilizadas para la inspección y detección de vulnerabilidades dentro de una infraestructura tecnológica, es aplicar pruebas controladas de hacking ético con el propósito de hallar debilidades en los sistemas de seguridad, para posteriormente definir medidas correctivas y preventivas a fin de evitar que algún tipo

de amenaza se derive en un ataque que comprometa el desempeño de sus recursos informáticos.

La solución que se plantea se centra en la implementación de una plataforma Open Source que integre varios servicios de seguridad, basado en un Sistema conocido como UTM por sus siglas en inglés (Unified Threat Management); el cual se orienta a la gestión unificada de las amenazas en la red desde un solo dispositivo o sistema. Con esta decisión se pretende migrar hacia un UTM Open Source llamado PFsense, para cumplir con el decreto estipulado y centralizar el control de vulnerabilidades a través de herramientas de apoyo a sus servicios y procesos, sin exponer la información que circula en sus redes y sistemas.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar un sistema de seguridad perimetral en el edificio Zeus de ARCOTEL por medio de un UTM basado en herramientas open source para optimizar la gestión de la seguridad de información.

1.3.2 Objetivos Específicos

- Realizar un estudio inicial de la red de ARCOTEL para determinar sus fortalezas y debilidades.
- Aplicar técnicas controladas de hackeo ético para explotar las vulnerabilidades y brechas de seguridad en la red de la empresa.
- Realizar un estudio comparativo para seleccionar la alternativa de UTM Open Source que más se ajuste a las necesidades de la organización.
- Migrar el UTM de herramientas propietarias hacia un UTM fundamentado en OSS para la gestión de los módulos firewall, IDS, IPS y filtrado de contenidos.
- Realizar pruebas de pentesting para evaluar la solución implementada y establecer el nivel de seguridad de la organización.

1.4 Marco conceptual

1.4.1 Análisis de Trafico

1.4.1.1 Throughput

Se define como la capacidad efectiva de transferencia de datos sobre el enlace, medido en bits por segundo (bit/s o bps), donde influyen algunos factores como son la cantidad de tráfico, tipo de tráfico y la latencia. (Cisco, 2013)

1.4.2 Concepto y distribución de sistemas de código abierto

1.4.2.1 FreeBSD (Free Berkeley Software Distribution)

Sistema operativo libre avanzado para arquitecturas x86 derivado de BSD UNIX, versión desarrollada por la universidad Berkeley de California, con altas prestaciones en rendimiento, comunicaciones de red, seguridad y compatibilidad, sistema el cual es mantenido y mejorado por numerosas personas como equipo de contribución para arquitecturas futuristas en fases de implementación. (FreeBSD, 2014)

1.4.2.2 OSS (Open Source Software)

El software de código abierto es un software informático el cual no requiere de licenciamiento y su código fuente es público, permitiendo al portador manipular, modificar, mejorar y redistribuir el software con el fin de un propósito específico. (Fundation, 2019)

1.4.3 Consultorías de mercado

1.4.3.1 Cuadrante mágico de Gartner

Elaborado por grupo Gartner, empresa especializada en la consultoría e investigación del mercado. Es un método de ranking gráfico con publicación anual de los fabricantes con mejores soluciones y productos de las nuevas tendencias tecnológicas. (Big Data Marker, 2015)

1.4.3.2 IT Central Station

El IT Central Station es una plataforma dinámica de conocimiento colaborativo con revisiones y recomendaciones que ofrece información fiable, objetiva y relevante para tecnologías empresariales; permitiendo a los expertos en TI empresarial y startups compartir su experiencia a la comunidad de tomadores de decisiones tecnológicas. (Russell Rothstein y Naftali Marcus, 2013)

1.4.4 Dispositivos de entorno virtual

1.4.4.1 Hypervisor

Hipervisor o monitor de máquina virtual es una plataforma donde se incorpora diversas técnicas de control que permiten la integración de distintos sistemas operativos mediante un hardware físico subyacente. (Recio, 2015)

1.4.4.2 UCS (Unified Computing System)

Es una plataforma informática integrada para la siguiente generación de data center donde incorpora el computo, la red, el acceso, el almacenamiento y la virtualización dentro de un sistema integral con el propósito de reducir el costo de propiedad e incrementar la agilidad de la compañía. (Cisco, 2010)

1.4.5 Herramientas de Seguridad Informática

1.4.5.1 IDS (Intrusion Detection System)

Sistema de seguridad preventivo para monitorización de la red; este examina intentos no solicitados de acceso o cualquier actividad sospechosa. El IDS se comporta de manera pasiva, detecta los ataques, mas no los detiene y las emite mediante alertas anticipadas dirigidas a los administradores de sistemas. (Panda Security S.L., 2018)

1.4.5.2 IPS (Intrusion Prevention System)

Dispositivo de hardware o software donde se ejecuta el control de acceso en una red para la identificación y bloqueo ante cualquier actividad maliciosa. El IPS se comporta de manera activa, detecta los ataques; en consecuencia, los detiene de forma automática e inmediata regida en una serie de reglas en el firewall corporativo. (Panda Security S.L., 2018)

1.4.5.3 UTM (Unified Threat Management)

La gestión unificada de amenazas o UTM es un elemento de seguridad que integra en un solo dispositivo herramientas de seguridad primordiales como son antivirus, antispyware, antispam, firewall, IPS, IDS, filtrado de contenido y prevención de fugas, entre otros, otorgando simplicidad y facilidad de administración. (Kaspersky Lab., 2016)

1.4.6 Seguridad de la Información

1.4.6.1 Confidencialidad

Solamente las personas autorizadas pueden tener acceso a la información, es decir que cualquier otro individuo no debe tener ningún acceso a los datos, la forma principal de proteger dichos datos es cifrarlos antes de enviarlos a través de la red. (Santos & Stuppi, Networking Security Concepts, 2015)

1.4.6.2 Disponibilidad

Aplica a los datos y sistemas, si la red o sus datos no están disponibles a usuarios autorizados, tal vez está ocurriendo a un ataque de denegación de servicio o a un fallo general de la red. (Santos & Stuppi, Networking Security Concepts, 2015)

1.4.6.3 Integridad

Los datos pueden ser cambiados solo por el personal o sistemas autorizados, es decir se refiere a la fiabilidad de la información, estos datos deben estar completos, sin variaciones para considerarlo confiable y exacto. (Santos & Stuppi, Networking Security Concepts, 2015)

1.4.7 Metodología de Auditoría para Seguridad en la red

Las pruebas de pentesting dependen de los recursos disponible en la empresa, es decir que cada empresa es un mundo diferente, las personas capacitadas que auditan adoptan cierta manera o metodología para llevarlas a cabo que puede tratarse de:

- Pasos prácticos que se desarrollan con listas de comprobación.
- OSSTMM- Open-Source Security Testing Methodology Manual.
- Estrategias particulares para un ataque especifico.

1.4.7.1 Pasos prácticos que se desarrollan con listas de comprobación.

Esta metodología implica listas o plantillas que contengan objetivos a realizar pruebas, información recopilada en hardware y software, podrá o no incluir: (Verdesoto, 2007).

- Características de equipos que tiene la organización
- Información de la organización

- Seguridad física de equipos y dispositivos de red.
- Detalle de aplicaciones y protocolos abiertos por equipos.
- Detalle de puertos abiertos por equipo.
- Detalle de Software utilizado para pruebas.

1.4.7.2 Open Source Security Testing Methodology Manual.

El Manual de la Metodología Abierta de Pruebas de Seguridad, creado por Peter Herzog, con el objetivo de realizar pruebas controladas de penetración tomando en cuenta áreas de seguridad como: (Verdesoto, 2007)

- Seguridad de la información
- Seguridad en los procesos
- Seguridad de tecnologías de internet
- Seguridad en las comunicaciones
- Seguridad Inalámbrica
- Seguridad física.

1.4.7.3 Estrategias particulares para un ataque específico.

Esta metodología se adapta con fines específicos para una organización se crea pasos o instrucciones para ejecutar un objetivo en particular, ya sea auditar red de la organización, pruebas de Pen-test, instalar software, configuraciones especificas u otras actividades con un orden especifico.

Esta metodología hace relación a una tarea planteada y ejecutada por el administrador del proyecto, en base a conocimientos especializados acerca de Ethical Hacking. (Verdesoto, 2007)

1.4.8 Fases para realizar pruebas de Ethical Hacking.

1.4.8.1 Recolección de Información

Se recopila toda la información posible importante para el test con la mayor cautela con la finalidad de encontrar puntos vulnerables, este proceso usa la técnica de footprinting, se pretende de manera discreta elaborar un aprendizaje de cualquier aspecto mínimo de la red u organización, puede incluir clientes, empleados, operaciones, red y sistemas de una organización, no se pretende penetrar en la red, más bien identificar y documentar información. (Maria Narváez, 2018)

1.4.8.2 Identificación de servicios y protocolos.

Esta fase toma como principio la fase de reconocimiento, el probador escanea la red por información más específica en base a la información obtenida durante el reconocimiento de información, puede incluir el uso de diales, escaneadores de puertos, mapeos de red, sweeping, escaneador de vulnerabilidades. Un aspecto importante del escaneo es importante detectar los servicios que se encuentran publicados, identificación de aplicaciones y versiones del sistema operativo, extracción de banners entre otros. (Astudillo K., 2018)

1.4.8.3 Análisis de Vulnerabilidades

Durante este proceso se ejecuta tareas para detectar vulnerabilidades con herramientas de uso libre o licenciadas, esta actividad engloba identificación de vulnerabilidad de los servicios usando banners, explotación y verificación de falsos positivos y falsos negativos, enumeración y clasificación de vulnerabilidades halladas, estimar rutas, impacto y escenarios para su explotación. (Astudillo K., 2018)

1.4.8.4 Exploits de Vulnerabilidades

La explotación de vulnerabilidades y pruebas de intrusión se las realizan verificando si las vulnerabilidades son encontradas, las pruebas pueden contener intrusiones manuales, inyección de código Sqlmap, Ataques a la capa de red, trasporte y aplicación, intentos de autenticación por medios de fuerza bruta diccionarios de usuarios y contraseñas. (Ortiz, 2015)

1.4.8.5 Reporte

El informe se encarga de mostrar de forma clara y comprensible la información útil adquirida en las diferentes fases, es decir el auditor genera un reporte detallado con la explicación de los resultados encontrados de las vulnerabilidades y soluciones que se le recomienda a la empresa tome en cuenta para mejorar la seguridad del sistema. (Astudillo K., 2018)

1.4.9 Herramientas para Ethical Hacking.

1.4.9.1 Nslookup

Es un software de código abierto para consultar información sobre servidores DNS (Domain Name System) que se encuentran en el internet. (Maria Narváez, 2018)

1.4.9.2 Whois

Es una herramienta útil para enlistar y encontrar los detalles del dominio en todos los sistemas operativos basados en Linux. (Maria Narváez, 2018)

1.4.9.3 Nmap

Network Mapper es un escáner de red de código abierto para descubrir hosts, puertos y servicios en una red local e Internet. (Security Offensive, 2019)

1.4.9.4 Nessus

Es una solución de evaluación de vulnerabilidad en diversos sistemas operativo que previene ataques de red con Tenable Nessus Professional. (Tenable, 2019)

1.4.9.5 Slowloris

Es un tipo de herramienta para Denegación de Servicio creada por Robert Hansen que permite apagar una máquina de la red desde otra máquina. (Imperva, 2019)

1.4.10 Especificación de Vulnerabilidades y Riesgos.

1.4.10.1 National Vulnerability Database (NVD).

Es el repositorio del gobierno de los Estados Unidos incluye bases de datos de listas de control de seguridad, fallas de software, errores de configuración, nombres de productos y métricas de impacto, se puede encontrar en la siguiente página https://nvd.nist.gov/. (Ortiz, 2015)

1.4.10.2 Common Vulnerabilities and Exposures

En esta base de datos se encontrará información con fechas actualizadas y su descripción de las vulnerabilidades reportadas, se puede dirigir a la página siguiente https://cve.mitre.org/.(Ortiz, 2015)

1.4.10.3 Tenable Network Security

La herramienta de los desarrolladores de Nessus, poseen una base de datos para poder consultar información de vulnerabilidades, el sitio web es el siguiente http://www.tenable.com/ (Ortiz, 2015)

1.4.11 Cuantificación de la importancia

Una vez tenemos clasificados los activos de la red corporativa y sus vulnerabilidades explotables, se procede a realizar una evaluación en el contexto del sistema, este proceso de la importancia se suele llevar también mediante los escáneres de vulnerabilidades ya que cuentan con sus propias puntuaciones para cada vulnerabilidad como podrían ser Qualys, Nessus o Acunetix. (Maria Narváez, 2018)

Tabla 1.1 Clasificación de Severidad de Vulnerabilidades

Severidad	Valor	Criterio
Critica	10	Situaciones que comprometen directamente a la víctima o logran ingreso no autorizado con privilegios de SYSTEM
Alta	7 - 9.99	Situaciones que comprometen directamente a la víctima o logran ingreso no autorizado, pero sin privilegios de SYSTEM
Media	4.1 - 6.99	Situaciones que no resultan inmediatamente una oportunidad de acceso, sin embargo, proporcionan una capacidad o información que junto a otras dan lugar a compromiso o acceso no autorizado a la red
Baja	0.1 – 4	Situaciones que no resultan directamente en el compromiso de la red, sistema, aplicación o información
0	0	Información que no compromete a los sistemas en absoluto

Clasificación de Severidad de Vulnerabilidades. Elaborado por Tenable-Nessus

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN INICIAL

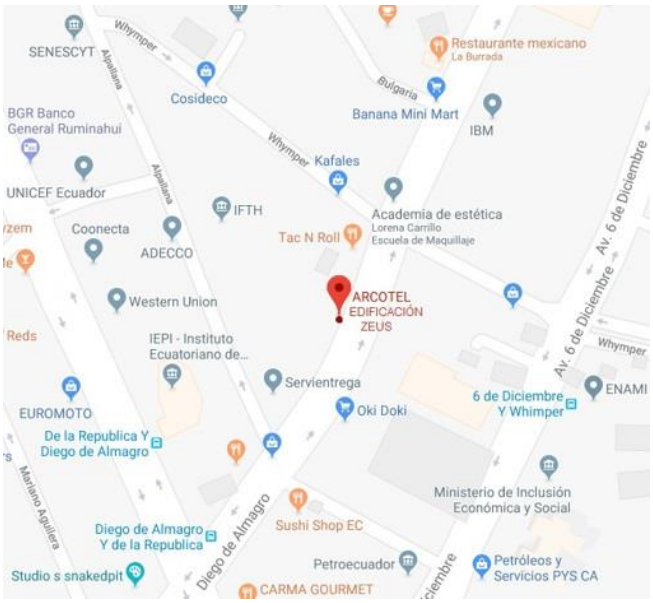
2.1 Información General de la ARCOTEL

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), se forma a partir de una normativa definida en la Ley Orgánica de Telecomunicaciones misma que fue aprobada en pleno de la Asamblea Nacional y su objetivo es el fortalecimiento de la estructura institucional y así como de los procesos de regulación y control de las telecomunicaciones, para garantizar los derechos de los usuarios a través de servicios de calidad con acceso libre a las tecnologías de la información y comunicación.

2.1.1 Ubicación de la Matriz ARCOTEL

La matriz de la ARCOTEL funciona en el edificio ZEUS, localizado en el Centro Norte de la ciudad de Quito, específicamente en la Av. Diego de Almagro N31-95 entre las calles Whymper y Alpallana.

Figura 2.1 Ubicación del Edificio Zeus de ARCOTEL



Ubicación del Edificio Zeus de ARCOTEL. Elaborado por: Andrés Pérez y Gabriel Pinto

2.1.2 Misión

Regular, controlar y administrar el uso, aprovechamiento y explotación del espectro radioeléctrico y los servicios del régimen general de las telecomunicaciones para garantizar el derecho de acceso a servicios convergentes con cobertura y disponibilidad optimas; en un ambiente de competencia, universalidad y aprecios asequibles, precautelando la seguridad de las comunicaciones y protección de datos en todo el territorio nacional.

2.1.3 Visión

Constituirse en un modelo de organismo de regulación, administración y control del espectro radioeléctrico y los servicios del régimen general de las telecomunicaciones a nivel regional.

2.2 Levantamiento de Información

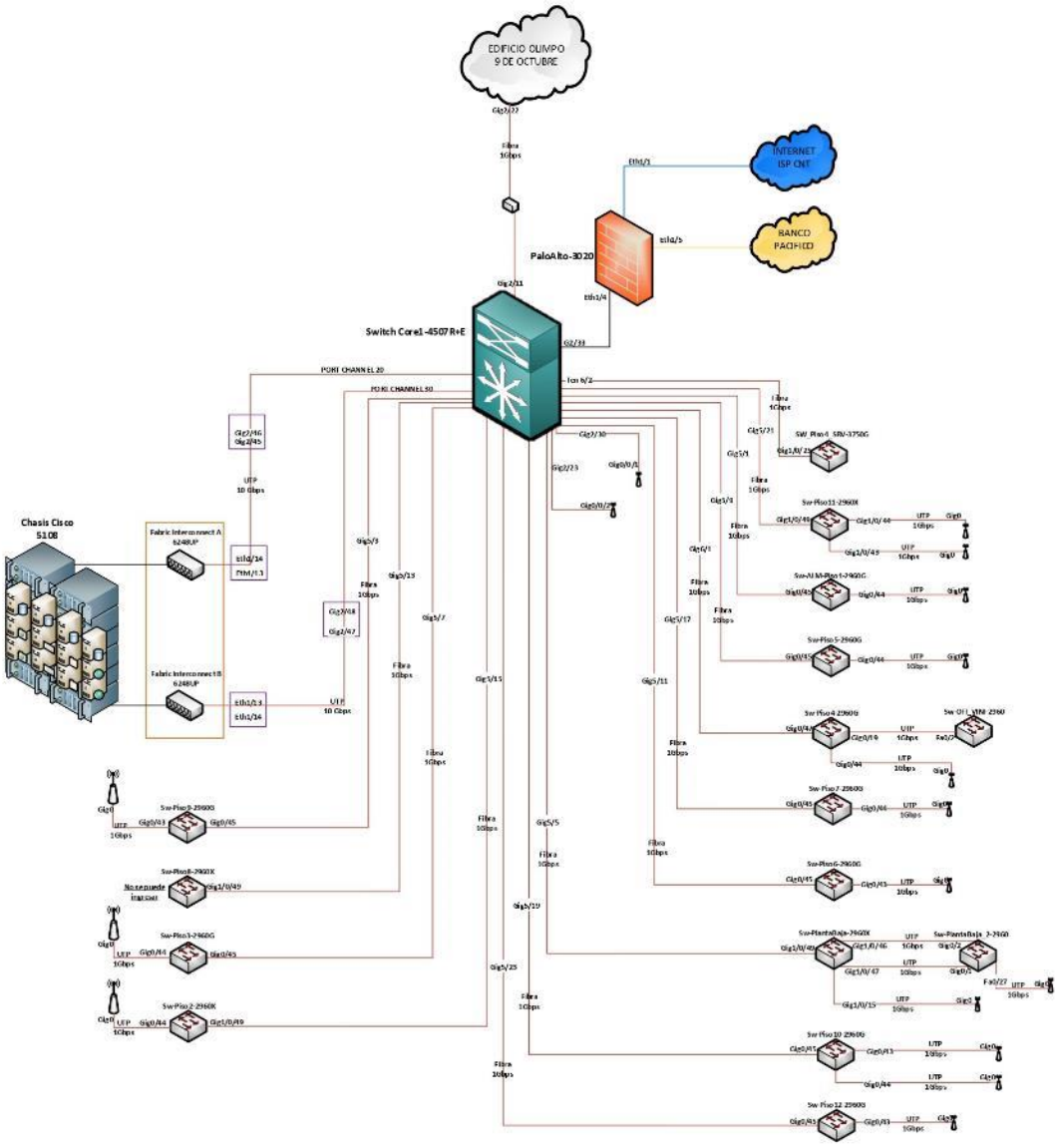
2.2.1 Topología Física de la Red

Actualmente, la infraestructura de la red LAN del edificio Zeus ARCOTEL se basa en un modelo jerárquico de núcleo colapsado, en el cual la capa de núcleo y distribución se fusionan en una sola, y a partir de ella se despliegan directamente los dispositivos de la capa de acceso.

La capa de núcleo se soporta en un switch 4507R+E como dispositivo central, el cual se encarga de la convergencia entre los distintos enlaces procedentes del edificio Olimpo de ARCOTEL, los switches de la capa de acceso y los Fabric InterConnect 6248UP que consecutivamente conectan con el chasis Cisco UCS 5108. A través de este switch central se derivan hacia la única conexión con PaloAlto 3020 como se aprecia en la figura 2.2

Los switches de la capa de acceso poseen enlaces troncalizados para transferir las distintas Vlans hacia el dispositivo central, además los multienlaces configurados mediante EtherChannel destinados a los Fabric InterConnect permiten el ingreso a los distintos servidores concentrados en el UCS, desde el cual se deriva un enlace dedicado hacia el firewall PaloAlto 3020,el mismo que filtra el tráfico generado de los switches de acceso, así como de varios servidores y Access Point que tienen como destino al Internet o el Banco del Pacífico.

Figura 2.2 Topología actual de la red



Topología actual de la red. Elaborado por: Andrés Pérez y Gabriel Pinto

Los Switches de acceso C2960X y C2960G son dispositivos administrables que se encargan de la interconexión entre varios dispositivos finales como PC's, teléfonos IP, Access Point e impresoras de los distintos departamentos.

Los dispositivos Fabric InterConnect 6248UP son switches principales que interconectan el UCS con la SAN y funcionan esencialmente como bastidores de comunicación encargados de enlazar estos componentes a los servidores. Se dispone de un Cisco UCS 5108 Blade Server de 8 slots B200 M2, cada uno posee un procesador Intel Xeon E5649 a 2.53GHz, 48GB RAM y 12 Mb de memoria cache conectados con una SAN de 24 discos SAS 600Gb a 10K de revoluciones para el soporte de

almacenamiento; toda esta infraestructura se gestiona por el Hipervisor VMware ESXi 5.5 donde se alojan diversos servidores virtuales tanto privados que son de uso exclusivo para los distintos departamentos de la ARCOTEL, como públicos que pueden acceder desde cualquier red de Internet.

Los servidores privados que posee ARCOTEL son:

- Base de datos SIRATV y SPECTRA PLUS
- Servicios financieros: Facturación electrónica y Banco del Pacifico;
- Seguridad: F-Secure (para servidores virtuales y ESET Nod32 para los dispositivos finales y resto de servidores;
- Antispam : Sophos para el correo público e institucional y
- IPS: de la línea comercial McAfee para el enlace LAN.

En relación a los servidores públicos cabe señalar que se gestionan tanto en el edificio Zeus como Olimpo; sin embargo, los servicios administrados que se ubican en la matriz son correo electrónico y acceso web, los mismos que se encuentran publicados desde la red interna hacia Internet.

