IMPLEMENTACIÓN DE UN UTM (UNIFIED THREAT MANAGEMENT) PARA LA SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD PONTIFICIA BOLIVARIANA SECCIONAL MONTERÍA

LUIS ENRIQUE MADERA SALGADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MONTERÍA – CÓRDOBA
2017

IMPLEMENTACIÓN DE UN UTM (UNIFIED THREAT MANAGEMENT) PARA LA SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD PONTIFICIA BOLIVARIANA SECCIONAL MONTERÍA

LUIS ENRIQUE MADERA SALGADO

Monografía para optar el título de
Especialista en Seguridad Informática

Asesor
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MONTERÍA – CÓRDOBA
2017

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Montería, 10 de junio de 2017

DEDICATORIA

A Dios. Por darme la salud, bondad y amor para poder lograr mis nuevos logros a nivel profesional y mis objetivos de vida.

A mi esposa Luz Stella, por haberme apoyado en todo momento sacrificando el tiempo que se debe compartir en familia por el dedicado por mí para el estudio por las noches y fines de semana, por su gran apoyo para momentos difíciles y motivación para la culminación de esta especialización.

A mi madre Cenobia que está en los cielos, por darme los valores humanos, disciplina y el amor en mi formación personal y profesional a pesar de las dificultades familiares y económicas.

A Dios. Por darme la salud, bondad y amor para poder lograr mis nuevos logros a nivel profesional y mis objetivos de vida.

A mi esposa Luz Stella, por haberme apoyado en todo momento sacrificando el tiempo que se debe compartir en familia por el dedicado por mí para el estudio por las noches y fines de semana, por su gran apoyo para momentos difíciles y motivación para la culminación de esta especialización.

A mi madre Cenobia que está en los cielos, por darme los valores humanos, disciplina y el amor en mi formación personal y profesional a pesar de las dificultades familiares y económicas.

Luis Enrique.

AGRADECIMIENTOS

Luis Enrique expresa sus agradecimientos a:

Esp. Ing. Freddy Acosta por su importante orientación metodológica en el desarrollo de este proyecto, por su dedicación y apoyo en el proceso de aprendizaje y aportes para la finalización del presente proyecto.

Quiero expresar también mis agradecimientos a mi familia por la comprensión del sacrificio de su tiempo y espacio familiar compartido para desarrollo de mi especialización y poder cumplir mis objetivos de vida planeados.

Al finalizar un trabajo tan arduo y con dificultades en el desarrollo de la tesis de la especialización, debo expresar más que mi mérito el significado que tiene para mí, el gran aporte que haya logrado alcanzar en conocimiento y producto final de solución en seguridad informática para la organización.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

CIBERSEGURIDAD: según lo explicado por Palo Alto Networks[1], la ciberseguridad consiste en proteger los datos y la red del uso de personas no autorizadas.

CRIPTOGRAFIA: **"**La criptografía es el conjunto de técnica y procedimientos que permiten alterar la información de tal forma que no sea posible conocer su contenido, salvo por las personas autorizadas"[2].

DoS: como la define Caballero, Silleros y Shansaifar[3]., es un ataque de denegación de servicios por sus siglas en inglés (Denial of Service); que consiste en ataques para evitar que usuarios legítimos tengan acceso a un sistema o recurso, el ataque se puede dar por diversas maneras como sobrecarga de red, imposibiltar la autenticación de usuario o desconexión de la red electrica de un servidor o base de datos.

DDoS: "El ataque DDoS (distributed Denial of Service, Denegación de servico distribuido), es conceptuaente el mismo ataque anterior, pero proviene de varias máquinas, en ocaciones cientos o miles de ellas"[4].

FIREWALL: es un sistema que protege a un computador o a una red de computadores contra ataques o intrusiones originadas desde Internet u otras redes de terereos. Los firewall se encargan de filtrar los paquetes que se intercambian a través de Internet[5].

IANA: (Internet Assigned Numbers Authority). Entidad autoritativa de asignación de direcciones de Internet o direcciones IP[6].

IDS: de sus siglas en inglés (Intrusion Detection System) sistemas de detección de intrusos. Consiste en la de detección de accesos no autorizados a un computador o sistema informático[7].

IP: protocolo de Internet; encargado del direccionamiento de paquetes a través de las redes de datos, funciona en la capa de red del modelo OSI[8].

---

[1] Palo Alto Networks. Disponible en Internet: https://www.paloaltonetworks.es/products/platforms/firewalls/pa-3000/overview.html

[2] CABALLERO, María; CILLEROS, diego y SHAMSAIFAR, Abtin. El libro del hacker. Madrid. Ediciones Anaya Multimedia. 2015. P. 23-52.

[3] Ibit., p. 29.

[4] Ibit., p. 29.

[5] KIOSKEA.NET. Firewall [en línea]. Junio de 2014. [Consultado 14 de marzo de 2016]. Disponible en Internet: http://es.ccm.net/contents/proteccion-2675306562#590

[6] CABALLERO. Op. Cit., p.63.

[7] Seguridad de la Información. Capitulo8 [en línea]. 2013 [Consultado 13 de mayo de 2016]. Disponible en internet: https://www.segu-info.com.ar/tesis/

[8] CABALLERO. Op. Cit., p. 56.

IPS: “Sistema de Protección de Intrusiones. Son necesarios para redes que incorporan servidores con aplicaciones críticas y deben ser protegidas con filtrado de anti-Spam en correos entrantes”[9].

MALWARE: como la define Caballero, Silleros y Shansaifar[10], software con un proposito malicioso, existen muchas variantes como: gusanos, troyanos, rootkits, spyware, keyloggers, etc.

PHISHING: caballero, Silleros y Shansaifar[11] lo define como el método más simple y rápido de ingeniería social. Es un ataque via correo con páginas web maliciosas, el usuario descarga contenidos que pueden ser algún tipo de malware o correo basura.

POP: como la define Caballero, Silleros y Shansaifar[12], (Post Office Protocol). Protocolo de oficina de correo, se utiliza para descargar los correos a un cliente POP desde un servidor de correos POP remoto.

SPAM: como lo explica Caballero, Silleros y Shansaifar[13], Correo electrónico que se recibe de manera indeseada, o con origen desconocido, normalmente contienen publicidad; pero pueden ser utilizados para obtener información de manera malintencionada.

SSL: como lo explica Caballero, Silleros y Shansaifar[14], (*Secure Sockets Layer.* SSL), protocolo de puerto seguro, utilizado por los navegadores para establecer canales seguros sobre Internet. Las páginas se identifican por HTTPS y se conectan a través del puerto 443 permitiendo comunicaciones de páginas web seguras.

TLS: como lo explica Caballero, Silleros y Shansaifar[15], Protocolo de capa de transporte seguro. (*Transport Layer Security*. TLS), nace a partir del SSL y su área de atención son los protocolos diferentes al HTTP, especialmente los correspondientes al correo electrónico (SMTP, POP, IMAP).

UTM: como lo describe Guerra[16], un UTM (Unified Thread Management), manejo centralizado de amenazas; es un dispositivo de red que realiza las funciones

[9] http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security
[10] CABALLERO. Op. Cit., p. 30.
[11] Ibit., p. 49.
[12] Ibit., p. 72.
[13] Ibit., p. 431.
[14] Ibit., p. 110.
[15] Ibit., p. 110.
[16] GUERRA, Cristian. Implementación de una red segura para los laboratorios del DEEE utilizando un dispositivo UTM [en línea]. Tesis de pregrado. Sangolquí: Escuela Politécnica del ejército. Departamento de Eléctrica y Electrónica, 2011. 149p. 2011. [Consultado 13 de febrero de 2016]. Disponible en Internet:http://repositorio.espe.edu.ec/handle/21000/4741

básicas de filtrado, pero también integra otras funciones como conexiones físicas y lógicas, direccionamiento IP, canales VPN, permisos de navegación, escaneo de antivirus, cifrado de conexiones, escaneo antispyware, anti spam, detección de intrusos (IDS), control a nivel de aplicaciones, la gestión del tráfico, entre otros.

VPN: red privada virtual; se utiliza para conexiones seguras entre empresas a través de Internet[17].

[17] CABALLERO, María; CILLEROS, diego y SHAMSAIFAR, Abtin. El libro del hacker. Madrid. Ediciones Anaya Multimedia. 2015. p. 423.

RESUMEN

El documento plantea la implementación de un UTM de nueva generación, a partir de análisis de tráfico de la red corporativa, pruebas en demostración de amenazas y fallos, análisis de los mejores Firewall UTM de nueva generación y la recomendación de implementación del firewall más adecuado para UPB Seccional Montería. Propone una tecnología para su adquisición e implementación.

Describe la identificación de la infraestructura actual de la red institucional de UPB Seccional Montería y el análisis de vulnerabilidades; evidenciándose las vulnerabilidades sobre todo el tráfico hacia y desde Internet que se cursa sin protección criptográfica, la no existencia de mecanismos de prevención de intrusiones y la falta de rigor técnico para implementar políticas de filtrado de páginas y contenidos Web no seguros y no permitidos, como causa también del problema se evidencia que no se puede hacer un buen monitoreo y buena gestión de la red.

El documento del proyecto propone el rediseño de la topología de Red de la UPB seccional Montería basada en las necesidades de seguridad para implementar una protección robusta en la integración del Firewall UTM de nueva generación perimetral, con el fin de mejorar la seguridad informática y el rendimiento de la red institucional.

Se describe el proceso de implementación de un Firewall UTM (Unified Threat Management) de nueva generación de acuerdo al análisis las diferentes tecnologías y viabilidad económica más adecuada para UPB seccional Montería.

Por último se propone las políticas y reglas de filtrado para el gestor unificado de amenazas, con base en los hallazgos o notificaciones de los reportes generados por el UTM.