En cuanto a la gestión de seguridades de la información existentes en ARCOTEL, cabe mencionar que la mayoría del control del tráfico se concentra en el Appliance Firewall PaloAlto 3020, el cual está configurado para brindar seguridad perimetral y actúa como un único punto crítico de contención de las comunicaciones hacia y desde los servidores en base a varias políticas de seguridad que se centran en registrar principalmente las amenazas originadas desde el Internet. Este dispositivo emplea un software propietario llamado PAN-OS, el cual exige de un pago anual de licenciamiento para garantizar su normal funcionalidad, así como las actualizaciones y el respectivo soporte.

2.2.2 Direccionamiento Lógico de la Red

Los departamentos de ARCOTEL se encuentran organizados bajo un esquema de direccionamiento IPv4, distribuido en un conjunto de Vlans configuradas en un switch 4507R+E y que se describen en la Tabla 2.1

Tabla 2.1 Direccionamiento lógico de la red

Vlan	Red	Gateway
Conex. Olimpo	172.20.X.X/24	172.20.X.X
Internet CNT	192.168.X.X /24	192.168.X.X
Servidores	192.168.X.X/24	192.168.X.X
Conatel	192.168.X.X/24	192.168.X.X
Secretaria Gral.	192.168.X.X/24	192.168.X.X
Conatel Int.	192.168.X.X/24	192.168.X.X
Telecomunicaciones	192.168.X.X/24	192.168.X.X
Jurídico	192.168.X.X/24	192.168.X.X
Contraloría Ges.	192.168.X.X/24	192.168.X.X
Financiero	192.168.X.X/24	192.168.X.X
Espectro Ges.	192.168.X.X/24	192.168.X.X
Informática	192.168.X.X/24	192.168.X.X
Desarrollo	192.168.X.X/24	192.168.X.X
Planificación	192.168.X.X/24	192.168.X.X
Auditoria	192.168.X.X/24	192.168.X.X
Regionales	192.168.X.X/24	192.168.X.X
Telf. Inalámbrica	192.168.X.X/24	192.168.X.X
Wifi Publica	192.168.X.X/24	192.168.X.X
Wifi VIP	192.168.X.X/24	192.168.X.X
Administración	192.168.X.X/24	192.168.X.X
VoIP	192.168.X.X/24	192.168.X.X
Red Wifi	192.168.X.X/24	192.168.X.X
Cámaras Accesos	192.168.X.X/24	192.168.X.X
Contraloría	192.168.X.X/24	192.168.X.X

Direccionamiento lógico de la red. Elaborado por: Andrés Pérez y Gabriel Pinto

Las interfaces del Firewall PaloAlto 3020 que interconectan con las redes Internet y Banco del Pacifico se describen en la Tabla 2.2

Tabla 2.2 Interfaces Palo Alto Firewall

Interfaz	Red	Gateway
FastEhternet 1 / 1	ISP	200.107.X.X/27 200.107.X.X--X/32
FastEhternet 1 / 4	192.168.X.X/24	192.168.X.X
FastEhternet 1 / 5	192.168.X.X/24	192.168.X.X

Interfaces Palo Alto Firewall. Elaborado por: Andrés Pérez y Gabriel Pinto

2.2.3 Distribución de equipos finales

Actualmente, el edificio Zeus cuenta con 13 plantas, en las que se ubican de forma planificada las direcciones de los departamentos que conforman el organismo público, y que se presentan en la Tabla 2.3

Tabla 2.3 Distribución de Equipos Finales

Planta	Dirección	Número de Empleados	Número de Hosts
Planta Baja	Recepción	8	19
Planta 1	Financiero	9	22
Planta 2	Administración	9	21
Planta 3	Telecomunicaciones	10	21
Planta 4	Espectro Electromagnético	8	23
Planta 5	Jurídico	7	19
Planta 6	Auditoria	10	23
Planta 7	Planificación	8	19
Planta 8	Desarrollo	10	22
Planta 9	Informática	9	22
Planta 10	Contraloría	10	23
Planta 11	Secretaria Gral.	7	18
Planta 12	Ejecutiva	8	20

Distribución de Equipos Finales. Elaborado por: Andrés Pérez y Gabriel Pinto

2.2.4 Equipos Tecnológicos de Telecomunicaciones.

El equipamiento activo de la matriz que está administrado por el departamento de Tecnologías de la Información y Comunicación se describe a continuación:

Tabla 2.4 Catalogación de Equipos Activos de Telecomunicaciones

Equipo	Marca	Modelo	Cantidad
Switch de núcleo colapsado	Cisco	C4507R+E	1
Chasis UCS	Cisco	5108	1
Fabric InterConnect UCS	Cisco	6248UP	2
Switch	Cisco	C2960	2
Switch	Cisco	C2960G	9
Switch	Cisco	C2960X	4
Switch	Cisco	C3750G	1
AP	Cisco	AIR-CAP2602E	17
Firewall	PaloAlto	3020	1

Catalogación de Equipos Activos de Telecomunicaciones. Elaborado por: Andrés Pérez y Gabriel Pinto

2.2.5 Servicios de red

Los servidores de acceso público que se gestionan en el edificio matriz son:

2.2.5.1 Servidor de Aplicaciones Web

Este servidor virtual cuenta con 2vCPU Intel Xeon E5649 2.53Ghz, 6Gb de RAM y 150Gb de almacenamiento, con las siguientes plataformas instaladas:

- Sistema operativo con Windows Server 2008 R2 Standard a 64bits.
- F-Secure Antivirus, como solución de antivirus del servidor.
- Microsoft Visual C++ 2008 Redistributable, para el uso de ciertos programas programados con Visual C++.
- Microsoft Policy Plataform, para permitir que los clientes evalúen la configuración de cumplimiento.
- Crystal Reports Basic Runtime for Visual Studio 2008, como generador de informes desde distintas bases de datos.

2.2.5.2 Servidor de Correo Electrónico

El servidor presenta 4vCPU Intel Xeon E5649 2.53Ghz, 8Gb de RAM y 1Tb de almacenamiento, con las siguientes plataformas instaladas:

- Sistema operativo con Windows Server 2008 R2 Standard a 64bits.
- ESET file security, como solución de antivirus y antimalware del servidor.
- ESET management agent, para administración remota de ESET file security.
- F-Secure PSC Prerequisities, como solución de anti-phishing del servidor.
- Microsoft Exchange 2007 Enterprise, como servidor de correo electrónico.
- Microsoft SQL Server 2005 Express Edition, como motor de base de datos para las aplicaciones de la empresa.
- Microsoft Visual C++ 2008 Redistributable, para el uso de ciertos programas programados con Visual C++.

2.3 Problemas detectados

De acuerdo al análisis realizado en la infraestructura tecnológica de ARCOTEL, a continuación, se detallan los problemas más importantes, relacionados con la seguridad:

- Los equipos activos que conforman la infraestructura de telecomunicaciones no han sido auditados ni evaluados dentro de estos últimos 2 años, lo cual ha generado incertidumbre sobre el estado real de los riesgos de seguridad a los que se ve expuesto la Entidad Gubernamental.
- El acceso hacia y desde los servidores públicos existentes (web y correo electrónico) presentan un peligro potencial, ya que están expuestos al Internet sin una adecuada protección. Considerando que estos equipos se encuentran en la red interna se convierten en un factor de alto riesgo con puntos de vulnerabilidad que deben ser corregidos.
- Los servicios de seguridad existentes como son los antivirus ESET Nod32 y F-Secure, el antispam perteneciente a Sophos y el IPS de línea comercial McAfee, están configurados para funcionar bajo sus respectivas plataformas, provocando que la gestión de seguridad sea dispersa y genere servicios heterogéneos e inconexos.
- El firewall PaloAlto constituye el único dispositivo que centraliza casi todas las funciones de seguridad de la institución, convirtiéndolo en un punto crítico que afronta las amenazas externas. Su fecha de licenciamiento anual está próxima a caducar, lo cual provocaría que se suspendan sus actualizaciones y el soporte, convirtiéndolo así en un elemento de alto riesgo.
- Finalmente, se debe indicar que todas estas situaciones están sujetas al uso de herramientas propietarias lo cual se contraponen al decreto ejecutivo No. 1014, mismo que resalta el empleo de software de código abierto para los sistemas y equipamientos informáticos en instancias de la administración pública.

2.4 Requerimientos

De acuerdo a los problemas detectados, los requerimientos más importantes que tiene ARCOTEL en cuanto a sus sistemas de seguridad son:

Realizar pruebas de pentesting a los aplicativos que se presentan expuestos en el internet para definir los riesgos de seguridad, determinando las amenazas y vulnerabilidades de los servidores como Web y Correo.

Realizar un análisis de riesgos en la red para establecer las amenazas existentes y establecer medidas preventivas o correctivas viables que garanticen un nivel de seguridad satisfactorio.

Realizar una evaluación comparativa de varias soluciones de UTM basadas en código abierto que permitan reemplazar las propuestas comerciales, garantizando una alternativa rentable/efectiva como sustitución al Firewall perimetral empleado actualmente.

Centralizar los módulos de seguridad como el Firewall, IPS e IDS a través de una solución integral UTM, con el fin de asegurar la gestión y el desempeño normal del equipamiento informático de los distintos departamentos.

Instalar y configurar los distintos módulos del Sistema UTM Open Source seleccionado, contribuyendo al cumplimiento del decreto ejecutivo y que exima a la ARCOTEL de los elevados costos de licenciamiento anual.

CAPÍTULO 3

PRUEBAS DE PENTESTING Y HACKEO ÉTICO

Para el desarrollo del presente proyecto, se aplicará una metodología que abarca tres fases: Pruebas de Pentesting, Análisis de Riesgos, Evaluación técnica y Selección de soluciones UTM, las mismas que se describen a continuación:

3.1 FASE I: Pruebas de Pentesting

La plataforma a usar es Kali Linux versión 2018, la misma que se basa en GNU/Linux Debian, y que permitirá el despliegue de pruebas de penetración y auditorías de seguridad. Este SO se instalará en una máquina virtual VMware Workstation 15, y a partir de ella se realizarán pruebas de pentesting que permitirán entre otros aspectos recolección de información, identificación de sistemas y servicios, así como el análisis de vulnerabilidades, exploits y el respectivo reporte.

3.1.1 Recolección de Información

Una de las herramientas básicas para recolección de información que se usará es Nslookup que permitirá conocer las direcciones IP públicas, la respuesta del DNS de la página de Arcotel (www.arcotel.gob.ec) es 200.107.22.227, ver anexo 7.

Desde la plataforma Kali Linux, se usó el comando whois arcotel.gob.ec, para obtener información sobre el ISP (Proveedor de Servicio), tales como el nombre del proveedor: Corporación Nacional de Telecomunicaciones – CNT, el nombre del contacto: “Sandra López”, y otra información como la ubicación y dirección exacta, número de teléfono, rango de IP's públicas, como se aprecia en el anexo 8.

Usando el motor de búsqueda de Google se pudo confirmar la geolocalización del dominio, en la página web www.iplocation.net, se examina diferentes bases de datos, la latitud de -0.2298 con longitud de -78.5249 para la ciudad de Quito en IP2Location y la latitud de -1.2500 con longitud de -78.6167 para la ciudad de Ambato en ipinfo.io, ver anexo 9.

El comando who.is aportó la siguiente información de dominios: pichincha.andinanet.net para Quito y tungurahua.andinanet.net para Ambato. Ambos

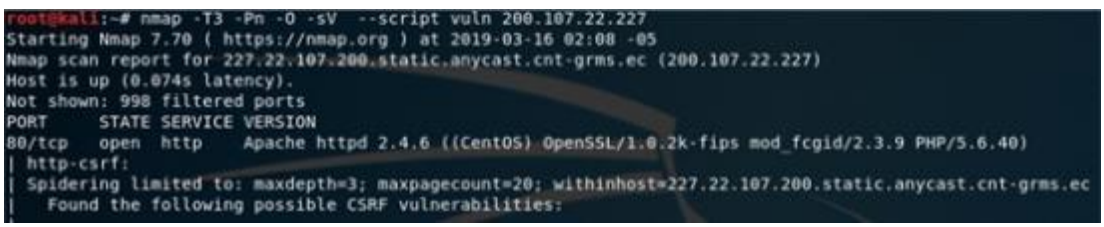
con un registro “NS” (Name Server) que determina el nombre del servidor autorizado; “A” se refiere a su dirección que se mapean normalmente para direcciones IPV4; “MX” (Mail Exchange) usado en intercambio de correo y “SOA” (Comienzo de Autoridad) almacenando información como última fecha de actualización, ver anexo 10.

Se verificó los dominios y subdominios relacionados con ARCOTEL, primero se extrajo el archivo “index.html” de la página principal y se filtró solamente las URL del archivo, de esta manera se observa el dominio del servidor web (arcotel.gob.ec) y servidor de correo (mail.arcotel.gob.ec) con ayuda del comando: grep “href=” index.html | cut -d “/” -f 3 | grep "\." | cut -d "" -f 1 | sort -u; “href” realiza una filtración indicando que se extraiga las líneas en el archivo que contengan URL´s como: https://mail.arcotel.gob.ec/, se delimitó con slash “/” y se extrajo el tercer campo de tal manera que queda (mail.arcotel.gob.ec) debido a que se realizara la traducción de los dominios, como se observa en el anexo 11 y 12; Se tradujo las URL´s del archivo arcotel.txt a sus direcciones IP´s con el comando: for url in$(cat arcotel.txt) < do host $url; done | grep “has address” | cut -d “ ” -f 4 | sort -u; el comando host realizó el DNS y el comando grep filtró las líneas donde se encuentra las direcciones y las imprimió, en el anexo 14 se evidencia las direcciones del Servidor WEB (200.107.22.227) y Correo (200.107.22.232).

3.1.2 Identificación de Sistemas y Servicios.

Utilizando las IP´s Públicas obtenidas en la fase anterior, se realizó un escaneo con Nmap para caracterizar los servicios de red activos. Se utilizó un Script de Nmap, sus comandos como T3 que realiza un escaneo por defecto este valor puede variar en el rango de 0 (sigiloso) a 5 (agresivo), -Pn evita el ping durante el escaneo, -O detecta el sistema operativo, -sV enseña información del banner y --script vuln, identifica las CVE más conocidas.

Figura 3.1 Escaneo Nmap Servidor Web parte 1



Escaneo Nmap Servidor Web parte 1. Elaborado por: Gabriel Pinto y Andrés Pérez.

Como resultado de estas pruebas, se detectaron varios puertos abiertos como el 80, 777 y el 8081 que trabajan con el protocolo TCP, información del banner como Apache httpd 2.4.6 con sistema operativo CentOS y un servicio de Apache TomCat/Coyote JSP engine 1.1; además la vulnerabilidad Slowloris DOS Attack con identificación de CVE-2007-6750.

Figura 3.2 Escaneo Nmap Servidor Web parte 2

Escaneo Nmap Servidor Web parte 2. Elaborado por: Gabriel Pinto y Andrés Pérez.

Las figuras 5 y 6, evidencian el escaneo del servidor de correo, en el que se detectaron los puertos abiertos 80, 143, 443, 993 con el protocolo TCP así como una vulnerabilidad en los puertos 143 y 993 CVE-2014-3566.

Figura 3.3. Escaneo Nmap Servidor de Correo parte 1

Escaneo Nmap Servidor de Correo parte 1. Elaborado por: Gabriel Pinto y Andrés Pérez.

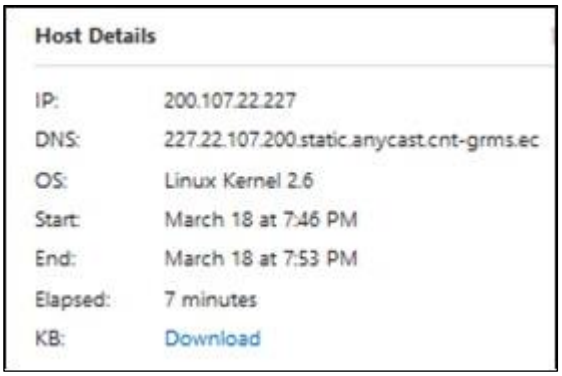
Figura 3.4 Escaneo Nmap Servidor de Correo parte 2

Escaneo Nmap Servidor de Correo parte 2. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.1.3 Análisis de Vulnerabilidades.

La herramienta Nessus se usó para analizar el servidor Web y el servidor de correo, dando como resultados información sobre la dirección del DNS: 227.22.107.200.static.anycast.cnt-grms.ec, IP (200.107.22.227), la versión el sistema operativo usado: Linux Kernel 2.6, además de la fecha de escaneo y el tiempo del proceso.

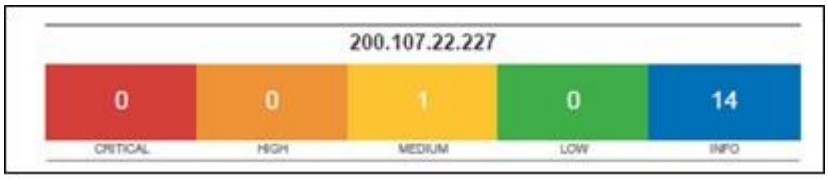
Figura 3.5 Escaneo Nessus Servidor Web.



Escaneo Nessus Servidor Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

Usando la herramienta Nessus se puede apreciar en base a colores, la criticidad de las vulnerabilidades detectadas y que son CVSS 6.8 con el nombre de Apache Tomcat Default Files, y 14 plugin de información con criticidad nula, ver anexo 15.

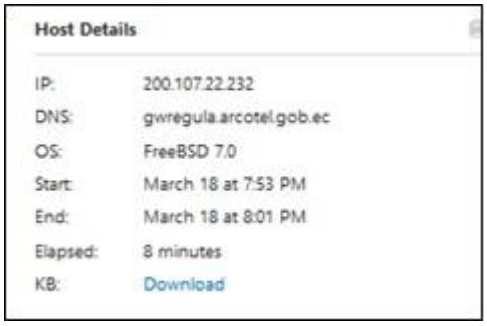
Figura 3.6 Clasificación de Vulnerabilidades por Nessus del Servidor Web.



Clasificación de Vulnerabilidades por Nessus del Servidor Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

El DNS del servidor de correo es gwregula.arcotel.gob.ec, el cual trabaja con un sistema operativo FreeBSD 7.0 según lo reportado por Nessus, ver anexo 16.

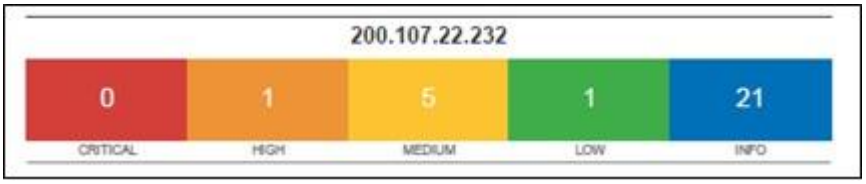
Figura 3.7 Escaneo Nessus Servidor de Correo



Escaneo Nessus Servidor de Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

El servidor de correo posee la url: mail.arcotel.gob.ec; así mismo la herramienta Nessus clasifica vulnerabilidades en críticas, altas, medias, bajas y brinda información de los plugins según la criticidad del caso, tal como se muestra en siguiente figura.

Figura 3.8 Clasificación de Vulnerabilidades por Nessus del Servidor de Correo.



Clasificación de Vulnerabilidades por Nessus del Servidor de Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

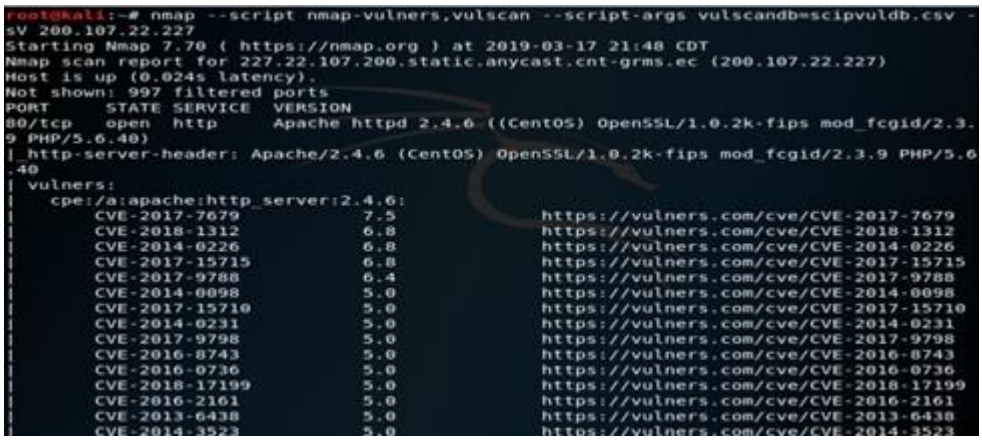
Se analizaron los servidores de aplicaciones web y de mail desde la red privada con las siguientes direcciones IP: 192.168.129.9 y 192.168.129.20. Se detectando un alto número de vulnerabilidades mismas que se clasifican según su criticidad en la siguiente figura:

Figura 3.9 Clasificación de Vulnerabilidades Internas del Servidor Web y Correo.

Clasificación de Vulnerabilidades Internas del Servidor Web y Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

A continuación, se reportan las vulnerabilidades detectadas con Nmap usando los scripts: nmap-vulners. vulscan y vulscandb=vulscandb scipvuldb.cvs, el servidor Web(200.107.22.227) reporta con códigos CVE (ver figura 12) y el servidor de Correo(200.107.22.232) informa mediante números de identificación (ver figura 13).

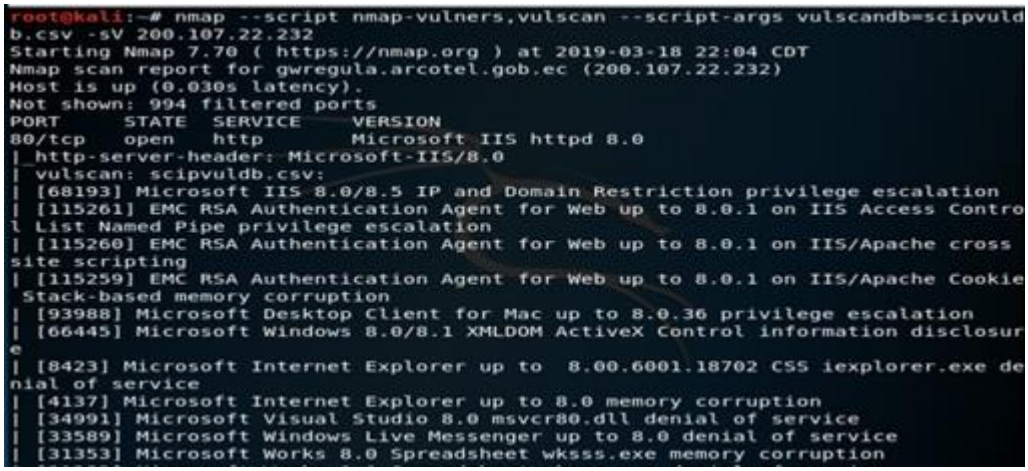
Figura 3.10 Análisis de vulnerabilidades Nmap Servidor Web.



```
root@kali:~# nmap --script nmap-vulners,vulscan --script-args vulscandb=scipvuldb.csv -
sV 200.107.22.227
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 21:48 CDT
Nmap scan report for 227.22.107.200.static.anycast.cnt-grms.ec (200.107.22.227)
Host is up (0.024s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.
9 PHP/5.6.40)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6
.40
| vulners:
|   cpe:/a:apache:http_server:2.4.6:
|       CVE-2017-7679           7.5       https://vulners.com/cve/CVE-2017-7679
|       CVE-2018-1312           6.8       https://vulners.com/cve/CVE-2018-1312
|       CVE-2014-0226           6.8       https://vulners.com/cve/CVE-2014-0226
|       CVE-2017-15715          6.8       https://vulners.com/cve/CVE-2017-15715
|       CVE-2017-9788           6.4       https://vulners.com/cve/CVE-2017-9788
|       CVE-2014-0098           5.0       https://vulners.com/cve/CVE-2014-0098
|       CVE-2017-15710          5.0       https://vulners.com/cve/CVE-2017-15710
|       CVE-2014-0231           5.0       https://vulners.com/cve/CVE-2014-0231
|       CVE-2017-9798           5.0       https://vulners.com/cve/CVE-2017-9798
|       CVE-2016-8743           5.0       https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-0736           5.0       https://vulners.com/cve/CVE-2016-0736
|       CVE-2018-17199          5.0       https://vulners.com/cve/CVE-2018-17199
|       CVE-2016-2161           5.0       https://vulners.com/cve/CVE-2016-2161
|       CVE-2013-6438           5.0       https://vulners.com/cve/CVE-2013-6438
|       CVE-2014-3523           5.0       https://vulners.com/cve/CVE-2014-3523
```

Análisis de vulnerabilidades Nmap Servidor Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

Figura 3.11 Análisis de Vulnerabilidades Nmap Servidor de Correo

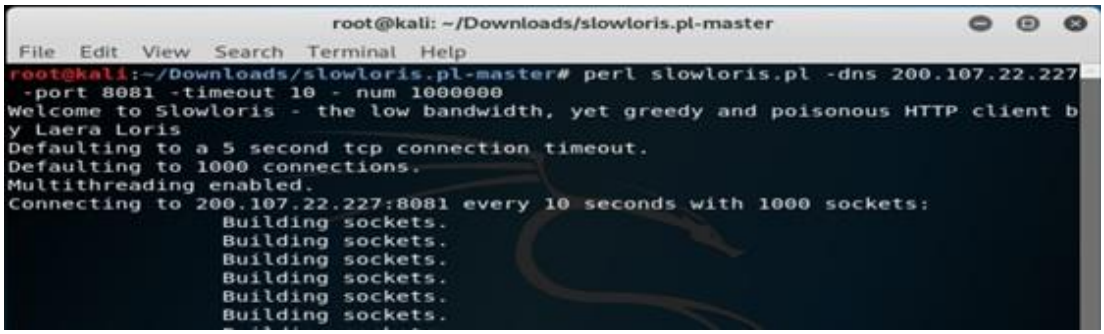


Análisis de vulnerabilidades Nmap Servidor de Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.1.4 Exploits

Para las pruebas de exploits, se procedió a realizar un ataque DoS saturando el servicio Web a través de peticiones "request" HTTP y HTTPS, mediante el envío de varias cabeceras para de esta manera forzar a mantener abiertas las conexiones hasta que alcance el máximo número de peticiones que pueda atender el servidor y denegar el servicio con ayuda del comando Slowloris. El script usado envió 1000000 paquetes cada 10 segundos por el puerto 8081 a la IP 200.107.22.227

Figura 3.12 Ejecución del comando Slowloris



Ejecución del comando Slowloris. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.1.5 Reporte

La tabla 6 muestra una lista general de las IP´s de Dominios y Subdominios expuestas a internet por parte de ARCOTEL, se comprueba que todas las aplicaciones web están

trabajando con el servicio de red TCP orientado en crear conexiones seguras y confiables verificando que todas usan el servicio http o https.

Tabla 3.1 Escaneo externo general con Nmap a los Aplicativos Web

Ip Pública	Protocolo	Puertos/Open	Servicios
200.107.X.X	Tcp	4XX	https
	Tcp	1XXX	h323q931
200.107.X.X (WEB)	Tcp	8X	http
	Tcp	7XXX	SSL/cbt
	Tcp	8XXX	http
200.107.X.X	Tcp	8X	http
200.107.X.X	Tcp	8X	http
200.107.X.X (CORREO)	Tcp	8X	http
	Tcp	1XX	Imap
	Tcp	4XX	https
	Tcp	9XX	Imaps
	Tcp	2XXX	ms-v-worlds
200.107.X.X	Tcp	8X	http
	Tcp	4XX	https
200.107.X.X	Tcp	8XX	http-proxy

Escaneo externo general con Nmap a los Aplicativos Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

Se presenta un análisis general de las vulnerabilidades (CVE) externas encontradas con Nessus con su respectiva criticidad (ver Tabla 1) y soluciones de las IP´s expuestas al contacto con internet.

Tabla 3.2 Escaneo externo con Nessus a los Aplicativos Web

IP	Vulnerabilidades	Severidad	Solución
200.107.X.X	SSL Certificate Cannot Be Trusted	Media	Parchar el propio certificado para el servicio
200.107.X.X	Apache Tomcat Default Files	Media	Eliminar la página de índice
	Apache Tomcat Detection	Info	----------
	HTTP Server Type and Version	Info	----------
200.107.X.X	Common Platform Enumeration (CPE)	Info	----------
200.107.X.X	Unix Operating System Unsupported Version Detection	Critica	Actualizar la versión del S.O. Unix
	Apache Banner Linux Distribution Disclosure	Info	----------
200.107.X.X	SSL Version 2 and 3	Alta	Desactivar SSL 2.0 y SSL 3.0
	SSL Certificate Cannot Be Trusted	Media	Parchar el propio certificado para el servicio

200.107.X.X	SSH Weak Algorithms Supported	Media	Eliminar los cifrados débiles
200.107.X.X	Host Fully Qualified Domain Name	Info	----------
200.107.X.X	Common Platform Enumeration (CPE)	Info	----------

Escaneo externo con Nessus a los Aplicativos Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

Internamente en la red de la empresa, se verifica los servicios levantados en los Servidores web y correo en la siguiente tabla:

Tabla 3.3 Escaneo interno con Nmap al Servidor Aplicaciones Web y Correo.

Ip Pública	Protocolo	Puertos	Servicios	Descripción
200.107.X.X (WEB)	Tcp	80	http	Servicio Web
	Tcp	135	Msrpc	Acceso y gestión de forma remota a Windows
	Tcp	139	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	Tcp	443	https	Servicio Web Seguro
	Tcp	445	microsoft-ds	Compartición de ficheros
	Tcp	3389	ms-wbt-server	Conexión remota de escritorio
	Tcp	49152:54	Unknown	Acceso a Xsan Filesystem
200.107.X.X (CORREO)	Tcp	25	Smtp	Transferencia Simple de Correo
	Tcp	80	http	Servicio Web
	Tcp	135	Msrpc	Acceso y gestión de forma remota a Windows
	Tcp	139	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	Tcp	143	Imap	Acceso a los mensajes almacenados
	Tcp	443	https	Servicio Web Seguro
	Tcp	445	Microsoft-ds	Compartición de ficheros
	Tcp	808	ccproxy-http	Servicios de suscripción entre clusters
	Tcp	993	Imaps	Acceso seguro a los mensajes almacenados
	Tcp	2525	ms-v-worlds	Alternativa de SMTP
	Tcp	3389	ms-wbt-server	Conexión remota de escritorio
	Tcp	67001:7	X11:1-7	Transferencia de datos entre el Cliente y Servidor

Escaneo interno con Nmap al Servidor Aplicaciones Web y Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

En la siguiente tabla 9, se presenta dos vulnerabilidades internas encontradas de la subred de Servidores.

Tabla 3.4 Escaneo interno con Nessus a la red de Servidores

IP	Descripción	Severidad	Solución
192.168.X.X/24	El servicio remoto con conexiones SSL 2.0 y / o SSL 3.0.	Alta	Deshabilitar SSL 2.0 y 3.0.
	El servidor NTP remoto en modo 6.	Media	Restringir las consultas del modo NTP 6.

Escaneo interno con Nessus a la red de Servidores. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.2 FASE II: Análisis de Riesgos

Cada organización tiene vulnerabilidades y riesgos diferentes, en muchos casos estos riesgos no se pueden eliminar por completo, pero en la mayoría de los casos es posible darle un tratamiento a través de controles.

3.2.1 Calificación de Probabilidad e Impacto

Para determinar los pesos de la probabilidad de ocurrencia de un suceso se usó la siguiente tabla:

Tabla 3.5 Clasificación de la Probabilidad de Riesgos.

Probabilidad		
P	**Tipo**	**Descripción**
4-5	Esperado	En la ausencia de cualquier control donde pueda ocurrir el aprovechamiento de vulnerabilidades y convertirla en amenaza.
3-4	Muy Probable	En la ausencia de cualquier control, es muy probable que ocurran el aprovechamiento de vulnerabilidades y convertirla en amenaza.
2-3	Probable	En la ausencia de cualquier control, es probable que ocurran el aprovechamiento de vulnerabilidades y convertirla en amenaza.
1-2	No Probable	En la ausencia de cualquier control, es baja la probabilidad que ocurra el aprovechamiento de vulnerabilidades y convertirla en amenaza.
0-1	Leve	En la ausencia de cualquier control, no se espera que pueda ocurrir el aprovechamiento de vulnerabilidades y convertirla en amenaza.

Clasificación de la Probabilidad de Riesgos. Elaborado por: Gabriel Pinto y Andrés Pérez.

Para evaluar las métricas referentes a los impactos que podrían provocar las amenazas en la red, se utilizó la tabla 11:

Tabla 3.6 Calificación del Impacto del Riesgo.

IMPACTO		
I	**Tipo**	**Descripción**
5	Critico	Impacto potencialmente irreparable
4	Alto	Recuperable de largo plazo
3	Significativo	Recuperable a corto plazo
2	Moderado	Temporal
0-1	Bajo	Impacto limitado

Calificación del Impacto del Riesgo. Elaborado por: Gabriel Pinto y Andrés Pérez.

Para realizar un mapeo de riesgos actuales de la red, se pidió realizar una valoración del Impacto y Probabilidad a tres funcionarios del Departamento de Tecnologías de la Información.

Tabla 3.7 Voto Impacto/Probabilidad de Funcionarios ARCOTEL

Amenaza	Tipificación de Riesgo	Voto / Cargo	Calificación Funcionario Nro. 1	Calificación Funcionario Nro. 2	Calificación Funcionario Nro. 3	Promedio
Lógicas Servidor Web	R1	IMPACTO	4,6	4,7	4,7	4,7
		PROBABILIDAD	1,5	2,1	2,0	1,9
	R2	IMPACTO	4,8	4,6	4,8	4,7
		PROBABILIDAD	2,0	2,2	1,6	1,9
	R3	IMPACTO	4,0	4,0	4,0	4,0
		PROBABILIDAD	1,4	1,0	1,0	1,1
	R4	IMPACTO	3,0	3,1	4,1	3,4
		PROBABILIDAD	4,6	4,1	4,1	4,3
	R5	IMPACTO	4,3	4,6	4,8	4,6
		PROBABILIDAD	2,0	2,0	2,0	2,0
	R6	IMPACTO	2,5	2,8	2,3	2,5
		PROBABILIDAD	4,7	4,2	4,5	4,5
	R7	IMPACTO	3,3	4,0	4,0	3,8
		PROBABILIDAD	2,0	2,0	2,0	2,0
	R8	IMPACTO	2,5	2,3	2,8	2,5
		PROBABILIDAD	4,5	4,3	4,5	4,4
	R9	IMPACTO	3,5	4,0	4,0	3,8
		PROBABILIDAD	2,0	2,0	2,0	2,0
	R10	IMPACTO	4,0	3,5	4,0	3,8

		PROBABILIDAD	2,3	1,5	2,1	2,0
Lógicas Servidor de Correo	R11	IMPACTO	2,3	2,5	3,0	2,6
		PROBABILIDAD	2,5	2,5	2,5	2,5
	R12	IMPACTO	3,0	3,0	3,0	3,0
		PROBABILIDAD	1,7	1,5	1,0	1,4
	R13	IMPACTO	2,5	3,1	2,5	2,7
		PROBABILIDAD	4,3	4,2	4,3	4,3
	R14	IMPACTO	2,5	2,9	2,0	2,5
		PROBABILIDAD	4,5	4,6	4,3	4,5
	R15	IMPACTO	3,2	3,2	3,2	3,2
		PROBABILIDAD	4,5	4,2	4,8	4,5
	R16	IMPACTO	3,3	3,4	3,1	3,3
		PROBABILIDAD	4,0	4,0	4,0	4,0
	R17	IMPACTO	3,1	3,2	3,5	3,3
		PROBABILIDAD	4,5	3,5	4,0	4,0
	R18	IMPACTO	3,7	3,1	3,3	3,4
		PROBABILIDAD	4,2	4,2	4,4	4,3
	R19	IMPACTO	3,3	3,7	3,3	3,4
		PROBABILIDAD	4,3	4,3	4,3	4,3
Usuarios Externos	R20	IMPACTO	4,8	4,2	4,5	4,5
		PROBABILIDAD	4,0	4,0	4,0	4,0
Desastres Naturales	R21	IMPACTO	4,6	4,0	4,8	4,5
		PROBABILIDAD	3,5	3,8	3,3	3,5
Wifi	R22	IMPACTO	3,3	3,8	3,5	3,5
		PROBABILIDAD	4,0	3,9	4,0	4,0

Voto Impacto/Probabilidad de Funcionarios ARCOTEL. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.2.2 Matriz y Mapeo de Riesgos.

Se realizó un Mapeo de riesgos general que se encuentra en la red de ARCOTEL determinando las amenazas de los servidores de WEB Y CORREO, usuarios externos como exempleados, el uso de la red wifi, posibles desastres naturales dándoles una criticidad, probabilidad e impacto y principios de la seguridad (Confidencialidad, Integridad y Disponibilidad).

Tabla 3.8 Matriz de Riesgos con Firewall Palo Alto

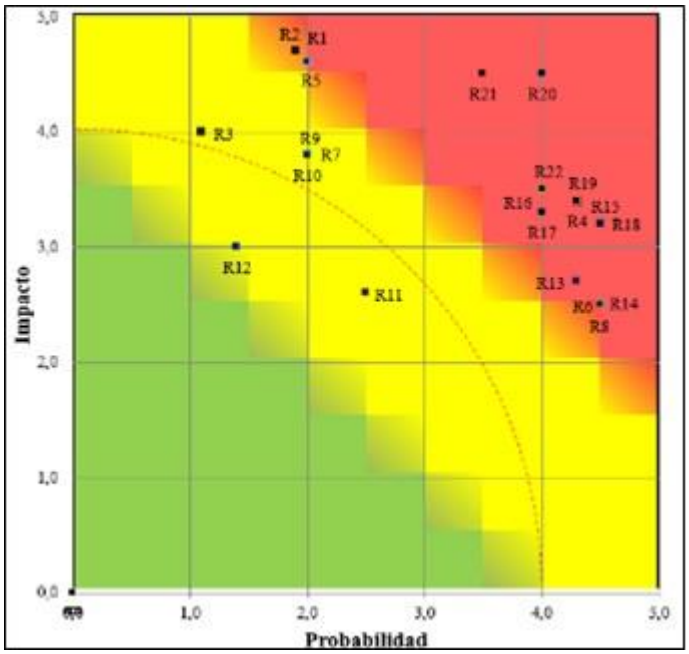
Amenaza	Tipificación de Riesgo	Riesgo	Incidente/ Problema identificado	Criticidad	Probabilidad	Impacto	Principio de Seguridad Infectado
Lógicas Servidor Web	R1	CVE-2017-7679	Apache httpd 2.4.x - 2.4.26, mod_mime.	Alto	1,9	4,7	C-I-A
	R2	CVE-2018-1312	Apache httpd before 2.4.29, HTTP Digest authentication	Alto	1,9	4,7	C-I-A
	R3	CVE-2017-15715	Apache httpd 2.4.0 to 2.4.29, <FilesMatch> match with $	Alto	1,1	4	C-I-A
	R4	CVE-2014-0226	Apache HTTP before 2.4.10, DoS (buffer overflow).	Medio	4,3	3,4	A
	R5	CVE-2017-9788	Apache 2.4.x before 2.4.27, key=value assignments	Alto	2	4,6	C-A
	R6	CVE-2014-0098	Apache HTTP before 2.4.8, (segmentation fault and daemon crash)	Medio	4,5	2,5	A
	R7	CVE-2017-15710	Apache httpd 2.4.0 to 2.4.29, mod_authnz_ldap, DoS	Alto	2	3,8	A
	R8	CVE-2014-0231	Apache HTTP before 2.4.10, does not have a timeout mechanism.	Medio	4,5	2,5	A
	R9	CVE-2016-8743	HTTP before 2.4.25, whitespace accepted from requests and sent in response lines.	Alto	2	3,8	I
	R10	CVE-2018-17199	Apache HTTP 2.4, mod_session checks the session	Alto	2	3,8	I
Servidor de Correo	R11	CVE-2014-4078	Microsoft (IIS) 8.0 and 8.5 does not properly process	Medio	2,5	2,6	C-I-A

			wildcard allow and deny rules				
	R12	CVE-2018-1233	EMC RSA Authentication Agent for Web hasta 8.0.1	Medio	1,4	3	C-I
	R13	CVE-2013-7331	Windows 8.1 and earlier, allows to determine the existence of pathnames	Medio	4,3	2,7	C-A
	R14	CVE-2007-0842	Microsoft Visual Studio 8.0, msvcr80.dll time.	Medio	4,5	2,5	A
	R15	CVE-2002-2380	Network Firmware 5.5.11 weak encryption	Medio	4,5	3,2	C-I
	R16	CVE-2012-0811	Postfix up to 2.3.0, backup.php.	Medio	4	3,3	C-I-A
	R17	CVE-2014-2655	Postfix Admin 2.3.6, functions.inc.php show_alias.	Medio	4	3,3	C-I-A
	R18	CVE-2011-1720	Postfix prior 2.1.0 memory corruption	Medio	4,3	3,4	C-I-A
	R19	CVE-2011-0411	Postfix up to 2.7.2, weak encryption	Medio	4,3	3,4	C-I-A
Usuarios Externos	R20	Exempleados	Robo de información	Alto	4	4,5	C-I-A
Desastres Naturales	R21	Daños de Equipos	Back-up de equipos	Alto	3,5	4,5	C-I-A
Wifi	R22	Red Hackeada	Misma contraseña por periodos largos de tiempo	Alto	4	3,5	C-I-A

Matriz de Riesgo con Firewall Palo Alto. Elaborado por: Gabriel Pinto y Andrés Pérez.

Con el fin de visualizar de mejor forma la relación entre la probabilidad e impacto de las vulnerabilidades, se utiliza el mapa de riesgos para la prevención de emergencias o eventos adversos que puedan suceder a un futuro.

Figura 3.13 Mapeo de Riesgos con Firewall Palo Alto



Mapeo de Riesgo con Firewall Palo Alto. Elaborado por: Gabriel Pinto y Andrés Pérez.

3.3 FASE III: Evaluación Comercial, Técnica y Selección de Solución UTM

3.3.1 Cuadrante mágico de Gartner

Este cuadrante se define como punto de partida para identificar las posibles soluciones UTM que lideran el mercado. En la figura 3.14 se destacan Fortinet por su capacidad de ejecución y Sophos por su visión de mercado.

Figura 3.14 Cuadrante Mágico de Gartner en Soluciones UTM 2018

Cuadrante Mágico de Gartner en Soluciones UTM 2018. Elaborado por: Gartner,Inc

3.3.2 Ranking de Soluciones UTM

Según el nivel de aceptación evaluado por la IT Central Station mediante un ranking sobre las distintas plataformas propietarias o gratuitas, PFsense se destaca como la primera solución alternativa de código abierto dentro de 49 Firewalls evaluados como se aprecia en el anexo 17.

3.3.3 Evaluación Técnica

La comparación funcional garantiza que PFsense cumpla con todas las funcionalidades que brinda tanto un Appliance UTM de gama alta como el PaloAlto implementado en la ARCOTEL y se especifican en la Tabla 3.9

Tabla 3.9 Relación de funcionalidades de Soluciones UTM

Funcionalidades	**Fortinet FortiGate**	**UTM Sophos**	**Palo Alto**	**PFsense**

Interfaz gráfica basada en web	✓	✓	✓	✓
Ejecutable en entornos virtualizados	✓	✓	✓	✓
Backup y restauración de configuración	✓	✓	✓	✓
Panel configurable	✓	✓	✓	✓
Compatibilidad IPv4 e Ipv6	✓	✓	✓	✓
Control de tráfico o traffic shaping	✓	✓	✓	✓
Redundancia y alta disponibilidad	✓	✓	✓	✓
NAT	✓	✓	✓	✓
Soporte Multi-WAN	✓	✓	✓	✓
Herramientas de diagnóstico de red	✓	✓	✓	✓
Equilibrio de carga de entrada del servidor	✓	✓	✓	✓
Ipsec-OpenVPN-L2TP-PPPoe	✓	✓	✓	✓
Gráficos de tráfico en tiempo real	✓	✓	✓	✓
DNS dinámico	✓	✓	✓	✓
Portal Cautivo	✓	✓	✓	✓
VLAN	✓	✓	✓	✓
LACP o LAGG	✓	✓	✓	✓
GRE	✓	✓	✓	✓
IPS	✓	✓	✓	✓
IDS	✓	✓	✓	✓
Antivirus	✓	✓	✓	✓
Filtrado de contenidos	✓	✓	✓	✓
Actualización de seguridad	✓	✓	✓	✓
Sin costo de licencia	✗	✗	✗	✓
Facilidad de acceso a información	✓	✓	✓	✓

Comparación de las soluciones UTM 2019. Elaborado por: Andrés Pérez y Gabriel Pinto.

PFsense cumple con los requerimientos más importantes de la ARCOTEL, catalogándose como una solución muy competitiva para la sustitución de PaloAlto Debido a que es una plataforma libre de licenciamiento, no posee un datasheet específico para la implementación en entornos virtualizados; por tanto, fue necesario realizar una comparativa de sus especificaciones técnicas y del rendimiento del sistema frente a otras soluciones comerciales; para con ello realizar el dimensionamiento de la plataforma fundamentada en los parámetros técnicos de los UTM comerciales que se especifican en la Tabla 3.10

Tabla 3.10 Especificaciones Técnicas y de Rendimiento de Appliance de Fortinet, Sophos y Palo Alto

Especificaciones técnicas			
	Fortinet FG-VM00	Sophos CRiV-1C	PaloAlto VM-50
Plataforma Virtual	VMware ESXi 5.5	VMware ESXi 5.5	VMware ESXi 5.5
Soporte de vCPU (min/máx.)	1 / 1	1 / 1	1 / 2
Memoria soportada (min/máx.)	1 Gb / 4Gb	1 Gb / 4 Gb	4.5 Gb / ND
Almacenamiento (min/máx.)	32 Gb / 2 Tb	ND / ND	32 Gb / 2 Tb
Rendimiento del sistema			
	Fortinet FG-VM00	Sophos CRiV-1C	PaloAlto VM-50
Firewall Throughput	2 Gbps	1500 Mbps	100 Mbps
Threat Prevention Throughput	1 Gbps	450 Mbps	50 Mbps
Sesiones concurrentes	1000000	230000	50000
Nuevas sesiones / segundo	85000	25000	1000

Especificaciones Técnicas y de Rendimiento de Appliance de Fortinet, Sophos y Palo Alto. Elaborado por: Andrés Pérez y Gabriel Pinto.