1. INTRODUCCIÓN

Según Parraga[18], la seguridad de la información es un aspecto relevante hoy en día en el área de las redes y comunicaciones, por lo cual es importante contar con soluciones integrales que permitan gestionar de manera eficiente las amenazas informáticas que tratan de comprometer la disponibilidad de los servicios o lucrarse con información confidencial. Para utilizar los servicios Web exige la implementación de una infraestructura segura de conectividad que mitigue los riesgos y posibles ataques debido a las vulnerabilidades que se pueden presentar en materia de seguridad de la información.

Según Palo Alto Networks[19], líder en seguridad según el cuadrante de Gartner. Un Firewall unificado y de última generación es el componente de seguridad más estratégico para la implementación de políticas de seguridad, debido a que todo el tráfico de la red pasa por él por lo que se puede hacer control del tráfico de la red, prevención de ataques no solo a nivel de puertos de la red sino también a nivel de usuarios y aplicativos.

Los ataques de denegación de servicios (DoS), de inyección de código SQL a servidores de Bases de Datos vulnerables, que ponen en riesgo la confidencialidad de la información, entre otros; es posible tomar el control de servidores y el robo de información sensible y de gran valor para la institución, usuarios y clientes. Por ejemplo el robo de contraseñas.

Por las razones anteriores y las de dar un manejo seguro a la información como activo importante y de gran valor de la institución, la universidad Pontificia Bolivariana Seccional Montería se encuentra en la necesidad tecnológica de proteger todo su sistema información que pasa por su red Institucional y de Internet. Para ello la UPB Seccional Montería, preocupada por la seguridad de la red institucional, busca implementar controles y políticas de seguridad que minimicen los riesgos de pérdida de la confidencialidad, integridad y disponibilidad de la información.

[18] PARRAGA NÚÑEZ, Víctor. Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de ingeniería de sistemas computacionales. Tesis de pregrado [en línea]. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas, 2014. 259p. Dic. 2014. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://repositorio.ug.edu.ec/bitstream/redug/6672/1/TesisCompleta-536-2014.pdf.

[19] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

Por consiguiente, se propone implementar un gestor unificado de amenazas (UTM); aplicando las mejores prácticas y estándares de seguridad, que permitan una administración fácil y centralizada, a través de un gestor unificado de amenazas (UTM). Con su implementación se busca garantizar a usuarios, clientes y proveedores la confidencialidad, integridad, la disponibilidad de la información, la confiabilidad y prestigio institucional.

2. FORMULACIÓN DEL PROBLEMA

2.1 TÍTULO DESCRIPTIVO DEL PROYECTO

IMPLEMENTACIÓN DE UN UTM (UNIFIED THREAT MANAGEMENT) PARA LA SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD PONTIFICIA BOLIVARIANA SECCIONAL MONTERÍA

2.2 CAUSAS DEL PROBLEMA

Se entiende como causa principal de las vulnerabilidades de la red corporativa cableada e inalámbrica de la Universidad Pontificia Bolivariana Seccional Montería los siguientes factores:

Todo el tráfico hacia y desde Internet pasa sin protección criptográfica, no existen mecanismos de prevención de intrusiones y falta rigor técnico para implementar políticas de filtrado de páginas y contenidos Web no seguros y no permitidos.

Con la tecnología utilizada actualmente no se puede hacer monitoreo y realizar las métricas necesarias para la buena gestión de tráfico de la red que permita hacer un uso del ancho de banda de manera eficiente y hacer balanceo de tráfico por diferentes operadores de Internet para garantizar la disponibilidad del servicio.

Con el Firewall por software no se puede hacer una buena gestión unificada de amenazas para proteger de manera más eficiente todo el tráfico de la red. La infraestructura de proxy/firewall por software implementado en cada VLAN corporativa puede ser causa de fallas de seguridad por la complejidad de la administración. Además se presentan bloqueos de tráfico cuando se supera el ancho de banda dedicado instalado, debido a la falta de control de tráfico y capacidad de manejo del hardware donde corre el Firewall.

La falta de una buena gestión de reportes de alarmas o incidentes de red y de prevención de intrusiones es causa de problemas de seguridad que afectan la confidencialidad, la integridad y la disponibilidad de la información.

2.3 CONSECUENCIAS DEL PROBLEMA

La falta de la gestión unificada de amenazas (UTM) de la Universidad Pontificia Bolivariana Seccional Montería puede traer consecuencias como pérdida en la confidencialidad, integridad y disponibilidad de los datos relacionados con todos los procesos administrativos y académicos que se llevan a cabo en la institución, como la fuga de datos de usuarios, que puede ser aprovechada por los accesos no autorizado en la red cableada e inalámbrica a falta de cifrado de las conexiones a Internet, inyección de malware como virus, gusanos, troyanos, spyware, entre otros. Todo lo anterior puede ocasionar problemas como ralentización del sistema, espionaje, ataques de Denegación de Servicios, intercepción de tráfico, entre otros.

Se presenta consumo de ancho de banda inadecuado; debido a que no hay un buen control de tráfico de la red, filtrado Web, virus, spam y control de contenidos. Como consecuencia se afectan los servicios corporativos web por lentitud del sistema. También se presentan interrupciones del servicio por saturaciones de tráfico del servidor Proxy/Firewall, bajo rendimiento del canal o ancho de banda por falta de control centralizado y la falta de medidas preventivas de manera eficiente.

Por lo anterior se hace necesario la implementación de un Firewall de última generación para el manejo unificado de amenazas, control de tráfico y gestión de servicios, aplicativos web y usuarios.

3. JUSTIFICACIÓN

La Universidad Pontificia Bolivariana Seccional Montería cuenta con una Red Institucional (LAN, WiFi, Intranet e Internet); pero el rendimiento de la red se ha venido afectando por falta de controles de filtrados, manejos de contenidos y accesos no autorizados. Actualmente se hace una defensa proactiva de seguridad informática, no preventiva lo que puede dejar en riesgo a la institución educativa de sufrir pérdidas o fugas de información sensible. La infraestructura que se tiene actualmente con diferentes firewall lógicos en diferentes máquinas servidoras, complican la gestión y administración de la seguridad de la red. Adicionalmente, el crecimiento de la red y los servicios ofrecidos por Internet hacen más complejas las labores de monitoreo y prevención de ataques de seguridad. Actualmente no se realiza un buen control de tráfico por el funcionamiento de firewall separados en diferentes VLAN (Administrativa, Académica e Inalámbrica), lo que dificulta una buena administración de seguridad de la Red. Por lo tanto se hace necesario la implementación de firewall robusto y de manejo centralizado que proteja toda la red y los Sistemas de Información de UPB Montería contra amenazas, protección de datos personales y continuidad del negocio. De todo lo anterior surge el siguiente interrogante:

¿Por qué y cual tecnología de Firewall de nueva generación se debe implementar para protección de la red institucional de UPB Montería?

La implementación de un Firewall perimetral de nueva generación UTM garantizará una mejor gestión de seguridad informática de manera centralizada; esto mitigará las vulnerabilidades de seguridad presentes actualmente. El UTM incluye funcionalidades de Firewall, filtrado de navegación Web, protección antivirus, administración de ancho de banda, sistemas de prevención de intrusos, entre otras funcionalidades que ayudarán a fortalecer la seguridad del tráfico de red entrante y saliente, garantizando la confidencialidad, integridad y disponibilidad de la información.

4. OBJETIVOS GENERAL

Implementar un Firewall de nueva generación UTM (Unified Threat Management) que provea los servicios de seguridad informática perimetral para la red corporativa de la Universidad Pontificia Bolivariana Seccional Montería.

4.1 OBJETIVOS ESPECÍFICOS

- Identificar la infraestructura de la red institucional de UPB Seccional Montería y la seguridad de la red mediante la recolección de información, para luego del análisis de los posibles fallos o vulnerabilidades establecer las mejoras que se deban hacer para integrar el UTM.

- Rediseñar el modelo de la topología de Red de la UPB Seccional Montería basada en las necesidades de seguridad para implementar una protección robusta en la integración del Firewall UTM perimetral, con el fin de mejorar la seguridad informática y el rendimiento de la red institucional.

- Analizar las diferentes tecnologías UTM, para implementar la más adecuada y viable para los recursos y requerimientos de seguridad de la UPB Seccional Montería.

- Implementar un Firewall UTM (Unified Threat Management) de nueva generación según análisis de la tecnología y viabilidad económica más adecuada para UPB, para mejorar la funcionalidad y seguridad de la red institucional en la Universidad Pontificia Bolivariana Seccional Montería.

- Afinar las políticas y reglas de filtrado propuestas para el gestor unificado de amenazas, en base a los hallazgos o notificaciones de los reportes generados por el UTM en pruebas para garantizar la seguridad en la red de manera continua.

5. ALCANCES Y LIMITACIONES

5.1 ALCANCES

El proyecto en desarrollo tiene como alcance la identificación de la infraestructura de red actual, el rediseño de esta de acuerdo a las necesidades y medidas de seguridad, análisis de las diferentes tecnologías de Firewall UTM de nueva generación, dimensionar los recursos de hardware necesarios pata la nueva tecnología e implementación de un Firewall de nueva generación en la Universidad Pontificia Bolivariana Seccional Montería ubicada en el campus principal de la ciudad de Montería.

Los aspectos de estudio comprenden el análisis de la tecnología adecuada UTM de nueva generación necesaria para cumplir con los requerimientos de seguridad informática de UPB Montería, teniendo en cuenta políticas de seguridad, el tráfico de la red, manejo de puertos, control de aplicativos, perfiles de usuarios y la factibilidad económica para su implementación.

5.2 LIMITACIONES

La UPB seccional montería no cuenta con el recurso humano suficiente y preparado para el soporte de alto nivel para la tecnología de firewall UTM de nueva generación que se recomiende de este estudio para su implementación. Por lo tanto en su implementación debe incluirse el soporte técnico de alto nivel suministrado por el fabricante.

El personal de soporte técnico especializado en seguridad informática de UPB Montería hará la administración, gestión y soporte técnico de primer nivel.

6. MARCO REFERENCIAL

6.1. ESTADO DEL ARTE

Consultando diferentes trabajos relacionados con la propuesta planteada, se tomaron algunos artículos y trabajos de grado que proponen soluciones a temáticas similares a las del proyecto, como se citan a continuación.