3.3.4 Throughput y Sesiones Concurrentes

Durante un periodo de evaluación comprendido entre noviembre 2018 y febrero de 2019. En el dispositivo PaloAlto-3020, se usó la herramienta Observium para realizar el monitoreo al enlace que conecta el switch central con la interfaz del Firewall, registrándose una tasa pico de transferencia de paquetes en la red LAN de aproximadamente 56.30 Mbps y se determinó un aproximado de 10930 sesiones concurrentes pico como se observa en el anexo 21 y 22.

3.3.5 Consideraciones Técnicas para la implementación del Appliance PFsense

El dimensionamiento de la plataforma se fundamenta en la comparación de sus recomendaciones tanto a nivel físico establecidas por Netgate, empresa que en sus soluciones de seguridad implementa el sistema PFsense, como a nivel virtual definida por PaloAlto, plataforma que más se ajusta con los parámetros de rendimiento del sistema evaluados a la red ARCOTEL como son Throughput y sesiones concurrentes obtenido previamente en los puntos anteriores y se describe en la Tabla 3.11

Tabla 3.11 Relación entorno físico y virtual

RENDIMIENTO DEL SISTEMA				
	Recomendación		Experimental	
Firewall Throughput	100 Mbps		56.30 Mbps	
Sesiones concurrentes	50000		10930	
ESPECIFICACIÓN TÉCNICA				
Entorno	Físico		Virtual	
	Recomendación (Netgate-PFsense)	Particular (UCS)	Recomendación (PaloAlto)	Estimación
Procesamiento	600 MHz o más veloz	2.53 GHz	2 vCPU	4 vCPU
RAM	512 MB o más	48 GB	4.5 GB	12 GB
Almacenamiento	4 GB o más	Storage	32 GB / 2 TB	200 GB

Relación entorno físico y virtual. Elaborado por: Andrés Pérez y Gabriel Pinto.

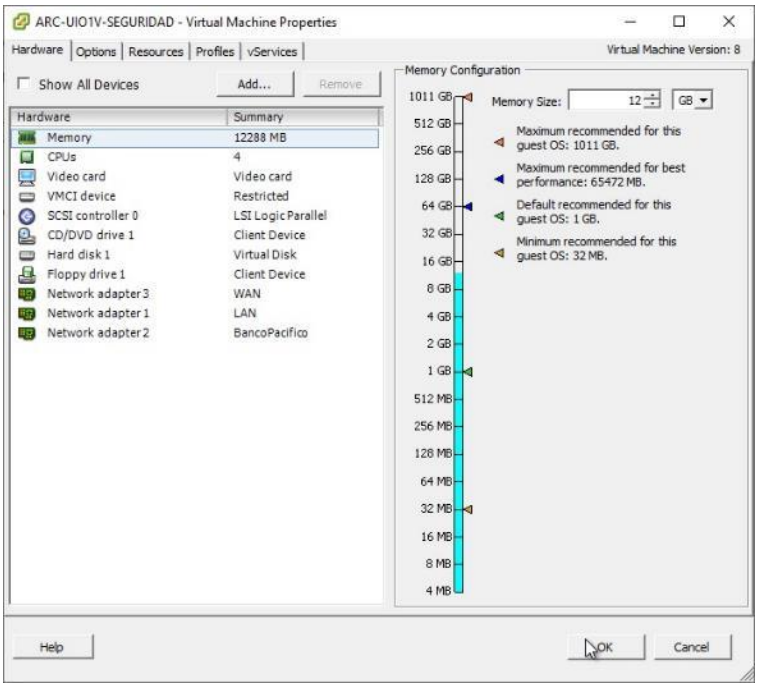
CAPÍTULO 4

IMPLEMENTACIÓN DE PFSENSE

4.1 Instalación de PFsense

Para la instalación y configuración de PFsense se consideraron algunos componentes técnicos como la memoria RAM estimada, el procesador, así como las interfaces de conexión en VMware, tal como se aprecian en la figura 4.1

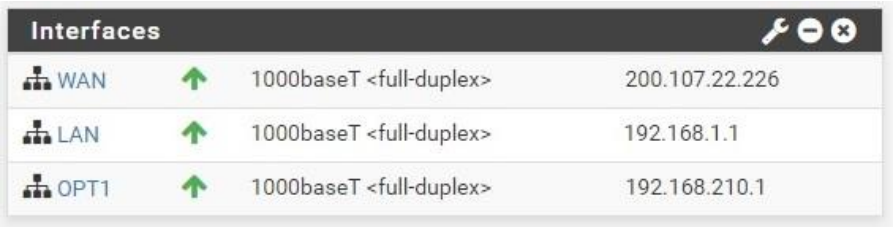
Figura 4.1 Componentes técnicos del Appliance PFsense.



Componentes técnicos del PFsense. Elaborado por: Andrés Pérez y Gabriel Pinto.

La instalación del sistema PFsense, requiere de la configuración de las IP's para las 3 interfaces: la primera para el enlace WAN destinado al Internet, la segunda para la red LAN designada para la red ARCOTEL y la tercera OPT1 dedicada a la conexión con el Banco del Pacifico.

Figura 4.2 Interfaces funcionales en PFsense



Componentes técnicos del PFsense. Elaborado por: Andrés Pérez y Gabriel Pinto.

Interfaces funcionales en PFsense. Elaborado por: Andrés Pérez y Gabriel Pinto.

La plataforma posee un tablero de control para su gestión mediante un cliente Web de la red institucional que brinda información importante, tales como: la identificación del dispositivo Netgate, la BIOS, la versión, el tipo de CPU como se aprecia en la figura 4.3

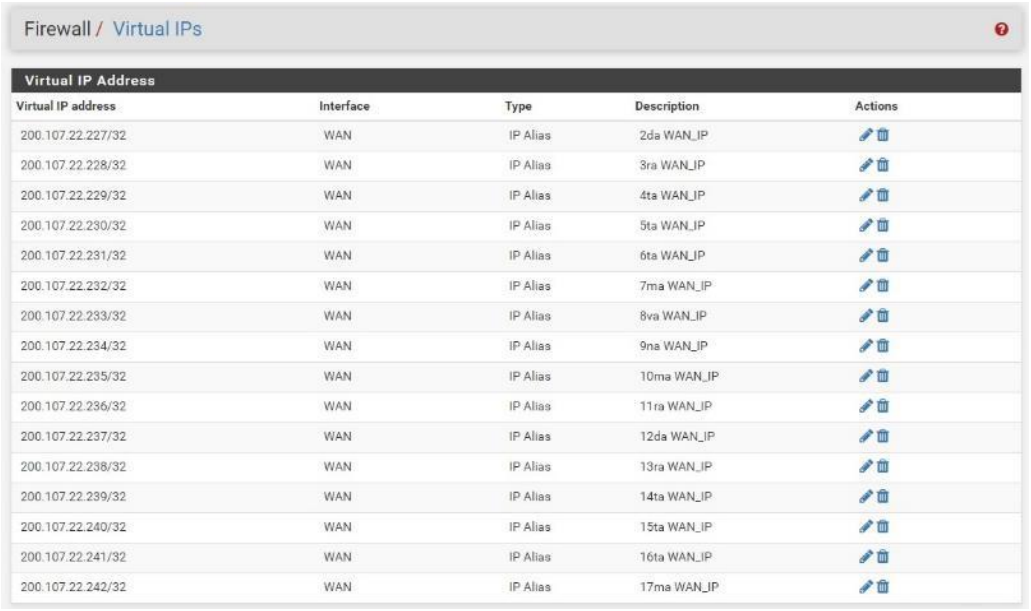
Figura 4.3 Interfaz GUI del Appliance PFsense

Interfaz GUI del Appliance PFsense. Elaborado por: Andrés Pérez y Gabriel Pinto.

4.1.1 Configuración del Firewall / Virtual IP´s

A continuación, se describen las IP virtuales creadas con el fin de traducir múltiples IP públicas en IP privadas sobre un único enlace WAN:

Figura 4.4 IP's virtuales



Virtual IP Address

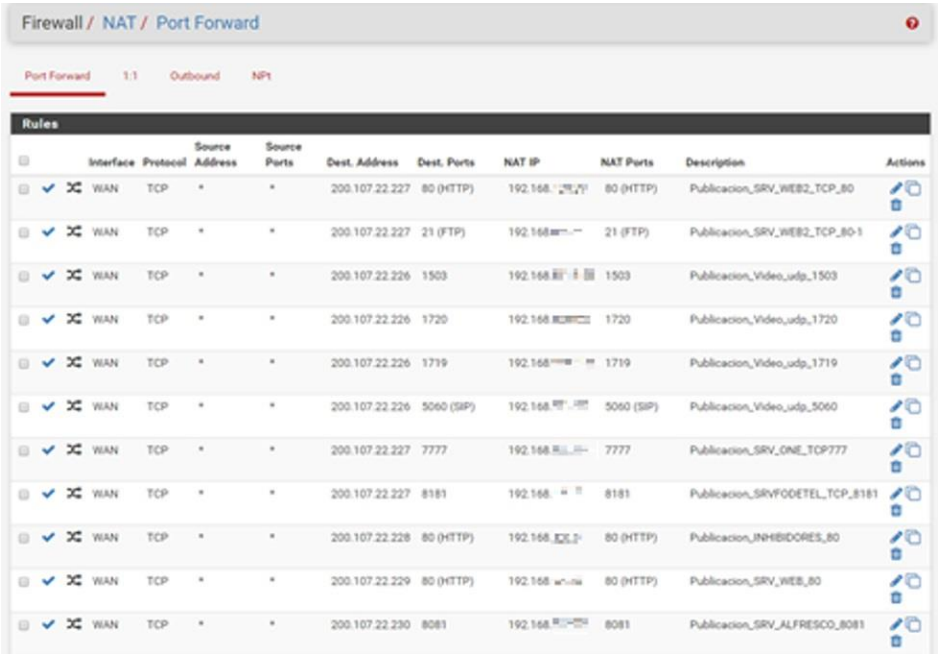
Virtual IP address	Interface	Type	Description	Actions
200.107.22.227/32	WAN	IP Alias	2da WAN_IP	
200.107.22.228/32	WAN	IP Alias	3ra WAN_IP	
200.107.22.229/32	WAN	IP Alias	4ta WAN_IP	
200.107.22.230/32	WAN	IP Alias	5ta WAN_IP	
200.107.22.231/32	WAN	IP Alias	6ta WAN_IP	
200.107.22.232/32	WAN	IP Alias	7ma WAN_IP	
200.107.22.233/32	WAN	IP Alias	8va WAN_IP	
200.107.22.234/32	WAN	IP Alias	9na WAN_IP	
200.107.22.235/32	WAN	IP Alias	10ma WAN_IP	
200.107.22.236/32	WAN	IP Alias	11ra WAN_IP	
200.107.22.237/32	WAN	IP Alias	12da WAN_IP	
200.107.22.238/32	WAN	IP Alias	13ra WAN_IP	
200.107.22.239/32	WAN	IP Alias	14ta WAN_IP	
200.107.22.240/32	WAN	IP Alias	15ta WAN_IP	
200.107.22.241/32	WAN	IP Alias	16ta WAN_IP	
200.107.22.242/32	WAN	IP Alias	17ma WAN_IP	

IP's virtuales. Elaborado por: Andrés Pérez y Gabriel Pinto.

4.1.2 Configuración del Firewall / Levantamiento de Servicios.

De acuerdo a los controles establecidos por la ARCOTEL, se definieron y configuraron un conjunto de reglas pre-routing que permiten la activación de los servicios como HTTP, FTP, SIP, entre otros usados en la red de ARCOTEL.

Figura 4.5 Publicación de Servicios.

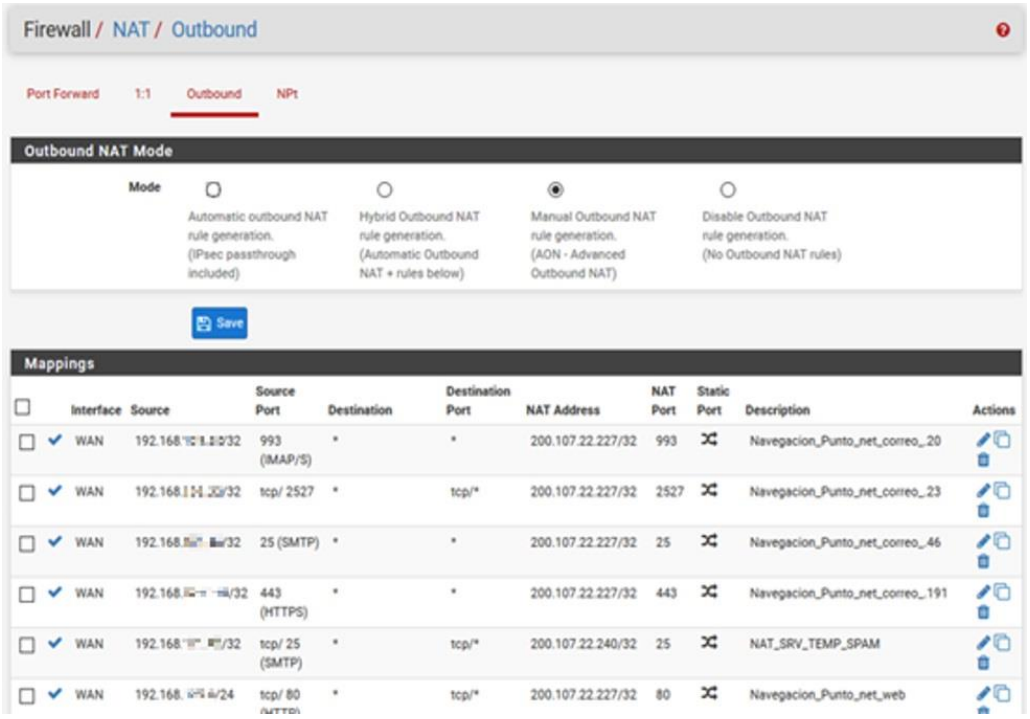


Publicación de Servicios. Elaborado por: Andrés Pérez y Gabriel Pinto.

4.1.3 Configuración del Firewall / Tráfico de Salida

Las reglas post-routing descritas a continuación permitieron direccionar la salida de los servicios hacia el Internet y las redes públicas.

Figura 4.6 Tráfico de Salida.

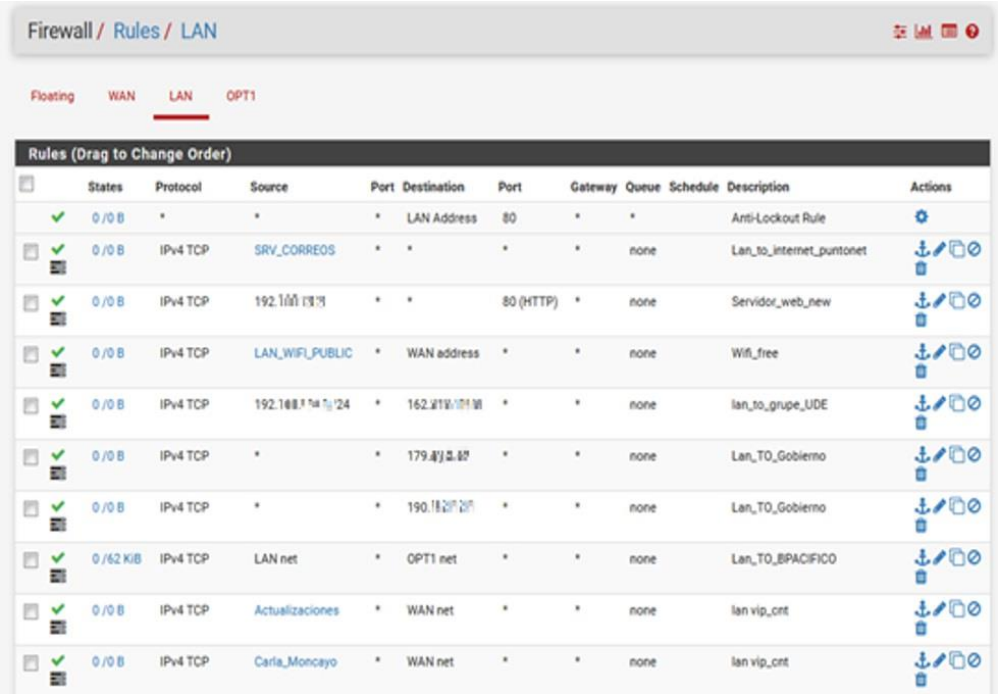


Tráfico de Salida. Elaborado por: Andrés Pérez y Gabriel Pinto.

4.1.4 Configuración del Firewall / Políticas de Seguridad

Las reglas dispuestas en la figura 4.7, definen el control de la ARCOTEL sobre el tráfico entrante y saliente de la red; por seguridad inicialmente se establece una primera regla antibloqueo para ingresar a la GUI del PFsense y posteriormente se configuran las reglas que definen los permisos de servicios como correo y web, y para las conexiones entre las interfaces OPT1 y LAN.

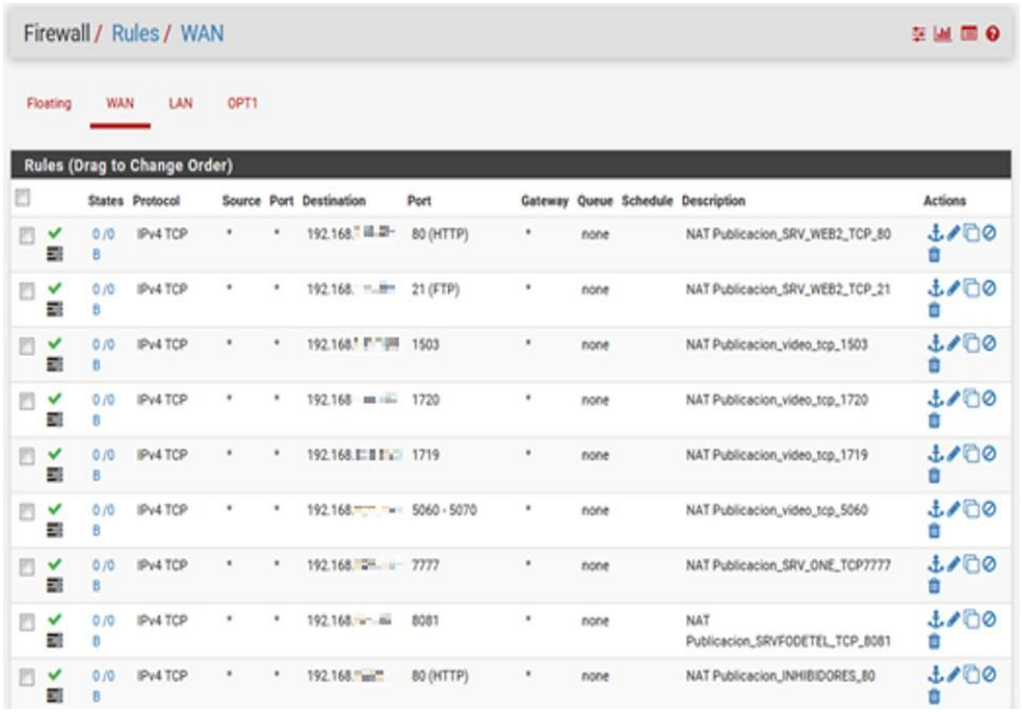
Figura 4.7 Políticas de Seguridad LAN



Políticas de seguridad LAN. Elaborado por: Andrés Pérez y Gabriel Pinto.

En la figura 4.8 se observan las políticas WAN que permiten el paso de las publicaciones de los servicios como HTTP, FTP, IMAP, SMTP, entre otros.

Figura 4.8 Políticas de Seguridad WAN



Políticas de seguridad WAN. Elaborado por: Andrés Pérez y Gabriel Pinto.

En la figura 4.9, se describe la regla que permite comunicar el tráfico desde las subredes del Banco del Pacifico a todas las subredes de la LAN.

Figura 4.9 Políticas de Seguridad OPT1

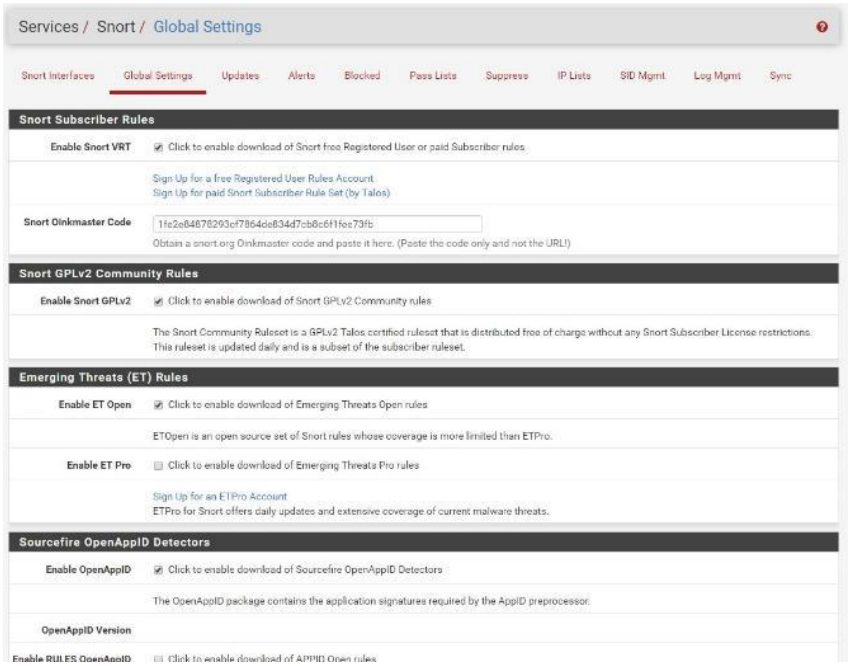
Políticas de seguridad OPT1. Elaborado por: Andrés Pérez y Gabriel Pinto.

4.1.5 Configuración del IPS/IDS

Se habilitaron las 4 reglas disponibles por la herramienta Snort para realizar la detección y prevención de amenazas: **Snort VRT** (Vulnerability Research Team) define un conjunto de reglas robusto y estable que permite un entorno empresarial seguro, **GPLv2** son reglas elaboradas por la comunidad Snort Integrators bajo la licencia GPL para la distribución de software libre; **ET** (Emerging Threats) cubren las últimas amenazas emergentes en el tráfico de red y por último la **OpenAppID** son

reglas que permiten el bloqueo de servicios, para el caso particular del proyecto se bloqueó servicios de redes sociales y contenido para adultos.

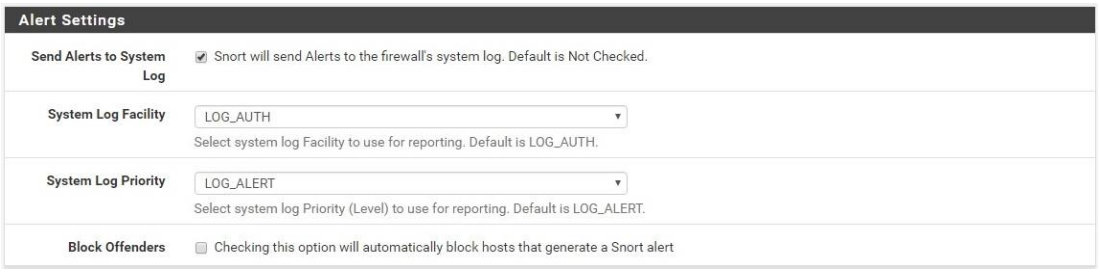
Figura 4.10 Habilitación de las reglas IPS/IDS



Habilitación de las reglas IPS/IDS. Elaborado por: Andrés Pérez y Gabriel Pinto.

Para el enlace WAN y OPT1 se deshabilitó la opción Block Offenders como se muestra en la figura 4.11; esto permite a los enlaces operar en modo IDS para realizar el sniffing de las amenazas.

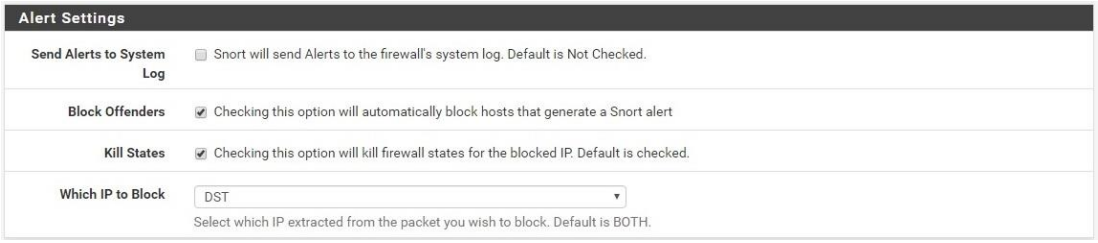
Figura 4.11 Configuración IDS



Configuración IDS. Elaborado por: Andrés Pérez y Gabriel Pinto.

A diferencia de los enlaces WAN y OPT1, en el enlace LAN se habilitó la opción Block Offenders, Kill States y se bloqueó el destino (DST), como se muestra en la figura 4.12; lo cual permite que actué el IPS para bloquear inmediatamente las intrusiones que se generan desde la red LAN.

Figura 4.12 Configuración IPS



Configuración IPS. Elaborado por: Andrés Pérez y Gabriel Pinto.

Finalmente se levantan los servicios IDS e IPS en las interfaces según corresponda la configuración establecida en cada enlace como se muestra en la figura 4.13

Figura 4.13 Interfaces IDS/IPS

Interfaces IDS/IPS. Elaborado por: Andrés Pérez y Gabriel Pinto.

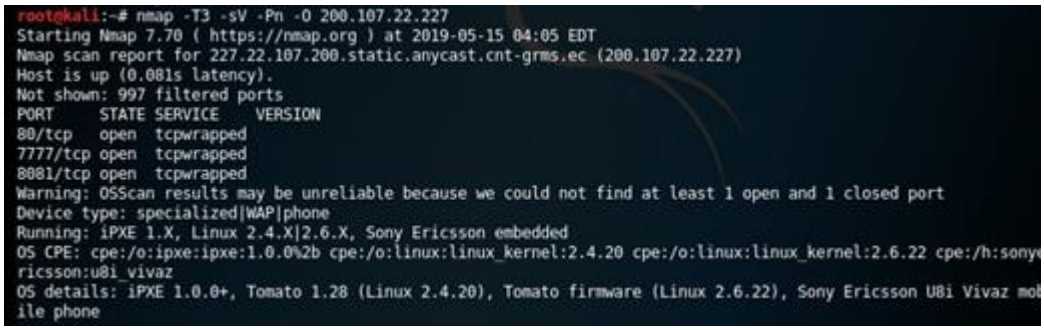
4.2 Pentesting en la red

La superficie de ataque es la suma de las vulnerabilidades presentes en la red y se puede definir mediante la detección de puertos abiertos y el uso de los aplicativos que se ejecutan en servidores que tienen contacto con internet, además se consideran también a los usuarios como exempleados que quisieran atentar contra la organización, por tal razón las pruebas de pentesting se realizan en dos fases que son: identificación de servicios y análisis de vulnerabilidades.

4.2.1 Identificación de servicios

Los puertos definen una lista de procesos TCP o UDP disponibles para aceptar datos, de tal manera es una referencia para establecer valores en el análisis de riesgo, se puede observar para el servidor Web los puertos 80, 7777, 8081.

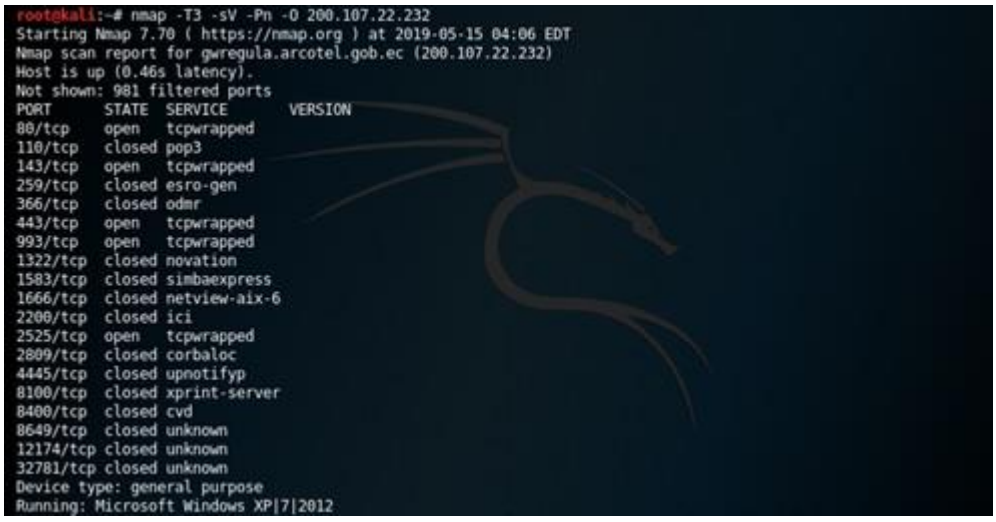
Figura 4.14 Escaneo de servicios con Nmap Servidor Web



Escaneo de servicios Nmap Servidor Web. Elaborado por: Gabriel Pinto y Andrés Pérez

El Servidor de correo usa el servicio IMAP y SMTP, con la característica de tcpwrapped, lo cual significa que se completó el enlace TCP, pero el host remoto cerró la conexión, lo cual comprueba que el UTM PFsense cumple con su cometido.

Figura 4.15 Escaneo de servicios Nmap Servidor de Correo



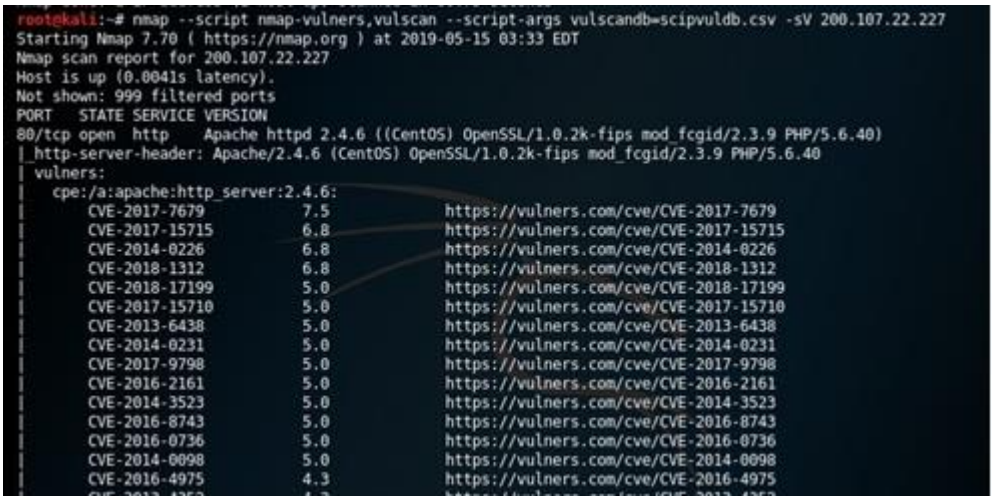
Escaneo de servicios Nmap Servidor de Correo. Elaborado por: Gabriel Pinto y Andrés Pérez

4.2.2 Análisis de vulnerabilidades

Para detectar los CVE´s se aplicaron scripts de nmap-vulners que consulta la base de datos de Vulners y de vulscan, el cual utiliza varias bases de datos preconfiguradas que están almacenadas localmente: scipvuldb.csv, sve.csv, osvdb.csv, securityfocus.csv, secutirytracker.csv, xforece.csv, exploitdb.csv, openvas.cvs. Estos scripts utilizan registros CVE, los scripts de NSE (Nmap Scripting Engine) identifica y produce información relevante acerca de CVE´s conocidos. Las debilidades

encontradas en el servidor web una vez implantado el sistema PFsense son las siguientes:

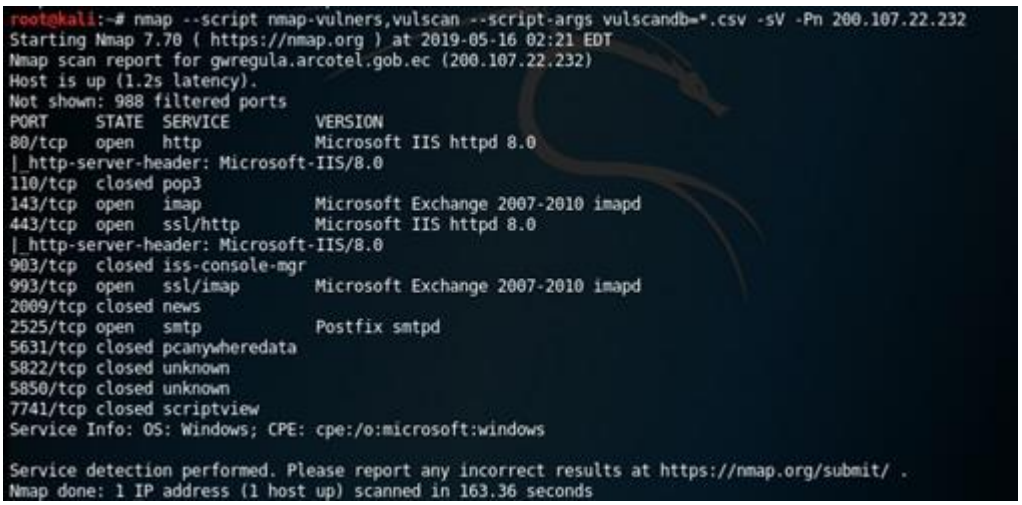
Figura 4.16 Análisis de vulnerabilidades Nmap Servidor Web



Análisis de vulnerabilidades Nmap Servidor Web. Elaborado por: Gabriel Pinto y Andrés Pérez.

En la siguiente imagen, se observa el análisis de vulnerabilidades del servidor de correo que tiene la IP 200.107.22.232 y muestra plugins de información que no poseen ningún riesgo para la organización.

Figura 4.17 Análisis de Vulnerabilidades Nmap Servidor de Correo



Análisis de Vulnerabilidades Nmap Servidor de Correo. Elaborado por: Gabriel Pinto y Andrés Pérez.

4.3 Análisis y Gestión de Riesgos

En este punto, se identifica, calcula y prioriza los riesgos en la red ARCOTEL del edificio Zeus, mediante la relación entre las amenazas, vulnerabilidades y la naturaleza de la organización y caracterizando a los agentes de amenaza, así como las

vulnerabilidades que puedan ser aprovechadas por estos agentes, las consecuencias, la probabilidad e impacto del suceso y el principio de seguridad q se verá infectado (Confidencialidad-Integridad-Disponibilidad).

4.3.1 Perfil de Riesgo Inherente

Para establecer un nivel de seguridad se aplicó el método T-V (Threat-Vulnerability), que establece un proceso de correlación entre amenazas y vulnerabilidades con el Appliance que se encuentra actualmente en funcionamiento.

Tabla 4.1 Matriz de Riesgos Inherente

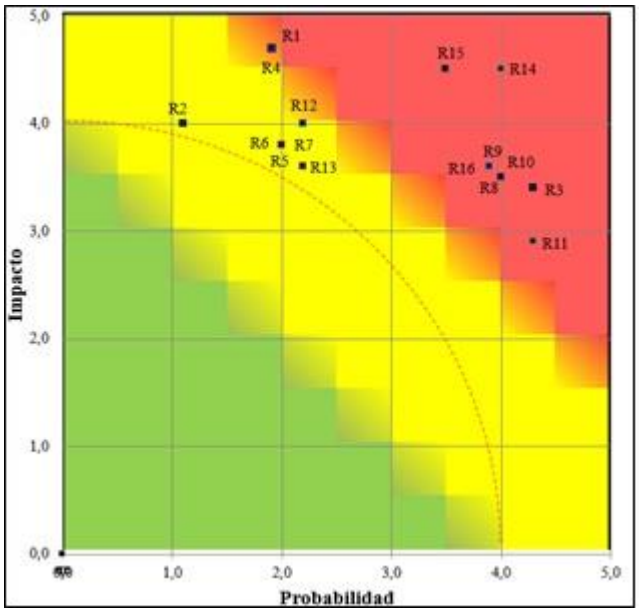
Amenaza	Tipificación de Riesgo	Riesgo	Incidente/ Problema identificado	Criticidad	Probabilidad	Impacto	Principio de Seguridad Infectado
Lógicas Servidor Web	R1	CVE-2017-7679	Apache httpd 2.4.x - 2.4.26, mod_mime.	Alto	1,9	4,7	C-I-A
	R2	CVE-2017-15715	Apache httpd 2.4.0 to 2.4.29, <Files Match> match with $	Alto	1,1	4	C-I-A
	R3	CVE-2014-0226	Apache HTTP before 2.4.10, (heap-based buffer overflow).	Medio	4,3	3,4	A
	R4	CVE-2018-1312	Apache httpd 2.2.0 to 2.4.29, HTTP Digest authentication	Alto	1,9	4,7	C-I-A
	R5	CVE-2018-17199	Apache HTTP 2.4, mod_session checks the session	Alto	2	3,8	I
	R6	CVE-2017-15710	Apache httpd 2.4.0 to 2.4.29, mod_authnz_ldap, DoS.	Alto	2	3,8	A
	R7	CVE-2016-8743	HTTP before 2.4.25, requests and sent in response lines and headers.	Alto	2	3,8	I
	R8	CVE-2017-9798	Apache HTTP before 2.4.27, read secret data from process memory	Alto	3,9	3,6	C
	R9	CVE-2016-0736	Apache HTTP 2.4.0 - 2.4.23, mod_session_crypto	Alto	3,9	3,6	C
Servidor de Correo	R10	CVE-2016-2183	DES/3DES ciphers used in the TLS and SSH	Alto	3,9	3,6	C

	R11	CVE-2015-2808	The RC4 algorithm, as used in the TLS and SSL	Medio	4,3	2,9	C
	R12	CVE-2014-3566	The SSL Protocol 3.0	Medio	2,2	4	C
	R13	CVE-2013-2566	The RC4 algorithm, as used in the TLS and SSL	Medio	2,2	3,6	C
Usuarios Externos	R14	Exempleados	Robo de información	Alto	4	4,5	C-I-A
Desastres Naturales	R15	Daños de Equipos	Back-up de equipos	Alto	3,5	4,5	C-I-A
Wifi	R16	Red Hackeada	Uso de la misma contraseña por periodos largos de tiempo	Medio	4	3,5	C-I-A

Matriz de Riesgo Inherente. Elaborado por: Gabriel Pinto y Andrés Pérez.

En la siguiente figura, se observa un mapeo de los riesgos con la plataforma PFsense, en el que se puede apreciar los valores del impacto versus la probabilidad de ejecución.

Figura 4.18 Mapeo de Riesgos Inherente



Mapeo de Riesgo Inherente. Elaborado por: Gabriel Pinto y Andrés Pérez.

4.3.2 Estrategia de Tratamiento

Para responder a los riesgos identificados se aplican cuatro acciones posibles: evitar el riesgo, reducir el riesgo, derivar el riesgo a otras partes y aceptar el riesgo

A continuación, se define las acciones tomadas según la criticidad de los riesgos detectados en la ARCOTEL:

Tabla 4.2 Tratamiento de Riesgos

Tipificación de Riesgo	Riesgo	Criticidad Riesgo Inherente	Estrategia de Tratamiento	Principio de Seguridad infectado
R1	CVE-2017-7679	Alto	REDUCIR	C-I-A
R2	CVE-2017-15715	Alto	REDUCIR	C-I-A
R3	CVE-2014-0226	Medio	REDUCIR	A
R4	CVE-2018-1312	Alto	REDUCIR	C-I-A
R5	CVE-2018-17199	Alto	REDUCIR	I
R6	CVE-2017-15710	Alto	REDUCIR	A
R7	CVE-2016-8743	Alto	REDUCIR	I
R8	CVE-2017-9798	Alto	REDUCIR	C
R9	CVE-2016-0736	Alto	REDUCIR	C
R10	CVE-2016-2183	Alto	REDUCIR	C
R11	CVE-2015-2808	Medio	REDUCIR	C
R12	CVE-2014-3566	Medio	REDUCIR	C
R13	CVE-2013-2566	Medio	REDUCIR	C
R14	Exempleados	Alto	COMPARTIR	C-I-A
R15	Daños de Equipos	Alto	ACEPTAR	C-I-A
R16	Wifi Hackeada	Alto	COMPARTIR	C-I-A

Tratamiento de Riesgos. Elaborado por: Gabriel Pinto y Andrés Pérez.

4.3.3 Perfil de Riesgo Residual

Una vez aplicados los controles de seguridad se pudo verificar una disminución sustancial en la criticidad de los riesgos inherente por cada vulnerabilidad con una nueva calificación de impacto y probabilidad.

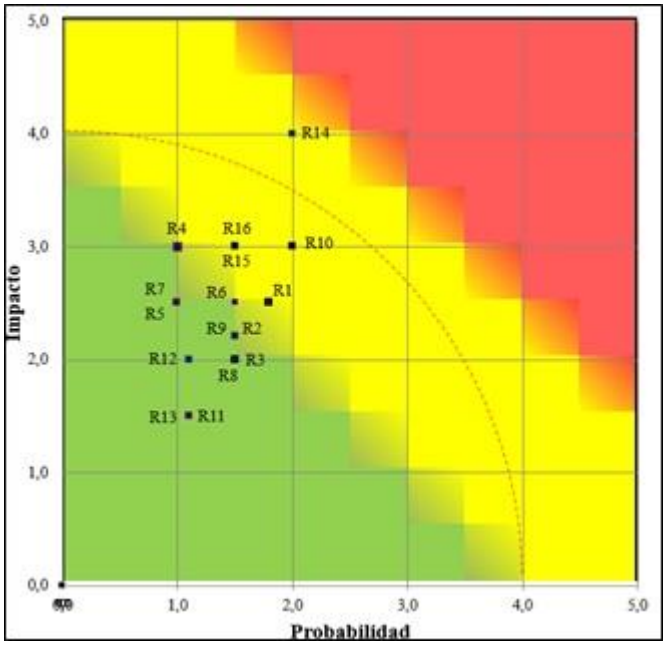
Tabla 4.3 Matriz de Riesgos Residual

Tipificación de Riesgo	Riesgo	Criticidad Riesgo Inherente	Tipo de control	Controles Sugeridos	Criticidad	Probabilidad	Impacto
R1	CVE-2017-7679	Alto	Sugerido	Actualizar	Medio	1,8	2,5
R2	CVE-2017-15715	Alto	Sugerido	Actualizar	Medio	1,5	2,0
R3	CVE-2014-0226	Medio	Sugerido	Actualizar	Bajo	1,5	2,0
R4	CVE-2018-1312	Alto	Sugerido	Actualizar	Medio	1,0	3,0
R5	CVE-2018-17199	Alto	Sugerido	Actualizar	Medio	1,0	2,5
R6	CVE-2017-15710	Alto	Sugerido	Actualizar	Medio	1,5	2,5
R7	CVE-2016-8743	Alto	Sugerido	Actualizar	Medio	1,0	2,5
R8	CVE-2017-9798	Alto	Sugerido	Actualizar	Medio	1,5	2,2
R9	CVE-2016-0736	Alto	Sugerido	Actualizar	Medio	1,5	2,2
R10	CVE-2016-2183	Alto	Sugerido	Cambiar Cifrado AES	Medio	2,0	3,0
R11	CVE-2015-2808	Medio	Sugerido	Desactivar SSL	Bajo	1,1	1,5
R12	CVE-2014-3566	Medio	Sugerido	Desactivar SSL	Bajo	1,1	2,0
R13	CVE-2013-2566	Medio	Sugerido	Desactivar SSL	Bajo	1,1	1,5
R14	Exempleados	Alto	Sugerido	Analista de seguridad	Medio	2,0	4,0
R15	Daños de Equipos	Alto	Sugerido	Analista de seguridad	Medio	1,5	3,0
R16	Red Hackeada	Alto	Sugerido	Analista de seguridad	Medio	2,0	3,0

Matriz de Riesgos Residual. Elaborado por: Gabriel Pinto y Andrés Pérez.

Se verifican además los datos individuales de los riesgos, dado que los riesgos son aceptados y reducidos para la estabilidad y seguridad de la información.