Según Parraga[20], la seguridad de la información es un aspecto relevante hoy en día en el área de las redes y comunicaciones, por lo cual es importante contar con soluciones integrales que permitan gestionar de manera eficiente las amenazas informáticas que tratan de comprometer la disponibilidad de los servicios o lucrarse con información confidencial. Este proyecto de tesis tiene como objetivo primordial implementar una solución tecnológica que permita la gestión unificada de amenazas de seguridad basado en la modalidad de investigación de proyecto factible ya que el mismo quedará funcionando al cien por ciento operativo previo una reingeniería de las estructura de red en la carrera. Los gestores unificados de amenazas o UTM van más allá del concepto de los firewalls ya que en sí engloba varios servicios de red en una sola plataforma, tales como VPN, DNS, IPS, WAF, etc. Para este estudio se utilizó la modalidad de investigación cualitativa y cuantitativa, realizando encuestas a los estudiantes docentes y personal administrativo, acogiendo también la opinión emitida por un experto en el área de seguridad y redes al cual se entrevistó. Con esta propuesta se busca disminuir el impacto que puedan causar las amenazas de seguridad, facilidad de administración y configuración, y reportes oportunos que permitan la toma acertadas de decisiones al administrador de la red, con lo cual resulta beneficiada toda la comunidad educativa.

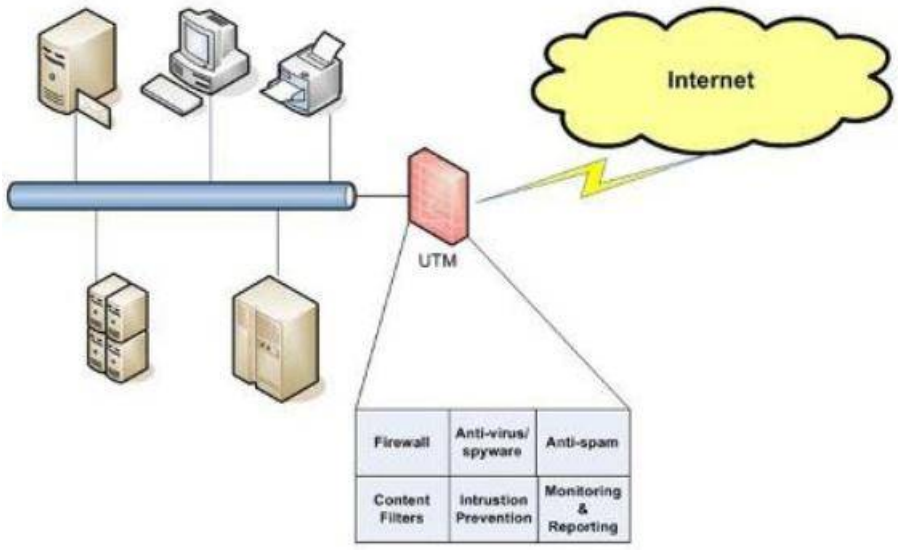
6.1.1 Similitud con el Problema Identificado[21]. La estructura de seguridad actual que tiene la red administrativa, permite todavía accesos de navegación no autorizados, penetraciones a la red, consumos no supervisados de ancho de banda y muchas debilidades expuestas que afectan la confidencialidad, integridad y disponibilidad de los datos, los intentos de intromisión por parte de las subredes de los laboratorios incrementa la posibilidad y probabilidad de ataques internos y contaminación de malware.

[20] PARRAGA NÚÑEZ, Víctor. Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de ingeniería de sistemas computacionales. Tesis de pregrado [en línea]. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas, 2014. 259p. Dic. 2014. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://repositorio.ug.edu.ec/bitstream/redug/6672/1/TesisCompleta-536-2014.pdf.

[21] Ibíd., p. 10-11

6.1.2 Solución dada al Caso[22]: según Parraga, la solución ofrecida por la Universidad de Guayaquil, se basa fundamentalmente en la implementación una solución integral tecnológica que permita la gestión unificada de amenazas de seguridad informática, en la estructura de red de la CISC, aplicando criterios basados en mejores prácticas de seguridad para proteger de manera centralizada el equipamiento lógico de la institución a nivel interno y perimetral asegurando la continuidad y operatividad de los servicios informáticos que son consumidos por la comunidad académica, y a su vez brindar al administrador de red facilidad de gestión e inmediata respuesta, frente a problemas o eventualidades presentados en la red. El problema de la Universidad de Guayaquil es muy semejante al de la Universidad Pontificia Bolivariana Seccional Montería frente a los problemas de vulnerabilidad presentados en la red, la necesidad de una gestión unificada de amenazas, es decir, la implementación de un UTM como solución tecnológica integral que permita mitigar los riesgos referentes a la seguridad informática. En la Figura 1 se representa el esquema de un Gestor Unificado de Amenazas (UTM).

Figura 1. Gestor Unificado de Amenazas en una Red



Fuente: Tesis de grado. Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/6672/1/TesisCompleta-536-2014.pdf

6.1.3 Evolución tecnológica de UTM. Los UTM han evolucionado en firewall de nueva generación, mejorando las funcionalidades integradas en un solo dispositivo,

[22] Ibíd., p. 52

el cual se conoce como UTM de nueva generación o Firewall de nueva generación, que puede funcionar por hardware con sistema operativo embebido en el dispositivo y que se conoce como Appliance, puede funcionar en versiones de software especialmente para ser instalado en servicios virtualizados o máquinas virtuales y también a nivel de alojamiento de dispositivos por hardware o software en la nube. Como explica Palo Alto Networks[23], la seguridad tradicional basada en puertos y en infraestructura de la red presenta vulnerabilidades dado el crecimiento de las aplicaciones móviles de usuarios. Contenidos web y los mismos servicios virtualizados que se ofrecen a nivel empresarial. Los riesgos que se pueden presentar a nivel empresarial pueden superarse con la incorporación de medidas de prevención no solo basadas en puertos, sino también en control de perfiles de usuarios y control de uso de aplicaciones y contenidos. Los Firewall UTM de nueva generación permiten una seguridad perimetral empresarial con políticas que se aplican en torno al control de aplicaciones, usuarios y protección de contenidos habilitados. Es decir plantea habilitar de forma segura las aplicaciones, usuarios y contenidos mediante la clasificación del tráfico, el objetivo empresarial y la aplicación de las políticas de seguridad para permitir o proteger el acceso a aplicaciones de uso institucional, evitar amenazas eliminando aplicaciones no deseadas y aplicando políticas selectivas para el bloqueo de explotación de vulnerabilidades, virus, spyware, botnets y malware desconocidos. Proteger los centros de datos por medio de la validación de aplicaciones, proteger los entornos virtualizados aplicando las mismas políticas de seguridad perimetral, extender las medidas de seguridad a la informática móvil, sus usuarios y dispositivos independientemente de su ubicación.

6.2. MARCO TEÓRICO

6.2.1 Redes TCP/IP. García[24] expresa que, las redes TCP/IP nacen en la década de los 60 como un proyecto auspiciado por la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos (DARPA); como medida preventiva contra ataques a las redes de Telecomunicaciones de los Estados Unidos debidos en época de la guerra fría. Para ello, DARPA financia la investigación delegando a diferentes universidades para el desarrollo de una red distribuida de computadores como solución a las telecomunicaciones en situación de guerra.

Como resultado a nivel experimental se obtuvo la red ARPANET; que es una red de conmutación de paquetes desarrollada a mediados de los años 70. En 1974

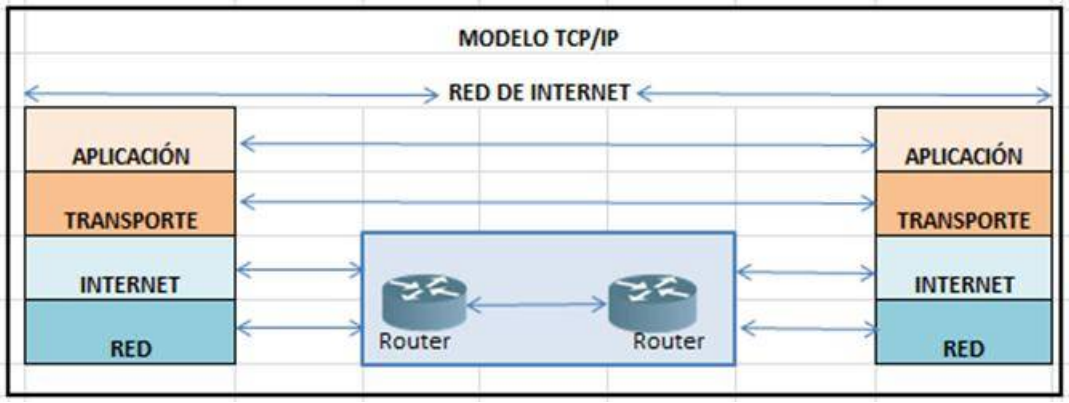
[23] Palo Alto Networks. Resumen de cortafuegos de nueva generación [en línea]. Mayo de 2016. [Consultado 17 de mayo de 2016]. Disponible en Internet: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-features-overview-es.pdf.

[24] HERRERA, Jordi, GARCÍA, Joaquín, PERRAMÓN, Xavier. Aspectos avanzados de seguridad en redes. Ataques contra redes TCP/IP. Barcelona. Universidad Abierta de Cataluña, 2004, p.5

evoluciona en la familia de protocolos que utilizamos y conocemos hoy en día como redes TCP/IP.

El conjunto de protocolos TCP/IP se representa en cuatro capas según sus funciones, a diferencia del modelo OSI (Open System Interconnection) de siete capas creado en 1980 por la Organización Internacional de Normalización o ISO (International Organization for Standardization); en el modelo TCP/IP las capas de aplicación, presentación y sesión del modelo OSI se representa en una sola capa llamada Aplicación y la capa física y enlace de datos del modelo OSI, se representa en una sola capa llamada de Red en el modelo TCP/IP. (Ver Figura 2).