Figura 4.19 Mapeo de Riesgos Residual



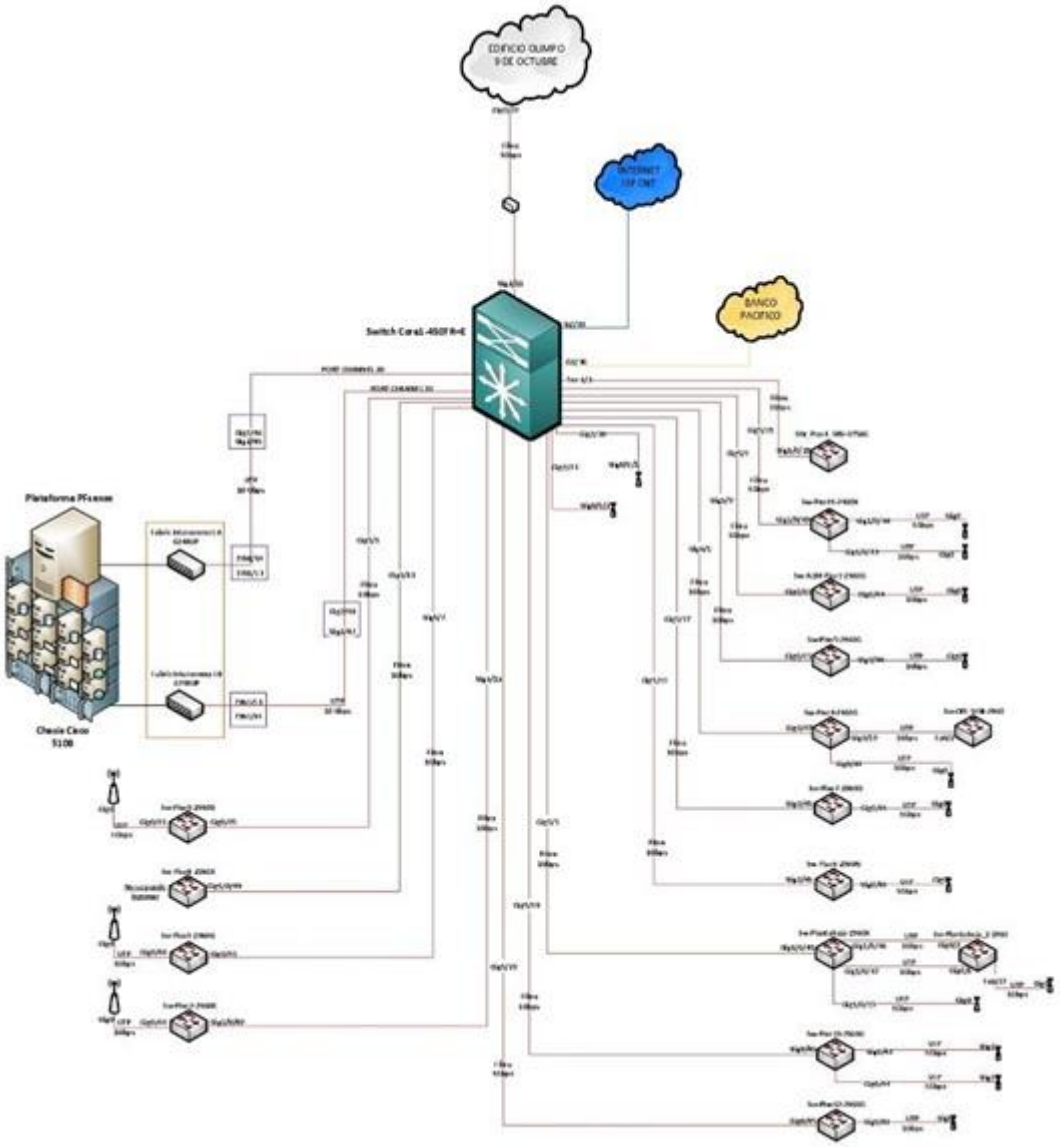
Mapeo de Riesgo Residual. Elaborado por: Gabriel Pinto y Andrés Pérez.

4.3.4 Topología Implementada

La nueva topología posee el servidor PFsense como sistema de seguridad perimetral, para la centralización de los servicios de seguridad, contribuir con el Decreto No 1014 y evitar los problemas de actualización por licenciamiento.

Esta plataforma sustituyó a PaloAlto 3020, mediante la conexión directa de las redes Internet y Banco del Pacifico hacia las interfaces g2/33 y g2/36 respectivamente del Switch 4507R+E como se aprecia en la figura 4.20

Figura 4.20 Topología establecida con la plataforma PFsense



Topología establecida con la plataforma PFsense. Elaborado por: Andrés Pérez y Gabriel Pinto.

CONCLUSIONES

Los procesos de detección, prevención y mitigación de riesgos constituyen estrategias fundamentales y prioritarias que están orientadas a definir las fortalezas y debilidades de una organización en cuanto a aspectos de seguridad y a partir de ellas se pueden desplegar un conjunto de medidas de control para proteger los activos de la organización.

La implementación de un UTM basado en PFsense permitió aprovechar varias de sus funcionalidades como son NAT, políticas de seguridad, multienlace WAN y herramientas de seguridad IPS e IDS; las mismas que se complementaron con su capacidad de tolerancia frente a factores que intervienen en el rendimiento del sistema como es el Throughput y sesiones concurrentes para respaldar el desempeño y estabilidad de la plataforma.

El uso de herramientas informáticas de código abierto representa una alternativa de gran relevancia e impacto ya que ofrecen iguales e incluso mejores funcionalidades y que los aplicativos propietarios y que apoyan la ejecución del Decreto Ejecutivo No.1014 sobre el uso de software libre en los sistemas informáticos de la administración pública del Ecuador con el propósito de alcanzar soberanía y autonomía tecnológica.

Las pruebas de pentesting permitieron identificar y priorizar las vulnerabilidades potenciales en la red de ARCOTEL, y a partir de ello se definieron los controles y tratamientos adecuados con el objetivo de reducir, eliminar, aceptar o transferirlos a fin de garantizar la continuidad operativa y un nivel de protección óptimo en la Institución.

RECOMENDACIONES

La capacidad de almacenamiento de PFsense en entornos de producción empresarial fue diseñada para soportar una carga anual de los logs del Firewall, así como del IPS e IDS, por lo tanto, se recomienda realizar un mantenimiento preventivo de los registros irrelevantes en el periodo estimado para evitar la afectación del desempeño y/o saturación del sistema.

Para optimizar la implementación de un UTM basado en Pfsense, se podría aprovechar la versatilidad que ofrece esta plataforma instalando varias máquinas virtuales como Firewall de frontera para cada subred según las necesidades particulares de las mismas donde se requiera impulsar el nivel de seguridad informático.

La fortaleza de un sistema de seguridad de la información es tan fuerte como como el eslabón más débil de una organización y que generalmente son las personas, razón por la cual las campañas de información y concientización representan una de las estrategias más importantes que coadyuvan a disminuir los riesgos y brechas de seguridad que puede presentar una organización.

El análisis y gestión de riesgos son actividades que deben realizarse de forma permanente ya que ayudan a visibilizar las vulnerabilidades existentes en una organización y a partir de ello mejorar los niveles de seguridad para evitar posibles eventos que perjudiquen a la entidad.

BIBLIOGRAFÍA

Russell Rothstein y Naftali Marcus. (29 de Abril de 2013). *IT Central Station*. Obtenido de https://www.itcentralstation.com/about

Astudillo K. (2018). *Hacking Ético* (3era ed.). Madrid: Ra-Ma 2018. Obtenido de Seguridad Informatica Facil: http://www.tecno-libro.es/ficheros/descargas/9788499647678.pdf

B. M. (Febrero de 2011). *Instituto Nacional de Ciberseguridad.* Obtenido de www.incibe.es: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Big Data Marker. (6 de Septiembre de 2015). *Big Data Social*. Obtenido de http://www.bigdata-social.com/informe-cuadrante-magico-gartner/

Cisco. (Septiembre de 2010). *www.cisco.com*. Obtenido de https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/unified-computing/at_a_glance_c45-523181.pdf

Cisco, A. (2013). Throughput. En W. Odom. United States of America: Cisco Press.

Divino, B. V. (2017-2018). *Evaluación y gestión de vulnerabilidades: Como sobrevivir en el mundo de los ciberataques.* Trabajo Fin de Grado, Universdad Politécnica de Valencia, Ingeniería Informática, Valencia.

Dominguez, J. P. (2015). *Analisis de Vulnerabilidades de una red Corporativa mediante herramientas de Descubrimiento Activas.* Escuela Técnica Superior de Ingeniería, Ingeniería Telemática, Sevilla.

FreeBSD. (3 de Marzo de 2014). *www.freebsd.org*. Obtenido de https://www.freebsd.org/es/about.html

Fundation, F. S. (21 de Marzo de 2019). *Free Software Fundation*. Recuperado el 15 de Abril de 2019, de https://www.gnu.org/philosophy/free-sw.es.html#mission-statement

Imperva. (2019). *Imperva Incapsula*. Obtenido de https://www.incapsula.com/ddos/attack-glossary/slowloris.html

Kaspersky Lab. (27 de Septiembre de 2016). *www.kaspersky.es*. Recuperado el 4 de Diciembre de 2018, de https://latam.kaspersky.com/resource-center/definitions/utm

Maria Narváez. (2018). *ANÁLISIS DE LA DISTRIBUCIÓN KALI LINUX, SU APLICACIÓN EN LA CONFIGRACIÓN DE UN SISTEMA DETECTOR DE INTRUSIONES Y LA VALIDACIÓN DEL SISTEMA EN LA RED DE DATOS DE LA SEDE SUR DE QUITO DE LA UNIVERSIDAD POLTÉCNICA SALESIANA.* Quito.

Ortiz, D. (2015). *Repositorio Universidad Los Libertadores.* Recuperado el 22 de Marzo de 2019, de https://repository.libertadores.edu.co/bitstream/handle/11371/342/DiegoFernandoOrtizAristizabal.pdf?sequence=2&isAllowed=y

Panda Security S.L. (3 de Septiembre de 2018). *Panda Security*. Recuperado el 4 de Diciembre de 2018, de https://www.pandasecurity.com/spain/support/card?id=31463

Recio, M. (2015). Gestión de mantenimiento en sistemas ERP y CRM. En *En UF1885 - Administración del sistema operativo en sistemas ERP-CRM* (5 ed., pág. 416). Málaga, España: Elearning S. L.

Santos, & Stuppi. (2015). Fundamentals of VPN Technology and Cryptography. En *CNNA Security 210-260 Official Cert Guide* (pág. 87). United States of America: Cisco Press.

Santos, & Stuppi. (2015). Networking Security Concepts. En *CNNA Security 210-260 Official Cert Guide* (pág. 6). United States of America: Cisco Press.

Santos, & Stuppi. (2015). VLAN and Trunking Fundamentals. En *CNNA Security 210-260 Official Cert Guide* (pág. 236). United States of America: Cisco Press.

Security Offensive. (2019). Obtenido de Kali Tools: https://tools.kali.org/information-gathering/maltego-teeth

Security Offensive. (2019). *Kali Tools*. Obtenido de https://tools.kali.org/uncategorized/metasploit

Security Offensive. (2019). *Kali Tools*. Obtenido de https://tools.kali.org/information-gathering/sublist3r

Security Offensive. (2019). *Kali Tools*. Obtenido de https://tools.kali.org/information-gathering/nmap

Tenable. (2019). *Nessus Professional*. Obtenido de https://www.tenable.com/products/nessus/nessus-professional

Verdesoto, A. (Octubre de 2007). *biblioteca digital EPN.* Recuperado el 2019 de 03 de 22, de http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

ANEXO A

AUTORIZACIONES

Anexo 1.- Solicitud de Autorización del Proyecto

AGENCIA DE REGULACIÓN Y CONTROL
DE LAS TELECOMUNICACIONES

EL GOBIERNO DE TODOS

Oficio Nro. ARCOTEL-CPDT-2018-0022-OF

Quito, D.M., 11 de septiembre de 2018

Asunto: Autorización para Plan de Tesis denominado: "Sistema de Seguridad Perimetral para el edificio Matriz de la Agencia de Regulación y Control de las Telecomunicaciones â ARCOTEL, basado en tecnologías UTM de código abierto".

Señor Ingeniero
Ramón Enrique Pérez Pineda
Docente de la Universidad Politécnica Salesiana
UNIVERSIDAD POLITECNICA SALESIANA
En su Despacho

De mi consideración:

Estimado Ingeniero, mediante el presente informó a usted, que ha petición de los señores Andrés Mauricio Pérez Lasso, portador de la cedula de ciudadanía No. 171971630-8 y Gabriel Elías Pinto Gutiérrez, portador de la cédula de ciudadanía No. 172205676-7 alumnos de la Universidad Politécnica Salesiana, y en mi calidad de Director de la Dirección de Tecnologías de la Información y Comunicación de la Agencia de Regulación y Control de las Telecomunicaciones — ARCOTEL, he autorizado para que el Área de Gestión de Infraestructura Tecnológica y Seguridad Informática, para que bajo mi supervisión se entregue la información e insumos requeridos a fin de que el peticionario pueda desarrollar con éxito del plan de tesis de grado que se fundamentará en el "Sistema de Seguridad Perimetral para el edificio Matriz de la Agencia de Regulación y Control de las Telecomunicaciones — ARCOTEL, basado en tecnologías UTM de código abierto".

Particular que pongo en su conocimiento, para los fines pertinentes.

Atentamente,

Agencia de Regulación y Control de las Telecomunicaciones

Mgs. Freddy Patricio Gallegos Guzman
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Copia:
Señor Ingeniero
Giovanny Marcelo Males Cevallos
Analista de Tecnologías de la Información y Comunicación 2

pg

UNIVERSIDAD POLITÉCNICA SALESIANA
DIRECCIONES DE CARRERA
12 SET. 2018
RECIBIDO
Mayra Guerrero
SECRETARIA

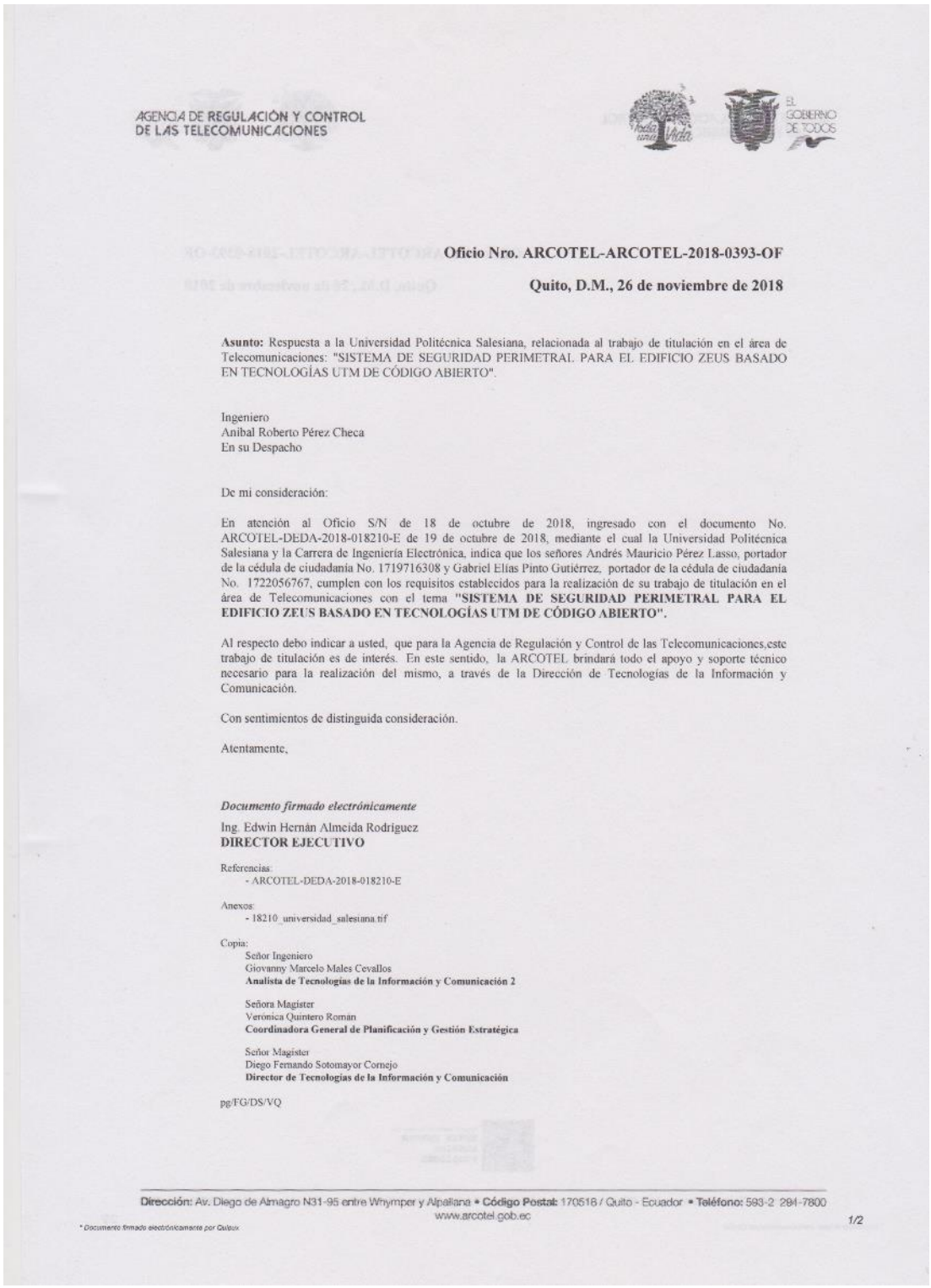
Dirección: Av. 9 de Octubre N 27-75 y Berlín • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 2946-400
www.arcotel.gob.ec

* Documento generado por Dojbux

1/1

Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 2.- Autorización del Director Ejecutivo



AGENCIA DE REGULACIÓN Y CONTROL
DE LAS TELECOMUNICACIONES

EL GOBIERNO DE TODOS

Oficio Nro. ARCOTEL-ARCOTEL-2018-0393-OF

Quito, D.M., 26 de noviembre de 2018

Asunto: Respuesta a la Universidad Politécnica Salesiana, relacionada al trabajo de titulación en el área de Telecomunicaciones: "SISTEMA DE SEGURIDAD PERIMETRAL PARA EL EDIFICIO ZEUS BASADO EN TECNOLOGÍAS UTM DE CÓDIGO ABIERTO".

Ingeniero
Aníbal Roberto Pérez Checa
En su Despacho

De mi consideración:

En atención al Oficio S/N de 18 de octubre de 2018, ingresado con el documento No. ARCOTEL-DEDA-2018-018210-E de 19 de octubre de 2018, mediante el cual la Universidad Politécnica Salesiana y la Carrera de Ingeniería Electrónica, indica que los señores Andrés Mauricio Pérez Lasso, portador de la cédula de ciudadanía No. 1719716308 y Gabriel Elías Pinto Gutiérrez, portador de la cédula de ciudadanía No. 1722056767, cumplen con los requisitos establecidos para la realización de su trabajo de titulación en el área de Telecomunicaciones con el tema **"SISTEMA DE SEGURIDAD PERIMETRAL PARA EL EDIFICIO ZEUS BASADO EN TECNOLOGÍAS UTM DE CÓDIGO ABIERTO".**

Al respecto debo indicar a usted, que para la Agencia de Regulación y Control de las Telecomunicaciones,este trabajo de titulación es de interés. En este sentido, la ARCOTEL brindará todo el apoyo y soporte técnico necesario para la realización del mismo, a través de la Dirección de Tecnologías de la Información y Comunicación.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Ing. Edwin Hernán Almeida Rodríguez
DIRECTOR EJECUTIVO

Referencias:
- ARCOTEL-DEDA-2018-018210-E

Anexos:
- 18210_universidad_salesiana.tif

Copia:
Señor Ingeniero
Giovanny Marcelo Males Cevallos
Analista de Tecnologías de la Información y Comunicación 2

Señora Magíster
Verónica Quintero Román
Coordinadora General de Planificación y Gestión Estratégica

Señor Magíster
Diego Fernando Sotomayor Cornejo
Director de Tecnologías de la Información y Comunicación

pg/FG/DS/VQ

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-7800
www.arcotel.gob.ec

* Documento firmado electrónicamente por Quipux

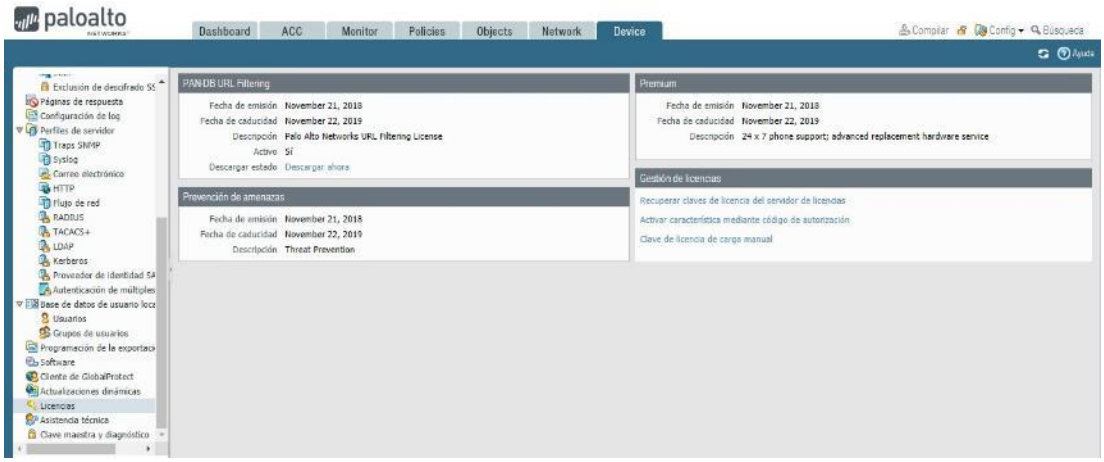
1/2

Elaborado por: Andrés Pérez y Gabriel Pinto

ANEXO B

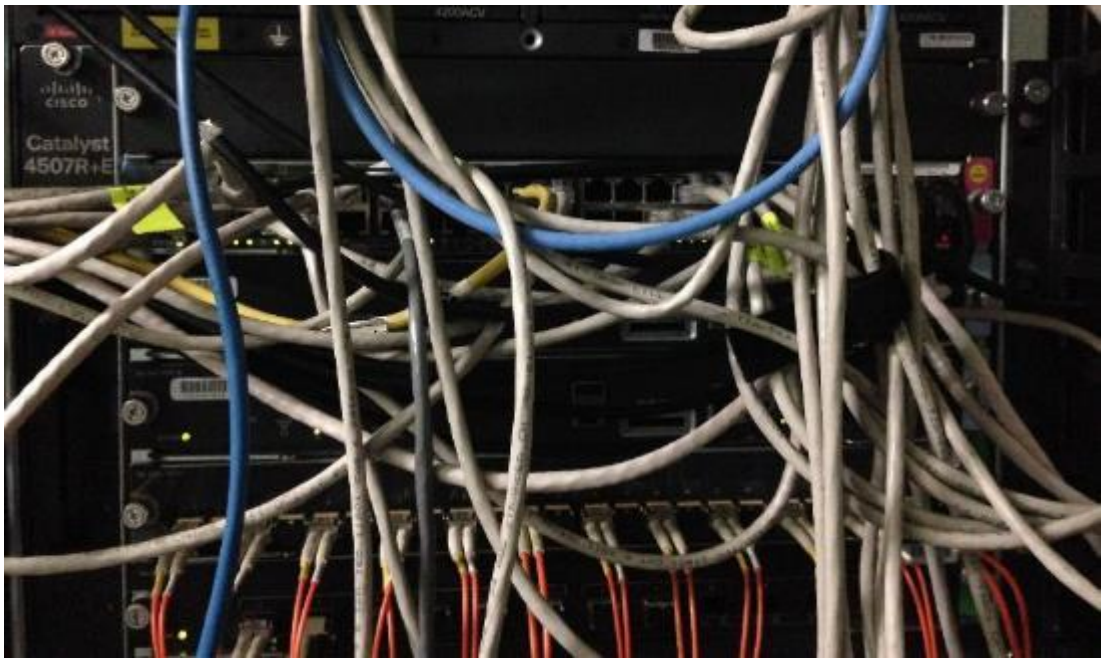
LEVANTAMIENTO DE INFORMACION

Anexo 3.- Fecha de Vencimiento del Firewall 3020



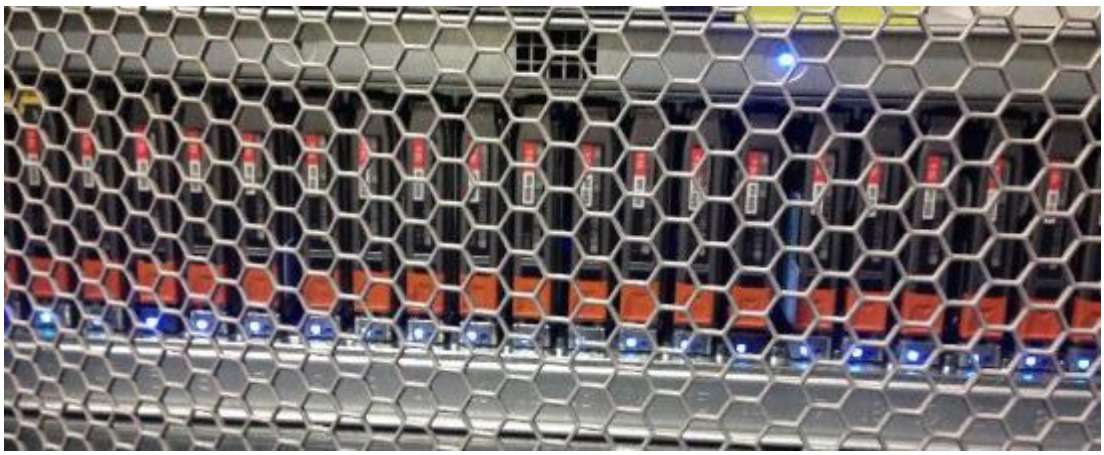
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 4.- Dispositivo Central Switch 4507R+E



Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 5.- Storage de 24 discos SAS 600Gb a 10K



Elaborado por: Andrés Pérez y Gabriel Pinto

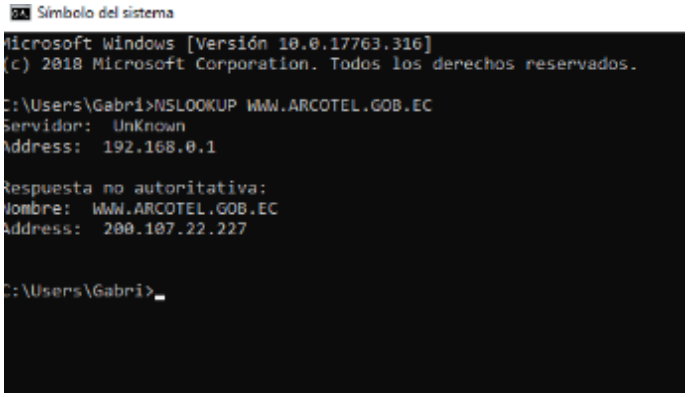
Anexo 6.- Blade Server UCS 5108 de 8 Slots

Elaborado por: Andrés Pérez y Gabriel Pinto

ANEXO C

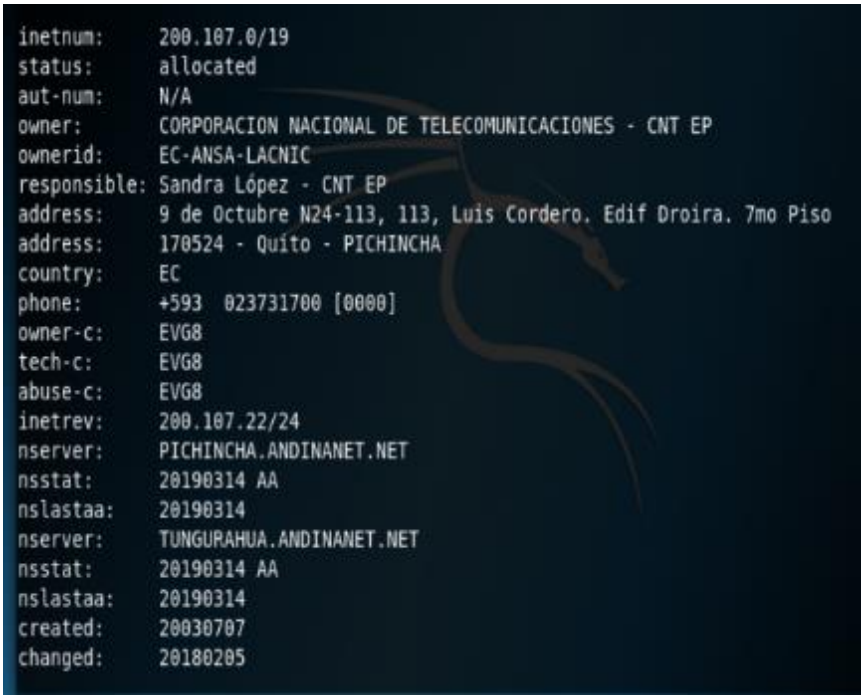
PENTESTING

Anexo 7.- IP del DNS de www.arcotel.gob.ec



Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 8.- Información con el comando who.is



Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 9.- Búsqueda del dominio en www.iplocation.net

Geolocation data from IP2Location (Product: DB6, updated on 2019-5-1)

IP Address	Country	Region	City
200.107.22.227	Ecuador	Pichincha	Quito
ISP	**Organization**	**Latitude**	**Longitude**
Corporacion Nacional de Telecomunicaciones - CNT EP	Not Available	-0.2298	-78.5249

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
200.107.22.227	Ecuador	Provincia del Tungurahua	Ambato
ISP	**Organization**	**Latitude**	**Longitude**
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP (andinanet.net)	-1.2500	-78.6167

Elaborado por: Andrés Pérez y Gabriel Pinto

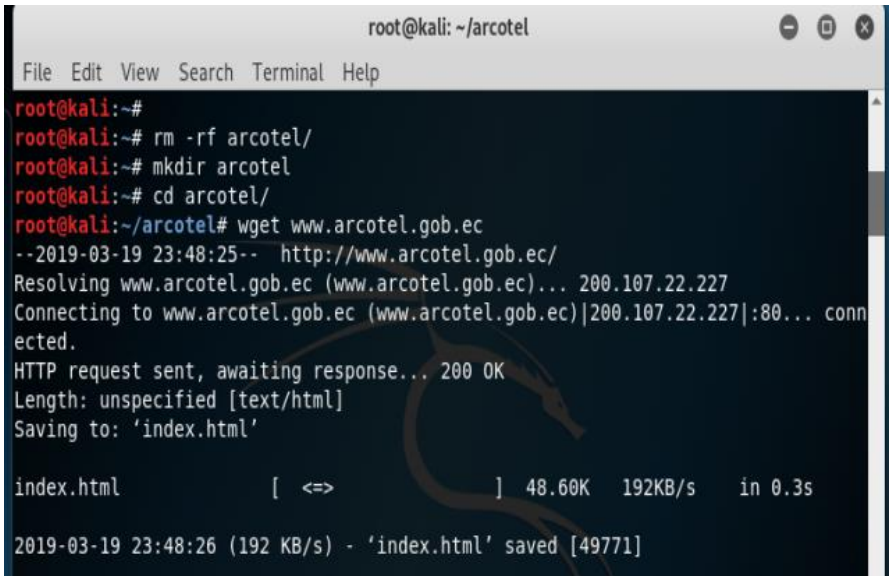
Anexo 10.- Búsqueda del dominio en who.is. Fuente: https://who.is/

DNS Records for arcotel.gob.ec

Hostname	Type	TTL	Priority	Content
arcotel.gob.ec	SOA	7199		root.andinanet.net hostmaster@andinanet.net 2018092401 14400 3600 604800 3600
arcotel.gob.ec	NS	7199		pichincha.andinanet.net
arcotel.gob.ec	NS	7199		tungurahua.andinanet.net
arcotel.gob.ec	A	7199		200.107.22.227
arcotel.gob.ec	MX	7199	10	mailregulacion.arcotel.gob.ec
arcotel.gob.ec	MX	7199	100	mx2.arcotel.gob.ec
www.arcotel.gob.ec	A	7199		200.107.22.227

Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 11.- Descarga del archivo index.html

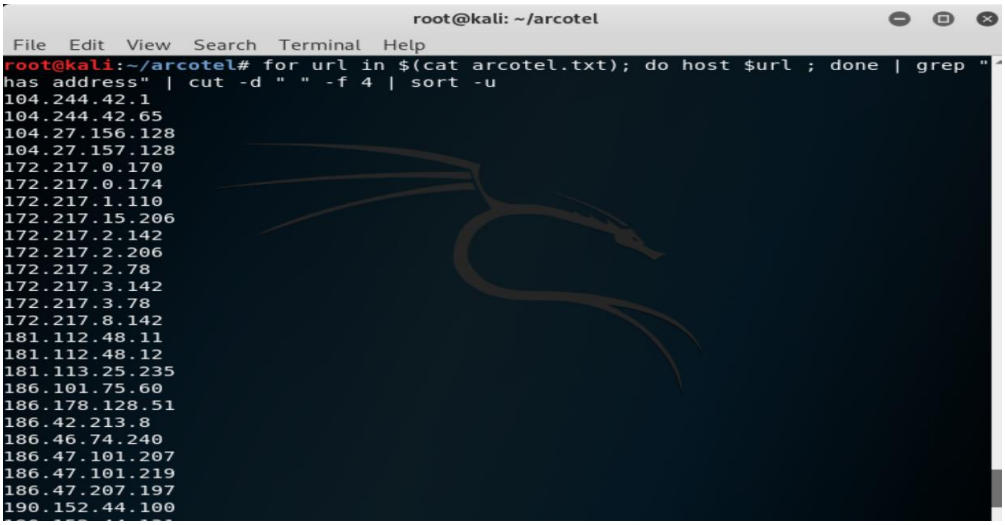


Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 12.- Filtrados de dominios y subdominios de Arcotel

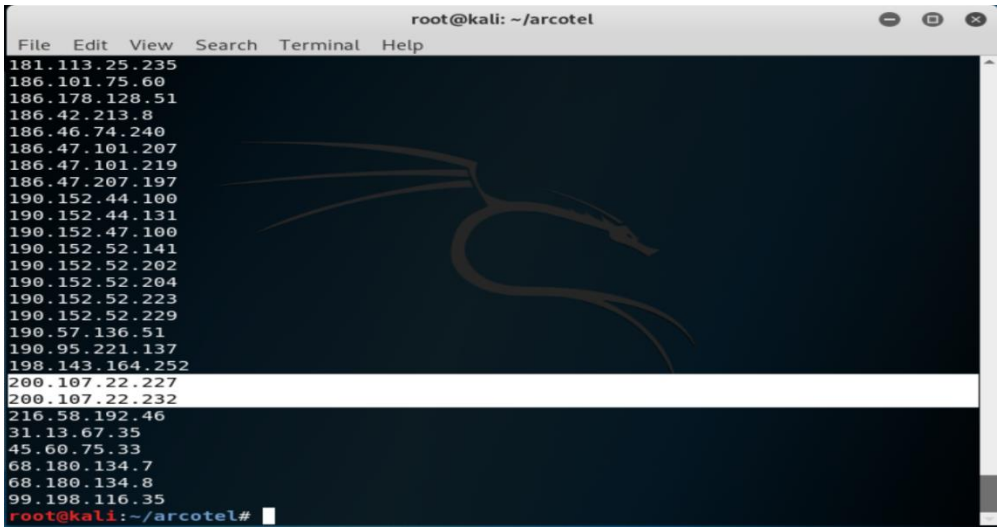
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 13.- IP´s de dominios y subdominios de Arcotel parte 1



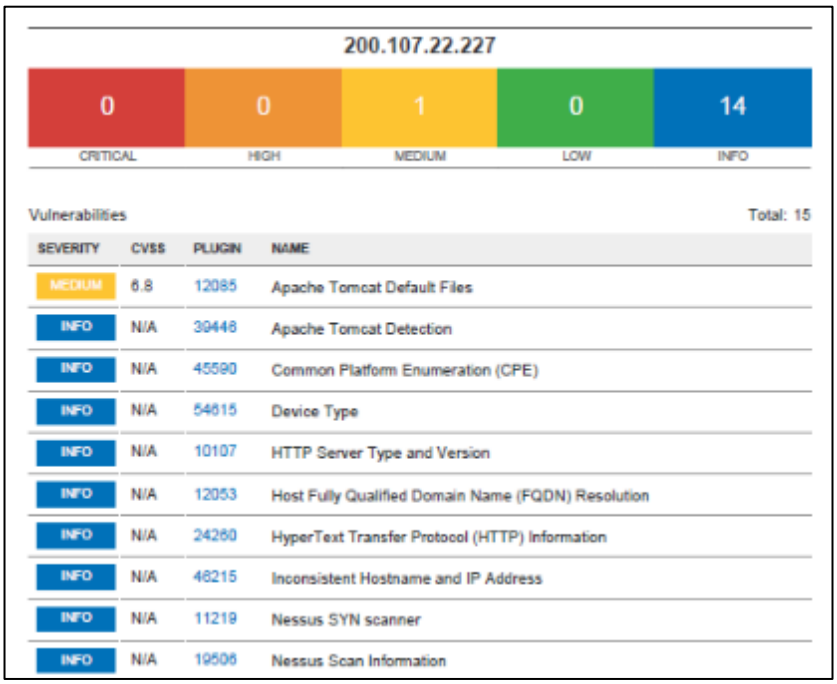
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 14.- IP´s de dominios y subdominios de Arcotel parte 2



Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 15.- Escaneo del Servidor Web con Nessus



200.107.22.227

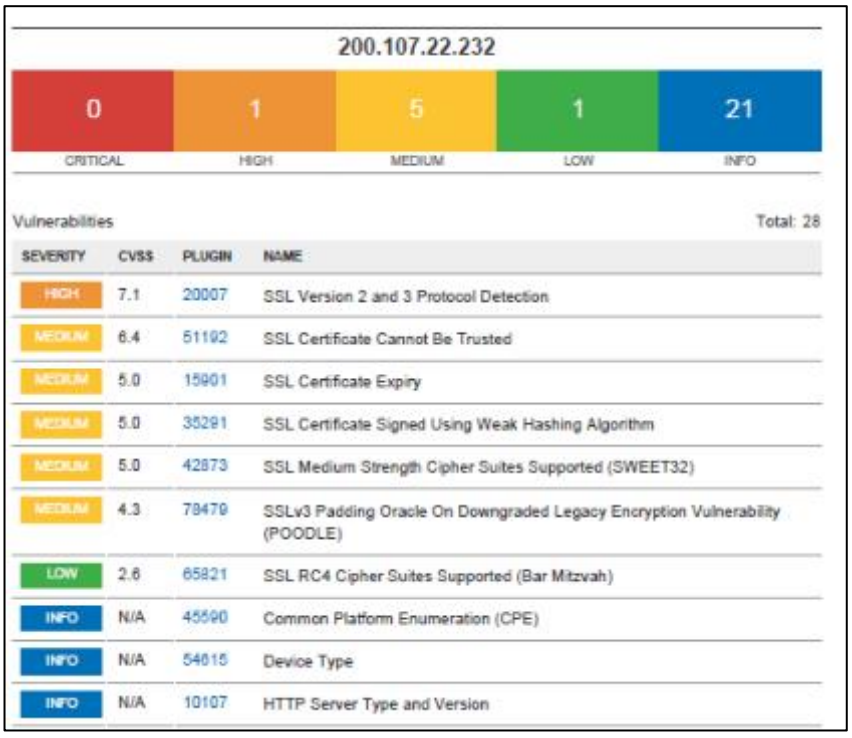
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	14

Vulnerabilities — Total: 15

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.8	12085	Apache Tomcat Default Files
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 16.- Escaneo del Servidor Correo con Nessus



200.107.22.232

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	5	1	21

Vulnerabilities — Total: 28

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	10107	HTTP Server Type and Version

Elaborado por: Andrés Pérez y Gabriel Pinto

ANEXO D

RANKING FIREWALLS

Anexo 17.- Ranking Firewalls de la IT Central Station

Elaborado por: IT Central Station

DATASHEET

Anexo 18.- Features Appliances Virtuales Fortinet

Fortinet FortiGate VM00

Consolidated Security for Virtual Environments

FORTINET PLATINUM PARTNER

Fortinet FortiGate Series

FortiGate VM00

FortiGate-VM virtual appliance designed for all supported platforms. 1x vCPU core, (up to) 2 GB RAM

#FG-VM00
List Price: ~~$1,799.00~~
Our Price: $1,326.04

Add to Cart

Overview | Deployments | Platform | Specifications | Services | Documentation

Specifications:

	FG-VM00	FG-VM01 / VM01V	FG-VM02 / VM02V	FG-VM04 / VM04V	FG-VM08 / VM08V	FG-VM16 / VM16V	FG-VM32 / VM32V	FG-VMUL / VMULV
Technical Specifications								
vCPU Support (Minimum / Maximum)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / Unlimited
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10
Memory Support (Minimum / Maximum)	1 GB / 2 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB	1 GB / 12 GB	1 GB / 24 GB	1 GB / 48 GB	1 GB / Unlimited
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 32	32 / 64	256 / 512	256 / 512	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum)	2 / 2	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Maximum Number of FortiTokens	1,000	1,000	1,000	5,000	5,000	5,000	5,000	5,000
Maximum Number of Registered Endpoints	200	2,000	2,000	8,000	20,000	20,000	20,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Performance								
Firewall Throughput (UDP Packets, SR-IOV Enabled)	12 Gbps	12 Gbps	15 Gbps	28 Gbps	33 Gbps	36 Gbps	50 Gbps	-
Concurrent Sessions (TCP)	1.0 Million	1.0 Million	2.6 Million	4.3 Million	8.5 Million	18.0 Million	38.0 Million	-
New Sessions / Second (TCP)	85,000	85,000	100,000	125,000	150,000	175,000	200,000	-
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	1.0 Gbps	1.0 Gbps	1.5 Gbps	3.0 Gbps	5.5 Gbps	6.5 Gbps	7 Gbps	-
Gateway-to-Gateway IPsec VPN Tunnels	2,000	2,000	2,000	2,000	40,000	40,000	40,000	-
Client-to-Gateway IPsec VPN Tunnels	6,000	6,000	12,000	20,000	40,000	50,000	64,000	-
SSL-VPN Throughput	800 Mbps	800 Mbps	830 Mbps	2 Gbps	4.5 Gbps	8.5 Gbps	8.6 Gbps	-
Concurrent SSL-VPN Users (Recommended Maximum)	1,000	1,000	2,000	4,500	10,000	25,000	40,000	-
IPS Throughput (HTTP / Enterprise Mix)[1]	3.5 Gbps / 1 Gbps	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8.0 Gbps / 3.0 Gbps	15.5 Gbps / 6.0 Gbps	25.0 Gbps / 12.0 Gbps	29.0 Gbps / 19.0 Gbps	-
Application Control Throughput[2]	2.0 Gbps	2.0 Gbps	2.6 Gbps	4.5 Gbps	9.0 Gbps	17.0 Gbps	17.5 Gbps	-
NGFW Throughput[3]	850 Mbps	850 Mbps	1.5 Gbps	2.5 Gbps	4.5 Gbps	9.0 Gbps	16.5 Gbps	-
Threat Protection Throughput[4]	700 Mbps	700 Mbps	1.2 Gbps	2.0 Gbps	3.5 Gbps	7.0 Gbps	13.0 Gbps	-

Elaborado por: Fortinet

Anexo 19.- Features Appliances Virtuales Sophos

Cyberoam Virtual Cyberoam CRiV-1C

Take Control of Your Security Infrastructure!

Cyberoam Virtual Series

Cyberoam Virtual Cyberoam CRiV-1C
Support for maximum 1 Virtual CPU Core

#01-CRiV-01C-01
Our Price: $459.00

Add to Cart

Technical Specifications

	CRiV-1C	CRiV-2C	CRiV-1C	CRiV-8C	CRiV-12C
Hypervisor Support	Vmware ESx/ESxi 4.0/4.1/5.0, VMware Workstation 7.0/8.0/9.0, VMware Player 4.0/5.0, Microsoft Hyper-V 2008/2012				
vCPU Support (Min / Max)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 12
Network Interface Support (Min / Max)	3 / 10	3 / 10	3 / 10	3 / 10	3 / 10
Memory Support (Min / Max)	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB	1 GB / 4 GB
System Performance*					
	CRiV-1C	CRiV-2C	CRiV-1C	CRiV-8C	CRiV-12C
Firewall Throughput (UDP) (Mbps)	1,500	3,000	3,500	4,000	4,000
Firewall Throughput (TCP) (Mbps)	1,200	2,500	3,000	3,500	4,000
New sessions/second	25,000	30,000	40,000	50,000	60,000
Concurrent sessions	230,000	525,000	1,200,000	1,500,000	1,750,000
IPSec VPN Throughput (Mbps)	200	250	300	350	400
No. of IPSec Tunnels	200	1,000	1,500	2,000	2,500
SSL VPN Throughput (Mbps)	300	400	550	550	750
WAF Protected Throughput (Mbps)	300	500	800	1,400	1,550
Anti-Virus Throughput (Mbps)	900	1,500	2,000	2,200	2,450
IPS Throughput (Mbps)	450	750	1,200	1,800	1,900
UTM Throughput (Mbps)	250	450	1,000	1,400	1,550
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

Elaborado por: Cyberoam Sophos

Anexo 20.- Feature Appliance Virtuales Paloalto

Palo Alto Networks Commerical List
Price Book

Palo Alto Networks	PAN-VM-50-PERP-BASC-PREMUSG-1YR-R	Palo Alto Networks Perpetual Bundle (Basic) for VM-Series that includes US Government Premium Support, 1 year, Renewal	160.0000
Palo Alto Networks	PAN-VM-50-PERP-BASC-PREMUSG-3YR	Palo Alto Networks Perpetual Bundle (Basic) for VM-Series that includes VM-50 and US Government Premium Support, 3 year	1100.0000
Palo Alto Networks	PAN-VM-50-PERP-BASC-PREMUSG-3YR-R	Palo Alto Networks Perpetual Bundle (Basic) for VM Series that includes US Government Premium Support, 3 year, Renewal	510.0000
Palo Alto Networks	PAN-VM-50-PERP-BASC-PREMUSG-5YR	Palo Alto Networks Perpetual Bundle (Basic) for VM Series that includes VM-50 and US Government Premium Support, 5 year	1350.0000
Palo Alto Networks	PAN-VM-50-PERP-BASC-PREMUSG-5YR-R	Palo Alto Networks Perpetual Bundle (Basic) for VM-Series that includes US Government Premium Support, 5 year, Renewal	740.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-1YR	Palo Alto Networks Perpetual Bundle (BND1) for VM-Series that includes VM-50, Threat Prevention subscription, and Premium Support	1000.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-1YR-R	Palo Alto Networks Perpetual Bundle (BND1) for VM-Series that includes Threat Prevention subscription, and Premium Support, 1 year, Renewal	280.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-3YR	Palo Alto Networks Perpetual Bundle (BND1) for VM-Series that includes VM-50, Threat Prevention subscription, and Premium Support, 3 year	1350.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-3YR-R	Palo Alto Networks Perpetual Bundle (BND1) for VM Series that includes Threat Prevention subscription, and Premium Support, 3 year, Renewal	670.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-5YR	Palo Alto Networks Perpetual Bundle (BND1) for VM Series that includes VM-50, Threat Prevention subscription, and Premium Support, 5 year	1800.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREM-5YR-R	Palo Alto Networks Perpetual Bundle (BND1) for VM-Series that includes Threat Prevention subscription, and Premium Support, 5 year, Renewal	1120.0000
Palo Alto Networks	PAN-VM-50-PERP-BND1-PREMUSG-1YR	Palo Alto Networks Perpetual Bundle (BND1) for VM-Series that includes VM-50, Threat Prevention subscription, and US Government Premium Support	1000.0000