Figura 2. Modelo TCP/IP de Internet



Fuente: El autor.

La capa de Acceso a Red integra las funciones de capa física y de enlace de datos del modelo OSI. Toda interconexión LAN y WAN utiliza esta capa para su direccionamiento físico con las direcciones MAC (Media Access Control) a través de los diferentes medios de transmisión por cable, fibra óptica, inalámbrica o microondas. En esta capa se encapsulan los datos de capas superiores como TCP e IP en lo que se llama trama Ethernet.

La capa de Internet permite la interconexión de la Red mediante direccionamiento lógico o direcciones del Protocolo de Internet IPv4 o IPv6. Permite la interconexión de redes a través de dispositivos de capa 3 o de Internet como los enrutadores o Switches con funciones de capa 3.

La capa de Transporte se encarga de darle fiabilidad a la conexiones de Internet, mediante los protocolos TCP (Protocolo de Control de Transmisiones); llevando un control de los segmentos o datagramas TCP. TCP realiza control de secuencias de

envíos o control de flujos, acuses de recibos de segmentos de datos y tamaños de ventanas de transmisión simultánea de segmentos de datos entre hosts. Todas estas funcionalidades hacen fiables las conexiones de Internet y suplen las funciones que no tiene el protocolo IP en el direccionamiento de capa 3. En la capa de transporte también funciona el protocolo UDP de cabecera más sencilla comparada con la de TCP, UDP es utilizado para transmisiones de datos en tiempo real por tener una cabecera más sencilla, ejemplo en videoconferencias; UDP no realiza retransmisión de datos en caso de pérdida de un datagrama.

La capa de Aplicación aloja todas las aplicaciones que ofrecen servicios por Internet, como son: Servicios Web mediante el protocolo http o https, servicios de correo electrónico, transferencias de archivos, servicios de resolución de nombres, entre otros. Esta capa es utilizada por servidores, computadores o equipos terminales de la red.

En resumen, como se muestra en la Figura 2, es que en la capa de aplicación se realizan las comunicaciones entre dos programas. La capa de transporte realiza las funciones de cómo se realiza la comunicación entre los dos programas haciendo uso de *puertos de servicios* o números estandarizados que identifican un servicio. La capa de red o de Internet realiza el transporte de esta comunicación entre dos equipos terminales identificados por su dirección IP asignada a sus interfaces de red. La capa de Acceso a Red se encarga de transportar la información de cada equipo a través del medio de transmisión, mediante tramas Ethernet que utilizan direcciones MAC que corresponde a la interfaz de cada dispositivo conectado a la red.

6.2.2 Puertos de servicios Web. De acuerdo como los define Ziegler[25], “Los servicios basados en red son programas que se ejecutan en una máquina a los que pueden acceder otros equipos de la red”, es decir, cada programa o servicios de red están identificados por un puerto en el modelo de Internet TCP/IP. Los puertos principales son bien conocidos y cubren el rango desde 1 a 1023. Estos puertos son asignados y coordinados por la autoridad de asignación de números de Internet (IANA, *Internet Assigned Numbers Authority*).
Los puertos de este rango inferior son llamados puertos privilegiados, son usados por programas con niveles de privilegios asignados por el Sistema Operativo, es decir tienen un nivel de root o súper usuario. Por lo tanto, se debe hacer una buena administración de los puertos abriendo solo los necesarios para los servicios Web ofrecidos.

Los servicios Web son anunciados a través de los puertos. Por ejemplo, si un servidor ofrece los servicios Web, este debe tener abierto el puerto 80 definido para http. Es decir, si una máquina se conecta al servidor asociado con el servicio Web, el servidor le va a dar respuesta a la solicitud realizada por la máquina de un usuario

[25] ZIEGLER, Robert. Guía avanzada Firewall Linux. Madrid: Prentice Hall. Iberia, 2000. p.6.

a través de la conexión al puerto 80. Por el contrario si el servidor no tiene abierto el puerto 80, el programa del cliente que hace la solicitud a este, va a recibir un error indicándole que el servicio no está disponible. Adicionalmente los puertos superiores, desde 1024 a 65.535 son puestos no privilegiados y son usados con doble propósito para la asignación dinámica de las conexiones entre máquinas clientes y servidor. Además los puertos de 1024 a 49.151 son registrados por la IANA y son asociados también a servicios particulares como SOCKS o servidor proxy especial; cuya función es permitir accesos a servicios Web en un puerto especial, por ejemplo 1080, también puede ofrecer otros servicios como clientes de mensajerías instantánea, transferencias de archivos, entre otros.

En la Tabla 1, se muestra un resumen de los puertos más conocidos y registrados por la IANA. Estos puertos son normalmente habilitados dependiendo de los servicios ofrecidos por un servidor. Es de aclarar que el uso de algunos puertos, como el 23 de Telnet podría traer problemas de seguridad dado que no usa cifrado en las sesiones de usuario y contraseña. De igual forma es necesario conocer que puertos manejan ciertos niveles de seguridad o no y así evitar vulnerabilidades que pueden poner en riesgo la seguridad de la red.

Tabla 1. Puerto TCP/UDP

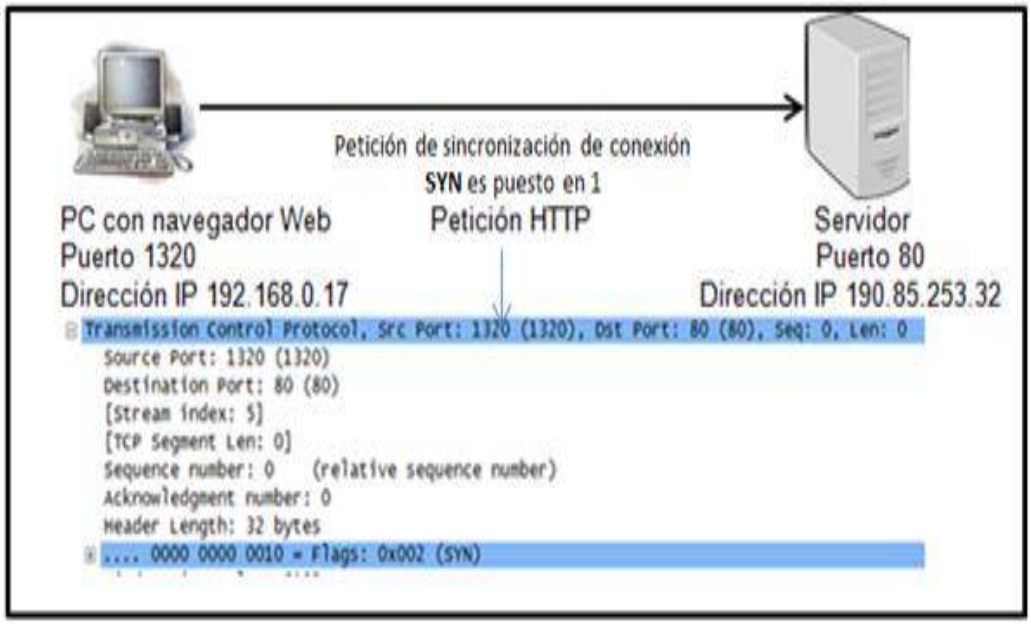
PUERTO	TCP o UDP	NOMBRE DEL PROTOCOLO	NOMBRE DEL SERVICIO
20	TCP	Protocolo de transferencia de archivos (FTP)	ftp-data
21	TCP	Control de FTP	ftp
22	TCP	Shell segura (SSH)	ssh
23	TCP	Telnet	telnet
25	TCP	Protocolo simple de transferencia de correo (SMTP)	smtp
53	TCP/UDP	Sistema de nombres de dominio (DNS)	domain
80	TCP	Protocolo de transferencia de hipertexto (HTTP)	http
110	TCP	Protocolo de oficina de correos (POP3)	pop3
115	TCP	Protocolo simple de transferencia de archivos (SFTP)	sftp
143	TCP	Protocolo de acceso a mensajes de Internet (IMAP)	imap
443	TCP	Secure Sockets Layer (SSL o “HTTPS”)	https
993	TCP	Mail IMAP4 sobre SSL	imaps
995	TCP/UDP	Mail POP3 sobre SSL	pop3s

Fuente: https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puerto

6.2.3 Conexiones TCP. Las conexiones TCP se establecen pasando por tres estados; en conexiones típicas un servidor Web escucha o espera peticiones de conexión sobre el puerto 80 de TCP para este servicio. Un usuario a través de su navegador web hace clic en el enlace o vínculo de una unidad de recursos URL,

este nombre de host y servicio se traduce en una dirección IP correspondiente al servidor Web, además se asigna un puerto de los no privilegiado del navegador para iniciar la conexión. Se crea un mensaje HTTP para enviar al servidor Web, este mensaje es encapsulado en el datagrama TCP con una petición SYN y luego este es encapsulado en el paquete IP; este paquete IP es enviado hacia su destino a través de la LAN o de la WAN. (Ver Figura 3).

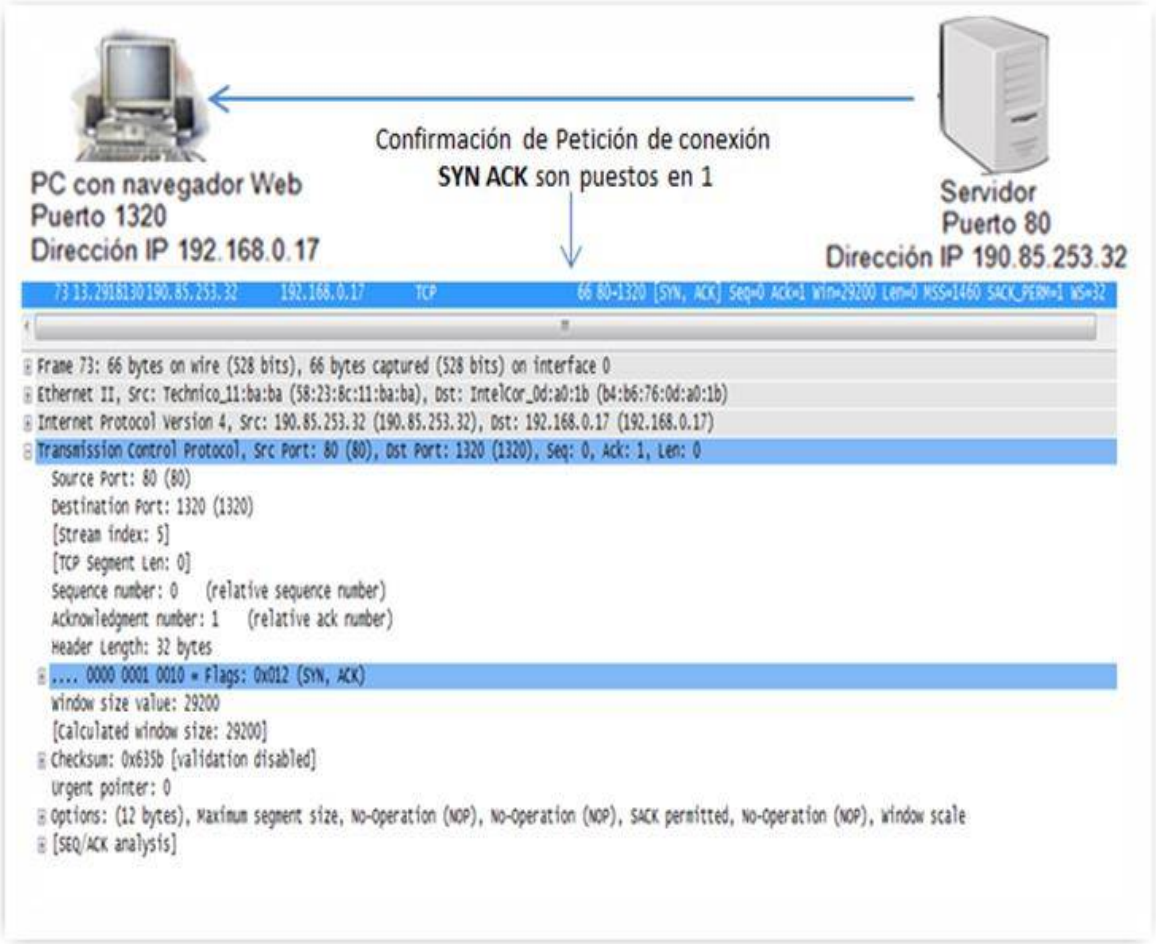
Figura 3. Petición de conexión



Fuente: el Autor.

El servidor recibe el paquete con el indicador de petición de conexión SYN puesto en 1 y ademas recibe el número de secuencia inicial del PC cliente como base de cotrol de secuencia de sus mensajes. El servidor al escuchar por el puerto 80 esa solicitud, asigna un nuevo socket a su IP 190.85.253.32 y lo asocia con el socket del cliente, es decir, asocia el puerto 80 al puerto 1320 del cliente con su respectiva dirección IP. El servidor Web responde la petición con una confirmación SYN ACK, inrementando el número de secuencia del cliente en uno; esto le indicará al cliente que el servidor recibió el mensaje enviado anteriormente, además el servidor indica al cliente que ese mensaje + 1 es el próximo mensaje que espera recibir. Del mismo modo el servidor envía la sincronización con el indicador SYN puesto en uno y su propio número de secuencia como base a seguir. (Ver Figura 4).

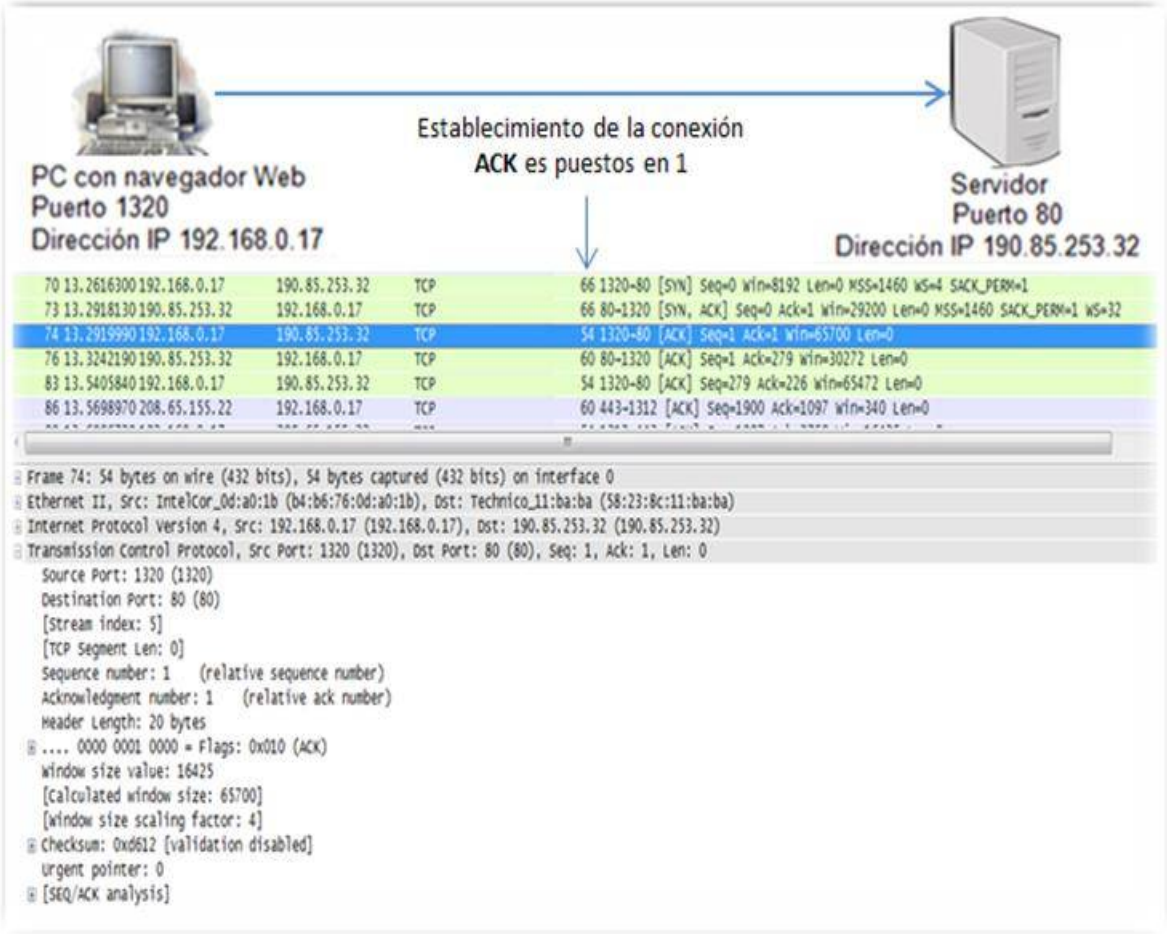
Figura 4. Confirmación de conexión TCP



Fuente: el Autor.

El servidor despues de este mensaje no vuelve a enviar el SYN activado. A partir de aquí todos los mensajes tendran solo activo el bit de ACK. El cliente recibe este mensaje y responde confirmando con su ACK puesto en uno y queda establecida la conexión. Todos los mensajes de aquí en adelante solo tendrán activo el bit ACK, con las secuencias correspondientes de la máquina cliente y servidor, y los sockets establecidos para los puertos 80 y 1320 para este caso de ejemplo, que para detallarlo me he valido de la herramienta Wireshark para monitorear los paquetes. (Ver Figura 5).

Figura 5. Establecimiento de la conexión TCP



Fuente: el Autor.

6.2.4 Vulnerabilidades de la red. Como plantea Jordi Herrera[26], las siguientes son las vulnerabilidades más comunes de las distintas capas:

Vulnerabilidades de la capa de red. Estas vulnerabilidades se presentan sobre el medio de conexión. Los fallos de seguridad son de control de acceso y de confidencialidad. Ejemplos de este nivel son interceptación intrusiva, escuchas no intrusivas en medios de transmisión inalámbricas, etc.

Vulnerabilidad de la capa de Internet. En esta capa son posibles los ataques que afectan los paquetes IP. Como las técnicas de *Sniffing,* la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes.

[26] HERRERA, Jordi; GARCÍA, Joaquín; PERRAMÓN, Xavier. (2004). Aspectos avanzados de seguridad en redes. Ataques contra redes TCP/IP. Barcelona. Universidad Abierta de Cataluña, p.17

Vulnerabilidad de la capa de Transporte. Se ven comprometidos los datagramas IP que llevan información TCP o UDP. Los fallos de seguridad presentados aquí son de problemas de autenticación, de integridad y de confidencialidad. Uno de los ataques más conocidos es el de las denegaciones de servicio debidas a protocolos de transporte.

Vulnerabilidades de la capa de Aplicación. Se presenta fallas de seguridad asociadas a los diferentes protocolos de capas superiores. Se presenta una gran variedad de ataques a este nivel, debido al gran número de protocolos pertenecientes a esta capa. Algunos ejemplos de deficiencias de seguridad a este nivel son: en servicios de nombres de dominio, en Telnet, en FTP, http, entre otros.

6.2.5 Explotando la vulnerabilidad. Una de los programas utilizados para explotar la vulnerabilidad de un sistema o programa informático, es el exploit. Como lo explica García, Fernandez, Martinez y otros. "Un exploit es un programa diseñado para aprovechar la vulnerabilidad, fallo o error de un programa, con el objetivo de ejecutar un código o programa en la máquina atacada para conseguir el dominio de la misma" [27].