Virtualization Specifications

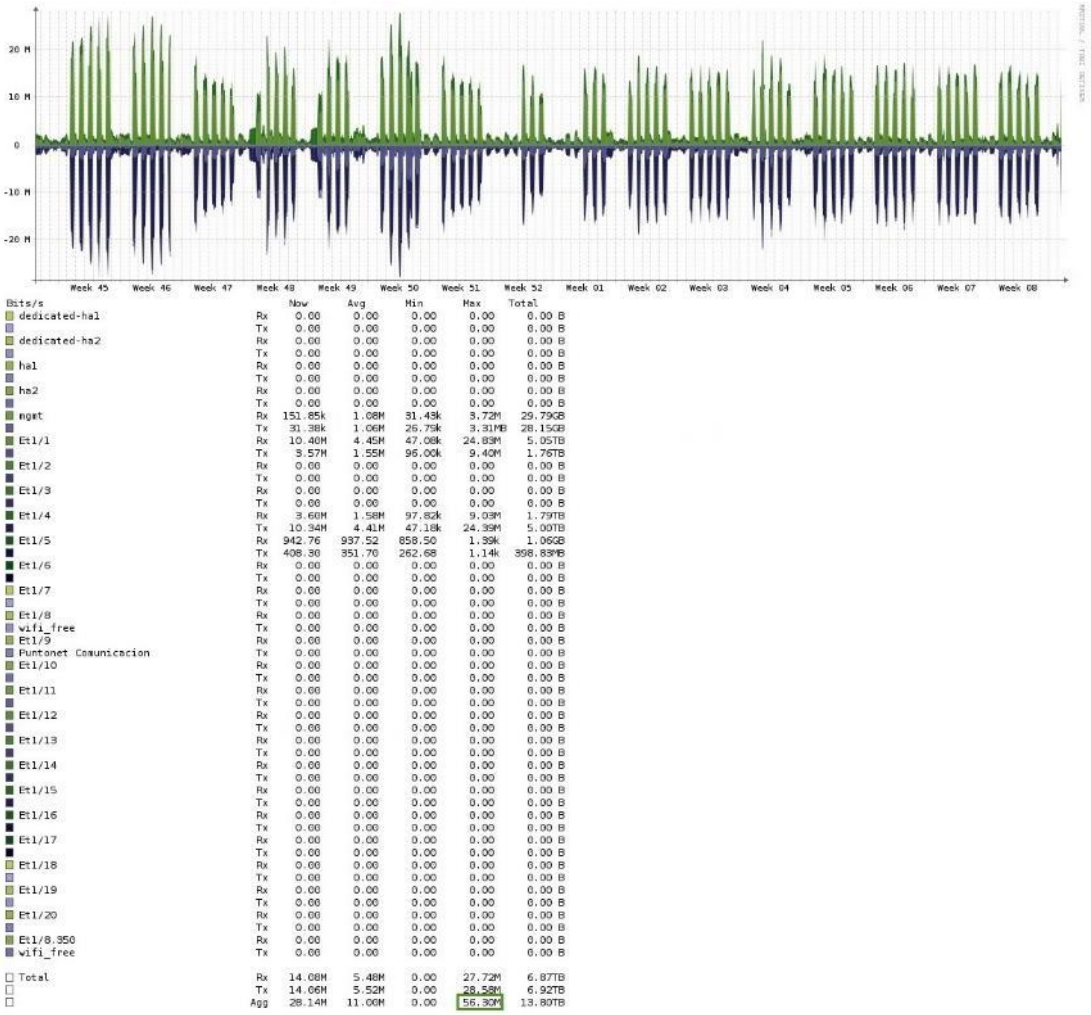
Image formats supported	OVA
Hypervisors supported	VMware ESXi 5.1, 5.5 and 6.0 VMware NSX Manager 6.0, 6.1 and 6.2
Network I/O options	• VMware paravirtual drivers (vmxnet3, e1000) • PCI pass-through • Single-root I/O Virtualization (SR-IOV)

Performance and Capacities	VM-50 (0.4 core)	VM-100/ VM200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 cores)
With Single Root I/O Virtualization (SR-IOV)/PCI Passthrough of I/O enabled					
Firewall throughput (App-ID enabled)	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
Threat prevention throughput	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
IPsec VPN throughput*	In process	In process	In process	In process	In process
With VMware Distributed Virtual Switch (VMXNET3)					
Firewall throughput (App-ID enabled)	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
Threat prevention throughput	50 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps
IPsec VPN throughput*	In process	In process	In process	In process	In process
Capacities					
New sessions per second	1,000	8,000	15,000	30,000	60,000
Max sessions	50,000	250,000	800,000	2,000,000	10,000,000

System Requirements	VM-50 (0.4 Core)	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 Cores)
vCPU configurations supported	2[1]	2	2,4	2,4 and 8	2,4,8 and 16
Memory (minimum)	4.5GB	6.5GB	9GB	16GB	56GB
Disk drive capacity (min/max)	32GB/2TB	60GB/2TB	60GB/2TB	60GB/2TB	60GB/2TB

Elaborado por: PaloAlto Networks

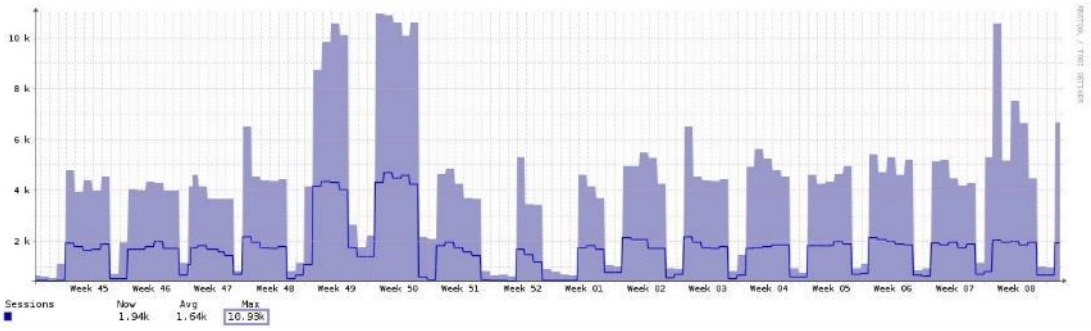
Anexo 21.- Throughput del enlace LAN de la matriz ARCOTEL



Bits/s		Now	Avg	Min	Max	Total
dedicated-ha1	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
dedicated-ha2	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
ha1	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
ha2	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
mgmt	Rx	151.85k	1.08M	31.48k	3.72M	29.79GB
	Tx	31.38k	1.06M	26.75k	3.31MB	28.15GB
Et1/1	Rx	10.40M	4.45M	47.08k	24.83M	5.05TB
	Tx	3.57M	1.55M	96.00k	9.40M	1.76TB
Et1/2	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/3	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/4	Rx	3.60M	1.58M	97.82k	9.08M	1.79TB
	Tx	10.34M	4.41M	47.18k	24.39M	5.00TB
Et1/5	Rx	942.76	937.52	858.50	1.39k	1.06GB
	Tx	408.30	351.70	262.68	1.14k	398.83MB
Et1/6	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/7	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/8	Rx	0.00	0.00	0.00	0.00	0.00 B
wifi_free	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/9	Rx	0.00	0.00	0.00	0.00	0.00 B
Puntonet Comunicacion	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/10	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/11	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/12	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/13	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/14	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/15	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/16	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/17	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/18	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/19	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/20	Rx	0.00	0.00	0.00	0.00	0.00 B
	Tx	0.00	0.00	0.00	0.00	0.00 B
Et1/8.350	Rx	0.00	0.00	0.00	0.00	0.00 B
wifi_free	Tx	0.00	0.00	0.00	0.00	0.00 B
Total	Rx	14.08M	5.48M	0.00	27.72M	6.87TB
	Tx	14.06M	5.52M	0.00	28.58M	6.92TB
	Agg	28.14M	11.00M	0.00	56.30M	13.80TB

Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 22.- Sesiones Concurrentes del Appliance Firewall 3020

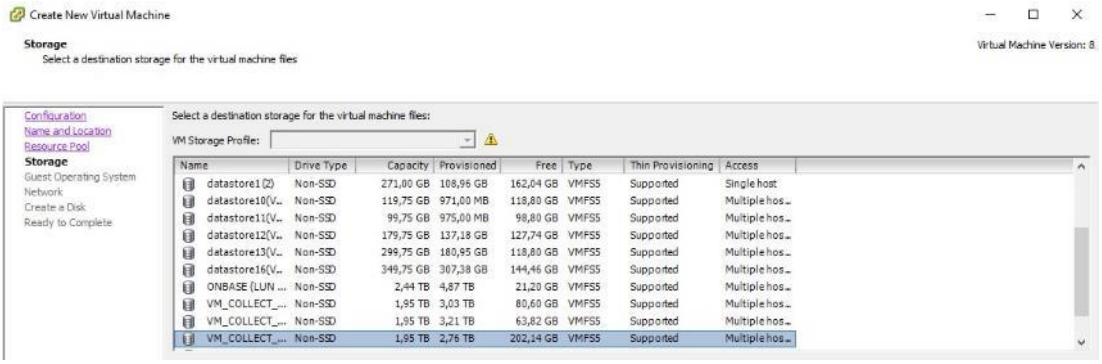


Elaborado por: Andrés Pérez y Gabriel Pinto

ANEXO E

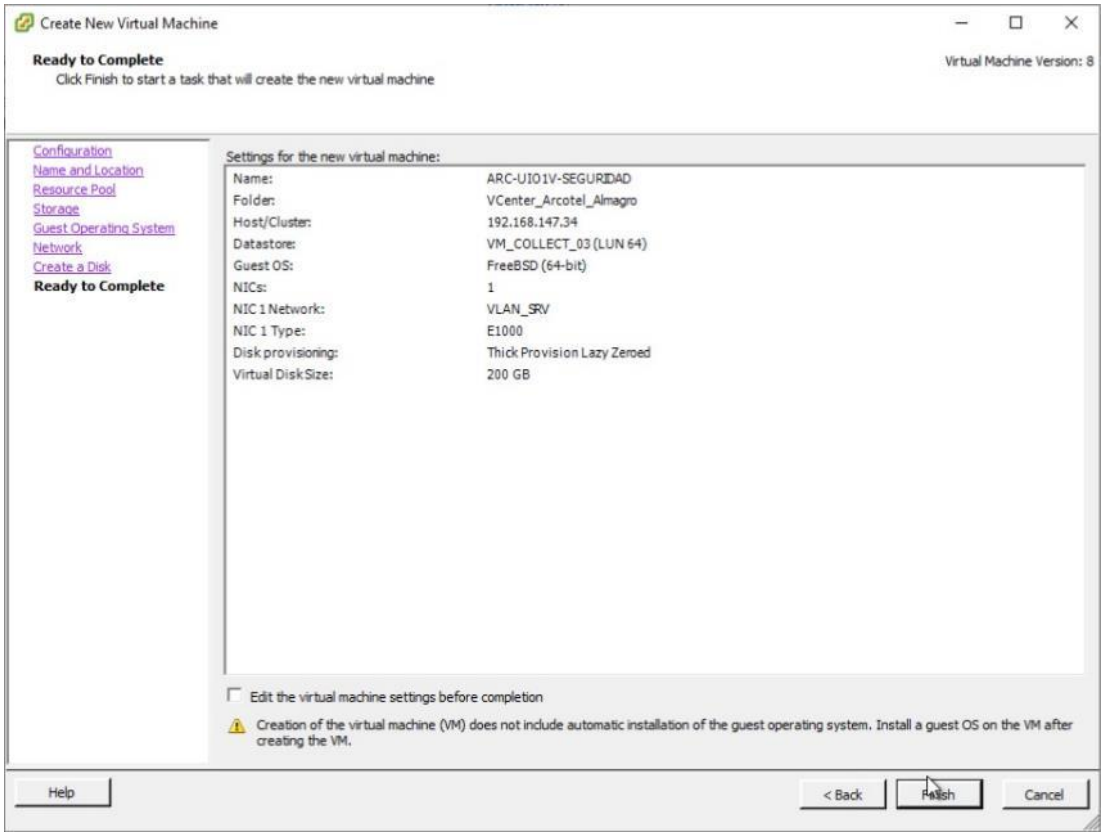
IMPLEMENTACIÓN DEL APPLIANCE

Anexo 23.- Características de la maquina en VMware



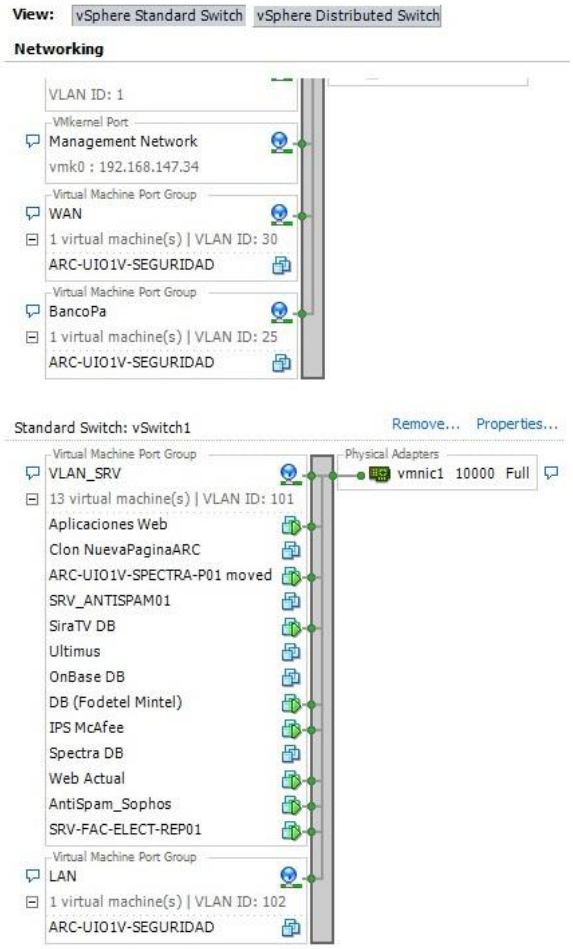
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 24.- Características de la maquina creada



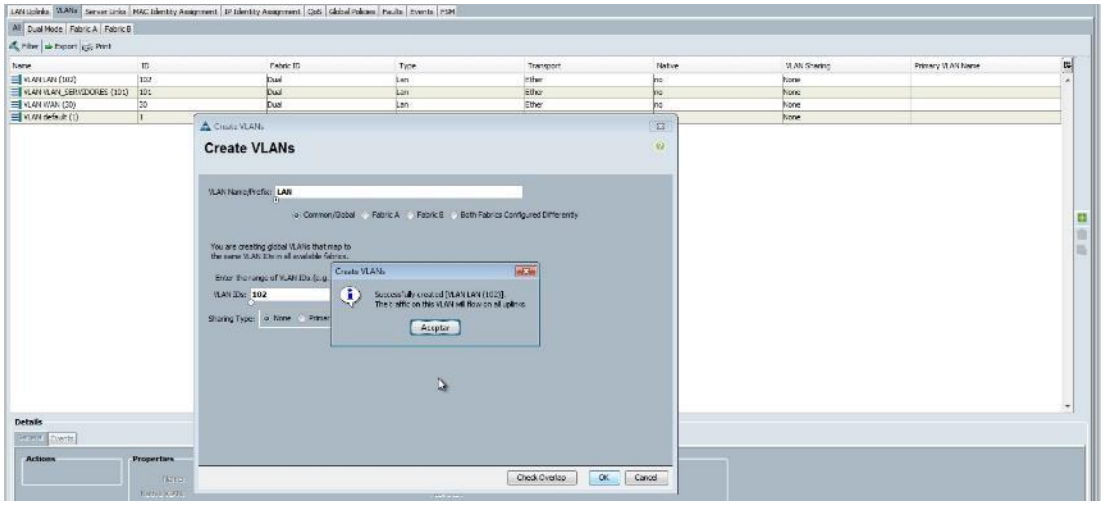
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 25.-Vlans de VMware



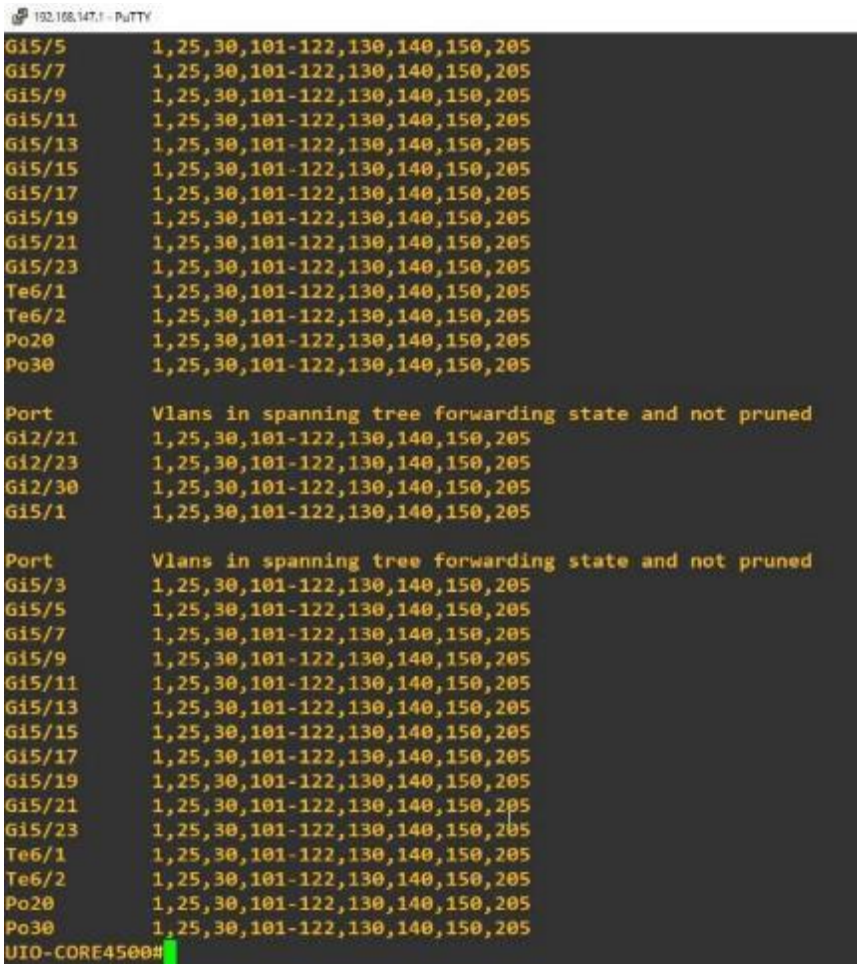
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 26.- Vlans UCS



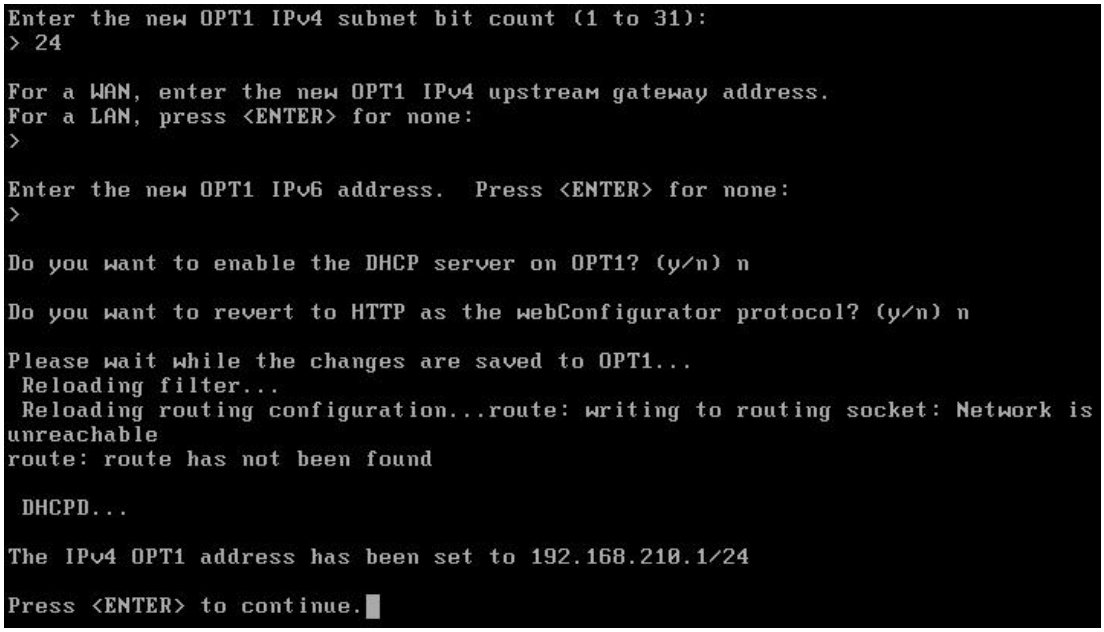
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 27.- Configuración en modo trunk en el SW 4507 de Vlans en VMware y UCS



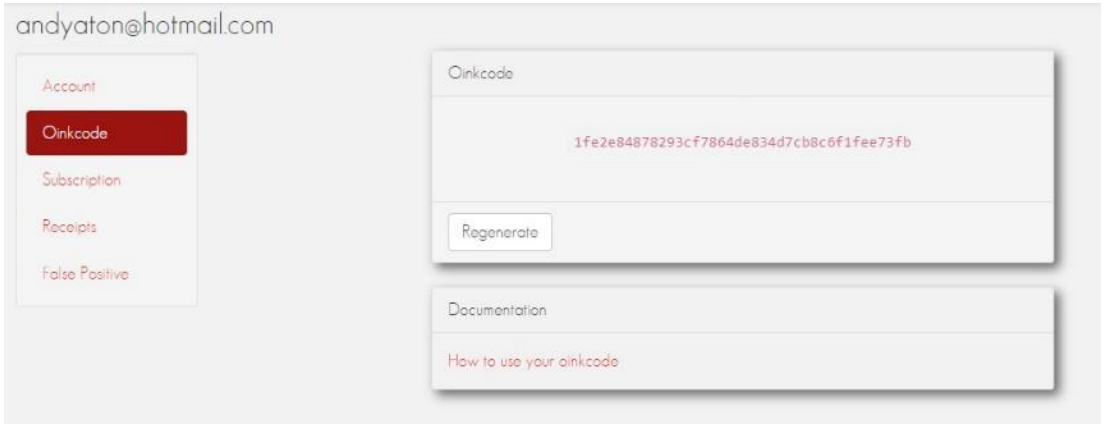
Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 28.- Configuración de la Interfaz Opt1



Elaborado por: Andrés Pérez y Gabriel Pinto

Anexo 29.- Código Oinkcode Snort



Elaborado por: Andrés Pérez y Gabriel Pinto