Un exploit puede llegar a conseguir los siguientes objetivos de ataques:

- Deshabilitar un servicio ofrecido por un servidor como por ejemplo un antivirus, el firewall o cualquier otro aplicativo web.
- Denegación de servicios (DoS).
- Conseguir el control de la máquina atacada por medio de la consola del sistema operativo de la máquina.
- Abrir una puerta trasera de un sistema operativo o informático para tener la posibilidad de un futuro ataque por esta.
- Crear una cuenta de usuario con privilegios para validarse de manera que no se despierte sospecha de validación de usuario en un sistema, entre otros objetivos de ataque.

Como explica García, Fernández, Martínez y otros[28] Los exploits pueden ser de tipo local o remoto. En el caso de los locales el ataque se realiza sobre una máquina de manera local por un usuario con privilegios restringidos con la posibilidad de mejorar sus privilegios hasta tener el de administrador; normalmente el objetivo de este ataque local es el de denegación de servicios DoS o tumbar un servicio Web. A diferencia del anterior el exploit remoto se realiza aprovechando una vulnerabilidad de un sistema remoto de servicios Web, correo electrónico, servicio FTP, entre otros.

[27] García, Jean; Fernández, *et al*. Hacking y seguridad en internet. Bogotá: Ediciones de la U. 2013. p. 112.
[28] Ibit., p. 115.

Según García, Fernández, Martínez y otros[29], la manera como se realicen estos ataques a través de exploit, pueden ser de tres tipos:

- **Ataques a través de páginas Web**; que son páginas web maliciosas con script generalmente escritos en Javascript que permite por error de código explotar un navegador web y aprovechar esta vulnerabilidad para inyectar software espía o maliciosa.

- **Ataque a un servicio que corre en un puerto**; consiste en enviar paquetes shellcode a través del o los puertos donde corre un servicio web y provocar un error en la maquina atacada. Este ataque puede también generar denegación de servicios a través de envíos masivos de paquetes de gran tamaño.

- **Ataque de inyección SQL**; consiste en atacar las bases de de datos a través de aplicaciones Web vulnerables, el ataque por medio de este exploit puede conseguir modificar o alterar o copiar una base de datos inyectando instrucciones maliciosas a la misma. Se puede conseguir también atacar el sistema operativo del sistema atacado.

6.2.6 Seguridad informática. "Según la ISO 27001, la seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización."[30]. Es decir, un sistema informático es confiable si cumple con las premisas de seguridad de: disponibilidad, confidencialidad e integridad de la información. La disponibilidad de un sistema de información es el acceso que se tiene a la información cuando se requiera y por el personal autorizado. La confidencialidad garantiza que solo la persona o personas autorizadas tienen accesos a ella. La integridad garantiza la calidad de los datos, es decir que los datos no han sufrido modificación sin permiso o pérdida de información. En la práctica es imposible tener un sistema completamente seguro, por tanto el objetivo es alcanzar un sistema confiable.

Las vulnerabilidades de seguridad que se pueden presentar se debe a varios factores como son: Código maliciosos como son los ataques de virus y habilitación de puertas traseras, atacantes internos que provienen de usuarios autorizados; vulnerabilidades en el equipamiento, por ejemplo, accesos no permitidos y errores de usuarios, fallas en la gestión de la seguridad de la empresa. Estos ataques tienen como objetivo romper con la confidencialidad, para luego conseguir el resto de la información.

[29] Ibit., p. 116.
[30] ISO 27000.ES:2013. El portal de ISO 27001 en español. [en línea]. 2013. [Consultado 14 de mayo de 2016]. Disponible en Internet: http://www.iso27000.es/sgsi.html.

Según como lo plantea Loinaz, Cortiñas y Ezeiza[31], las políticas de seguridad de un sistema informático están basadas en tres mecanismos: prevención, detección y recuperación.

6.2.7 La prevención. La prevención es el primer nivel de protección contra ataques dirigidos a la red. El sistema cortafuegos o firewall, es un mecanismo de control de acceso sobre la capa de red, actúa como una barrera central a los servicios que se ejecutan internamente y externamente de la red. Los cortafuegos suelen ser muchas veces computadores dedicados únicamente al control del tráfico.

Existen cortafuegos basados en Linux a través de la herramienta IPtables, también existen los de tipo hardware con software embebido con funcionalidades integradas de última generación y con una mayor prestación de manejo de tráfico y gestión unificada de amenazas como son los UTM.

6.2.8 Protecciones. Son las acciones que pueda realizarse para mantener la disponibilidad, la confidencialidad y la integridad de la información, es decir, son las protecciones para no permitir la vulneración del sistema de información.

Las protecciones se realizan en tres instancias de tiempo: Antes, Durante y Después, que son los mecanismos de: La prevención, la detección y la recuperación. Uno de los mecanismos de protección es la criptografía o cifrados de datos, la cual estudiaremos a continuación.

6.2.8.1 La criptografía. La criptografía es la herramienta que se usa como mecanismo de protección de redes de comunicación, el objetivo es hacer la transmisión segura de la información en un medio inseguro.
Herrera, García y Perramón. Explican, "La *criptografía* estudia, desde el punto de vista matemático, los métodos de protección de la información. *Criptoanálisis* estudia las posibles técnicas utilizadas para contrarrestar los métodos criptográficos, y es de gran utilidad para ayudar a que estos sean más robustos y difíciles de atacar. El conjunto formado por estas dos disciplinas, criptografía y criptoanálisis, se conoce como *criptología*."[32]

Entre los sistemas de criptografía se consideran como principales, la criptografía de clave simétrica o de clave secreta y, la criptografía asimétrica o de clave pública.

6.2.8.2 Criptografía de clave simétrica. Según como lo explica Herrera, García y Perramón[33]. Es la clave usada por el emisor y el receptor, se conoce como clave simétrica. Dado que el medio de transmisión puede ser inseguro se debe buscar

[31] LOINAZ, Iñaki, CORTIÑAS, Roberto y EZEIZA, Aitzol. (2005). *Linux*. *Administración del sistema y la red*. Madrid. PEARSON EDUCACIÓN S.A. 2005. p.135.
[32] HERRERA, Jordi; GARCÍA, Joaquín y PERRAMÓN, Xavier. Aspectos avanzados de seguridad en redes. Mecanismos de protección. Barcelona. Universidad abierta de Cataluña, 2004, p. 7.
[33] Ibit., p.107.

vías seguras para dar a conocer a los usuarios autorizados dicha clave. Ejemplo el uso del correo certificado. A continuación los diferentes métodos de cifrados:

DES (Data Encryption Standart): Desarrollado por IBM en 1977, EEUU lo adoptó como estándar para el cifrado de las comunicaciones seguras. Se conforma por bloques de 64 bits pero su clave realmente es de 56 bits debido a que usa sólo 7 de los 8 bits disponibles. Se puede usar para cifrar y descifrar.

TripleDES: Se toma la decisión de mejorar las debilidades de DES ante ataques de fuerza bruta; la mejora consiste en hacer cifrados múltiples a partir del mismo DES (tres veces) con diferentes claves y, en 1999 se cambió entonces el DES por el TripleDES, hasta que se definiera el nuevo estándar AES.

AES (Advanced Encryption Standart): Tras de proponer un concurso para escoger el nuevo AES, el NIST (National Institute of Standars Technology) en 1998, escogió entre cinco finalistas el algoritmo Rijndael como nuevo estándar AES. Sus autores son Vincent Rijmen y Joan Daemen de origen belga, los cuales conformaron un algoritmo que pudo superar los niveles de cifrado a 128 bits propuesto por AES, llegando a niveles de 192 o 256 bits, cuyas características terminaron por desplazar definitivamente al DES y su variante TripleDES.

6.2.8.3 Criptografía de clave pública. Según como lo explica Herrera, García y Perramón[34]. La clave pública o asimétrica funciona con el manejo de dos claves, el mensaje se cifra con una clave y este solo puede ser descifrado con la otra clave. Por tanto aunque la transmisión se haga por un medio inseguro ofrece más fortaleza que la clave privada. A continuación los diferentes métodos de clave pública:

Diffie-Hellman: En los 70´s los matemáticos Whitfield Diffie y Martín Hellman apoyados por Ralph Merkle (Informático), elaboraron un algoritmo capaz de realizar el intercambio de una clave de criptografía convencional utilizando un intercambio público de información.

RSA: Creado por Ron Rivest, Leonard Adleman y Adi Shamir en 1977, se fundamentaron en los algoritmos del Máximo común divisor de Euclides (Grecia 450-377 AC) y el Teorema de Fermat (Francia1601-1665). La fortaleza del sistema radica en que: se requiere mucho tiempo para factorizar n, y en caso de mejorar los recursos de cómputo para hacer los cálculos, se puede aumentar su tamaño garantizando la seguridad. Además, para descifrar se requiere que sin p y q (son secretos) no se puede encontrar.

[34] Ibit., p. 120.

Actualmente se puede implementar una infraestructura de clave pública conocida como *PKI***;** su funcionalidad consiste en que una entidad certificadora garantiza que el uso de la clave pública pertenece a sus usuarios propietarios.

Otro de los mecanismos de protección es el de protocolos seguros a nivel de transporte, como: SSL, TLS y WTLS.

El protocolo de transporte *Secure Sockets Layer* (SSL), fue desarrollado por Netscape a principios de los años 90. También es utilizado por otros navegadores para establecer canales seguros sobre Internet. Las páginas se identifican por HTTPS y se conectan a través del puerto 443, este protocolo está más orientado al servicio del comercio y a la banca electrónica. Permite el cifrado de datos por algoritmos simétricos como 3DES, y la clave de sesión con algoritmos asimétricos como RSA.

La especificación *Transport Layer Security* (TLS), elaborada por la IETF (Internet Engineering Task Force), fue publicado en el documento RFC 2246. Fue generado a partir de la versión 3.1 del SSL y su área de atención son los protocolos diferentes al HTTP, especialmente los correspondientes al correo electrónico (SMTP, POP, IMAP).

El protocolo Wireless Transport Layer Security (WTLS), perteneciente a la red de dispositivos móviles o inalámbricos. La base de este protocolo, es SSL/TLS, lo adicional de él, procura hacer una mejor administración de los dispositivos que es capaz de manejar, optimizando para tal efecto el uso del ancho de banda disponible.

Otra alternativa de protección es el establecimiento *red privada virtual o VPN*, que es un medio de comunicación confidencial que no puede ser interceptado por usuarios ajenos a la red, se fundamenta en el encapsulamiento de protocolos que se utilizan sobre la infraestructura de la red pública, como internet, para establecer por encima de ella una red virtual.

6.2.9 La recuperación. Este es uno de los mecanismos de seguridad más usado; consiste en la realización de copias de seguridad, esto garantiza la disponibilidad e integridad, para darle mayor eficacia se debe complementar con los mecanismos de prevención, detección y confidencialidad**.**

6.3. MARCO CONCEPTUAL

6.3.1 Firewall. Es un sistema que protege a un computador o a una red de computadores contra ataques o intrusiones originadas desde Internet u otras redes de terereos. Los firewall se encargan de filtrar los paquetes que se intercambian a

través de Internet[35]. El firewall incorpora interfaces para la red interna (Red a proteger) e interfaces para la red externa (Acceso a Internet). Pueden funcionar por hardware conocidos como apliance o software corriendo sobre un servidor y su funcionalidad consiste en filtrado de paquetes, filtrado de aplicaciones, portección de virus, spam y prevencion de intrusiones.

Como lo explica García, Fernández, Martínes y otros[36], los firewall son un sistema de defenza que permite o deniegan un servicio basados en reglas configurables y otros criterios predefinidos. Realizan bloqueos de paquetes por puertos, direcciones o rangos de IP, dominios, direcciones de correo, protocolos y aplicativos Web no autorizados. Adicionalmente los firewall generan reportes ´que son utilizados por el administrador de seguridad y verificar el comprotamiento de la red interna y externa, pueden almacenar registros o logs que son útiles para anális forence, permiten la segmentación segura de la red y además integran las funciones de defensa en contra de virus, spam, malware, ransomware, entre otros tipos de virus.

6.3.2 Clasificación de los Firewall. Como lo explica García, Fernández, Martínes y otros[37], pueden claificarse según su modo de empleo como:

- **Modelo de arquitectura.** Dependiendo del lugar donde se aplique, si se ubica en la parte externa de la red y se comunica con Internet se denomina *firewall de contención*, si se ubica internamente en la red y protege las redes internas se denomina *firewall bastión*. Si solo hay un firewall protegiendo la red se denomina bastón.

- **Firewall por Software.** Estos son instalados en un servidor, como son Iptables de Linux, Pfsense de Linux, VPN-1/Firewall-1 de Checkpoint, o ISA server de Microsoft entre otros.

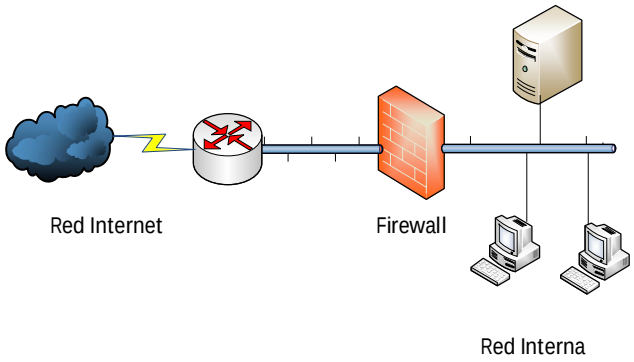
- **Firewall Appliance.** Es un dispositivo con aplicaciones de hardware embebidas con su propio sistema operativo y solo requiere configuraciones mínimas para funcionar, comos son: PIX Firewall de Cisco, Checkpoit, Palo Alto Network, SonicWall de Cisco, Fortinet, entre otros. Los Appliance presentan características de tener hardware y Software embebidos, el software se ejecuta en su propio sistema operativo, Se apoya con otros fabricantes para mejorar la seguridad, poseen un hardware de mejor rendimiento y procesamiento para ciertos algoritmos de cifrado de datos.

[35] KIOSKEA.NET. Firewall [en línea]. Junio de 2014. [Consultado 14 de marzo de 2016]. Disponible en Internet: http://es.ccm.net/contents/proteccion-2675306562#590
[36] García, Jean; Fernández, *et al.* Hacking y seguridad en internet. Bogotá: Ediciones de la U. 2013. p. 371.
[37] Ibit., p.372.

6.3.3 Arquitectura de firewalls. Como lo explica García, Fernández, Martínes y otros[38], existen diferentes arquitecturas de firewall según la ubicación y la forma como protege a la red, a continuación estudiaremos las siguientes:

6.3.3.1 Arquitectura con Firewall Bastión. Este tipo de arquitectura implementa normalmente un solo firewall que protege la red interna de la red exterior; que normalmente es la red de Internet. La Figura 6 siguiente muestra la arquitectura:

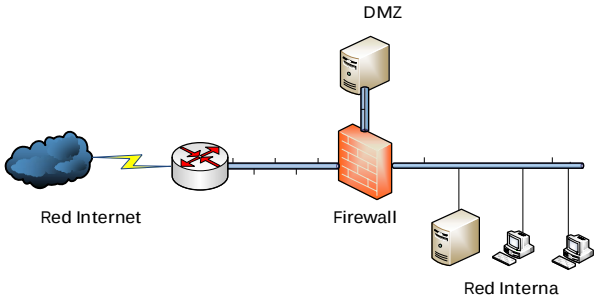
Figura 6. Arquitectura de Firewall Bastión.



Fuente: El autor.

6.3.3.2 Arquitectura Firewall DMZ y Red Interna. Esta arquitectura contempla una zona o zonas llamadas "Zonas desmilitarizadas" o DMZ; en esta zona se ubican los servicios que se requieren publicar a Internet o de acceso al público como son los servicos de correo lectrónico, servidores de página Web, servidores de dominios DNS, entre otros que requieren publicación a Internet. Por lo tanto el firewall requiere mínimo de tres interfaces: Una para proteger la red interna, otra para proteger la zona desmilitarizada DMZ y la tercera para la red externa o de Internet. La Figura 7 siguiente visualiza la arquitectura.

Figura 7. Arquitectura de Firewall DMZ y red interna.

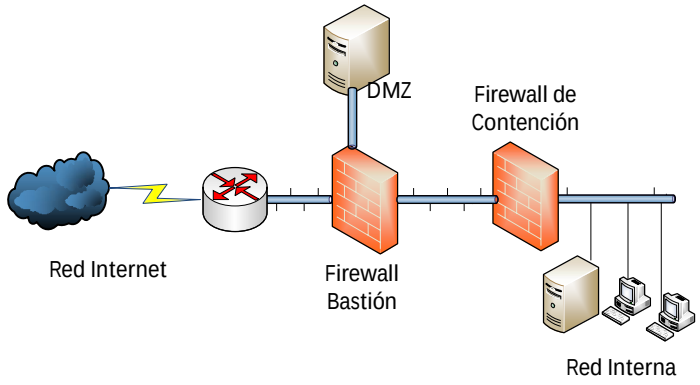


Fuente: el autor.

[38] Ibit., p.379.

6.3.3.3 Arquitectura firewall Contención – Bastión. Para esta arquitectura se utilizan dos firewall; el bastión protegiendo la DMZ de la red externa y uno interno entre la red DMZ y la red Interna; protegiendo la red interna del tráfico que entra de la DMZ, adicionalmente protege también de la red externa o de Internet. La configuración de las políticas en esta configuración es de mucho cuidado porque no son las mismas para cada firewall. La siguiente Figura 8 muestra la arquitectura.

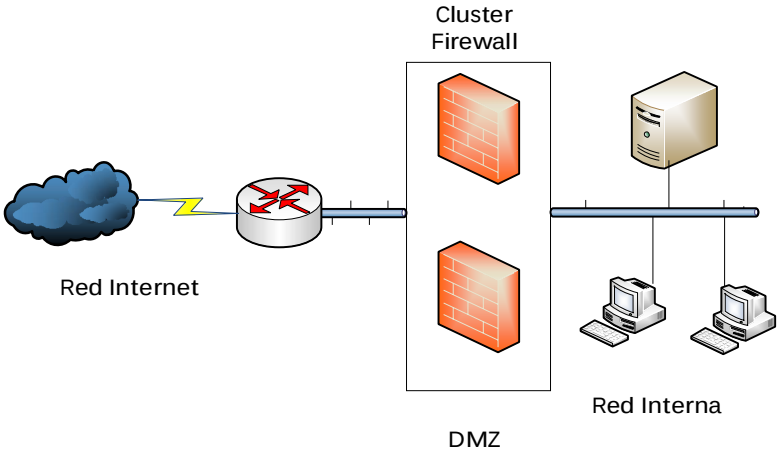
Figura 8. Arquitectura Firewall Contención-Bastión



Fuente: el autor.

6.3.3.4 Arquitectura de Alta Disponibilidad. Este tipo de arquitectura se implementa en firewall perimetrales de red y en la que se debe garantizar la continuidad del servicio. A falla de uno el otro firewall sigue funcionando. Esta funcionalidad se conoce como firewall en clúster. La Figura 9 muestra la arquitectura.

Figura 9. Arquitectura Alta disponibilidad.



Fuente: el autor.

Es importante explicar varios conceptos al implementar un firewall, como son:

6.3.4 NAT. Como lo explica García, Fernández, Martínes y otros[39] (Network Address Translation), consiste en el mapeo de direcciones IP, de tal manera que una dirección de servidor que necesita ser publicada en internet se le esconde con la del Firewall. Esto puede ser muy util en la escaces de direcciones IPv4 y además para mejorar la seguridad de la red puesto que el servidor no estaría expuesto directamente a Internet con una IP pública.

6.3.5 NAPT. (Network Address Port Translation), en este caso un grupo de puertos asociados a una dirección IP son trasladados a otros puertos de otra IP. Esta tralación es util para dar mejor protección de servicios en puertos conocidos.

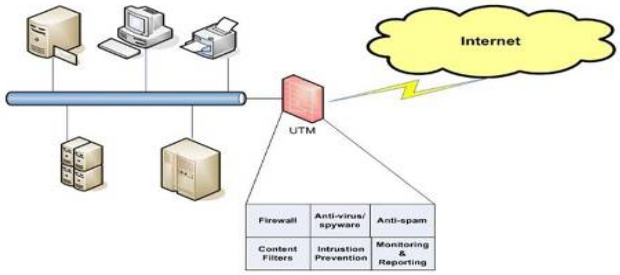
6.3.6 SPOOFING. Como lo explica García, Fernández, Martínes y otros[40], son paquetes con información falsa que provienen de una red externa pero que como origen tiene una dirección IP privada perteneciente al grupo de direcciones IP privadas en la red interna, esto puede confundirese como tráfico normal perteneciente al grupo de direcciones IP privadass de la red interna. Para controlar este tipo de tráico se debe configurar reglas en firewall para que no permita direcciones IP privades desde la red externa o de Internet, este mecaanismos se conoce como anti spoofing.

6.3.7 FRAGMENTACIÓN. Una de las vulnerabilidades del filtrado de paquetes era la fragmentación; es decir se revisaba solo el encabezado de paquetes fragmentados y luego se dejaba pasar los siguientes fragmentos sin verificación, por lo tanto la RFC 1858 define los metodos para detener la fragmetación y separación de los puertos TCP y UDP.

6.3.8 UTM (Unified Threat Management). Gestor unificado de amenazas, incorpora las funcionalidades de protección de la red en tiempo real contra múltiples amenazas cada vez más peligrosas y complejas por la misma evolución tecnológica y nuevos servicios integrados a la red. Es un dispositivo de hardware y software de nueva generación de los sistemas de protección de la red. Detectan y eliminan las amenazas presentes en contenidos de correo electrónico o tráfico Web como virus, gusanos, intrusiones, contenidos web maliciosos; con protecciones en tiempo real y sin degradación del tráfico de la red. La Figura 10 muestra un esquema de protección de la red con UTM, para diferentes dispositivos interconectados y diferentes servicios de protección contra amenazas.

[39] Ibit., p. 382.
[40] Ibit., p. 382

Figura 10. Esquema de protección con UTM



Fuente: http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security

Para la implementación de un UTM, es necesario considerar además de los requerimientos básicos de protección, otras considereaciones claves que se centran en la parte operativa como las siguientes:

6.3.9 Funcionalidad IPS. La primera consideración es la de que servios se necesitan y en donde están los que se necesitan. Para los sistemas de red con servidores que incorporan aplicaciones críticas, es necesario el Sistema de Protección de Intrusiones (IPS), con filtrado de anti-spam en correos electróncos entrantes. Si se considera un alto impacto de información privilegiada se puede pensar en implementación de de las IPS en los segmentos internos de la red que alojan vases de datos, dejando el filtrado para otros dispositivos UTM desplegados[41].

6.3.10 Rendimiento. Cuando se combinan muchas funcionalidades en un solo dispositivo es necesario considerar el rendimiento dependiendo de la cantidad de módulos en servicio en el UTM. Por ejemplo, si se incorpora la fucnionalidad de antivirus puede afectarse el rendimiento y se puede desmejorar si se incorpora otros módulos, como por ejemplo, protección contra denegación de servicios (DoS).

6.3.11 Balanceo de carga. Una forma de hacer frente a un aumento del tráfico es distribuir la carga de trabajo a través de múltiples dispositivos o hacer distribución de tráfico por diferentes interfaces. La configuración óptima dependerá de la particular, los patrones de tráfico y la arquitectura de una red, por lo tanto la estrategias de implementación puede ser un factor distintivo entre los dispositivos UTM. Otra cuestión a considerar durante las evaluaciones UTM es si los productos tienen una infraestructura de hardware modular que distribuye la potencia de procesamiento entre las contramedidas para lograr el mejor rendimiento general[42].

[41] http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security
[42] http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security

6.4. CIBERSEGURIDAD

Según lo explicado por Palo Alto Networks[43], la ciberseguridad consiste en proteger los datos y la red del uso no autorizado. Para ello se requiere de los Firewall con políticas de control de accesos detallados, además de garantizar la integridad de los datos, debido a que estos pueden ser dañados por amenazas ocultas, por lo que se requiere integrar muchas funcionalidades de protección para poder proteger los datos de las amenazas cada vez más complejas. Para alcanzar los niveles adecuados de seguridad, se debe reducir la superficie de ataques, evitar amenazas conocidas, detectar amenazas desconocidas y darlas a conocer y mitigar infecciones del día cero.

6.5. MARCO LEGAL

El marco legal colombiano en su constitución política contempla en el artículo 15 el derecho fundamental de habeas data y en el artículo 20 la libertad de información. Seguidamente se describe la legislación colombiana de manera cronológica:

6.5.1 Ley 527 de 1999[44]. "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disponibles".

6.5.2 Ley 1266 de 2008[45]. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".

6.5.3 Ley 1273 de 2009[46]. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y la comunicaciones, entre otras disposiciones".

---

[43] Palo Alto Networks. Disponible en Internet: https://www.paloaltonetworks.es/products/platforms/firewalls/pa-3000/overview.html

[44] Alcaldía de Bogotá. Ley 527 de 1999 nivel nacional. Diario Oficial 43.673 del 21 de agosto de 1999. [en línea]. 2017. [Consultado mayo 15 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. 16 p.

[45] Secretaría del Senado. Congreso de la República. Colombia. Ley estatutaria 1266 de 2008. Diario Oficial No. 47.219 de 31 de diciembre de 2008 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. 18 p.

[46] Alcaldía de Bogotá. Ley 1273 de 2009 nivel nacional. Diario Oficial 47.223 de enero 5 de 2009 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. 5 p.

6.5.4 Ley 1581 de 2012[47]. "Por la cual se dictan disposiciones generales para la Protección de Datos Personales".

6.5.5 Ley 1621 de 2013[48]. "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones".

6.5.6 Ley 1712 de 2014[49]. "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

6.5.7 Decreto 1727 de 2009[50]. "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información".

6.5.8 Decreto 2952 de 2010[51]. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".

6.5.9 Decreto 1377 de 2013[52]. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

6.5.10 Decreto 886 de 2014[53]. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".

---

[47] Alcaldía de Bogotá. Ley 1581 de 2012 Nivel Nacional. Diario Oficial 48587 de octubre 18 de 2012. [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. 15 p.

[48] Secretaría del Senado. Congreso de la República. Colombia. Ley estatutaria 1621 de 2013. Diario Oficial No. 48.764 de 17 de abril de 2013 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html

[49] Alcaldía de Bogotá. Ley 1712 de 2014 nivel nacional. Diario Oficial 49084 de marzo 6 de 2014 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882. 237 p.

[50] Alcaldía de Bogotá. Decreto 1727 de 2009 nivel nacional. Diario Oficial 47.350 de mayo 15 de 2009 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251. 6 p.

[51] Alcaldía de Bogotá. Decreto 2952 de 2010 nivel nacional. Diario Oficial 47793 de agosto 6 de 2010 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120. 4 p.

[52] Alcaldía de Bogotá. Decreto 1377 de 2013 nivel nacional. Diario Oficial 48834 del 27 de junio de 2013 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. 12 p.

[53] Alcaldía de Bogotá. Decreto 886 de 2014 nivel nacional. Diario Oficial 49150 de mayo 13 de 2014 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338. 6 p.

En el marco internacional, la Organización de Estados Americanos (OEA); en el área de Departamento de Derecho Internacional, contempla la reglamentación de datos personales regulada para cada país. Estados Unidos existen leyes especiales como:

6.5.11 La Ley de Libertad de Información, 5 U.S.C. § 552[54]. Enmendado por:
Ley Pública No. 110-175, 121 Stat. 2524. De estados Unidos de América.
Ley Pública No. 111-83, § 564, 123 Stat. 2142, 2184. De Estados Unidos de América.

[54] OEA. Organización de Estados Americanos. Departamento de Derecho Internacional. 2017 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_estados_unidos.asp

7. DISEÑO METODOLÓGICO

El proyecto está enmarcado en una investigación descriptiva y documental, tiene como finalidad plantear y ejecutar una propuesta de solución factible a un problema previamente detectado, que afecta la seguridad informática de la institución. Pretende detectar, identificar y medir las vulnerabilidades, amenazas y riesgos que afecten la confidencialidad, la integridad y la disponibilidad de la información.

De Moya[55], 2002, p.10, describe que para iniciar el diseño de un proyecto factible se plantean las siguientes preguntas: ¿qué hacer?, ¿para qué hacerlo?, ¿por qué hacerlo?, ¿cómo hacerlo?, ¿dónde hacerlo?, ¿qué magnitud tiene?, ¿cuándo se hará?, ¿quiénes lo harán?, ¿con qué medios y recursos se hará?, ¿qué sucede durante la ejecución?, ¿cuáles son las limitaciones?

Para el análisis de fallas o vulnerabilidades de seguridad informática en la red de la UPB Montería, se realizó el análisis de la infraestructura física y lógica de la red, incluidos switches, enrutadores, políticas de firewall, accesos al sistema de información, acceso a Internet, obteniendo como resultado de análisis que la solución más adecuada es la implementación de un firewall perimetral UTM de nueva generación, aplicando reglas de filtrado y controles de seguridad informática más eficiente.

Luego de diagnosticado el problema y proponer la solución de implementar un UTM de nueva generación, se plantea el rediseño nuevamente de la red para obtener una solución fiable que facilite la gestión unificada de amenazas.

Para la recolección de la información del estado actual de la red corporativa de UPB Seccional Montería, se realizaron sesiones de trabajo conjuntas con personal encargado de infraestructura del área de tecnologías de la información de UPB y docentes especializados. Luego se define la propuesta de solución y se afianza en consultas bibliográficas, artículos de seguridad, foros de internet y proveedores de infraestructura de seguridad especializados.

7.1. POBLACIÓN Y MUESTRA

La implementación de este proyecto beneficia directamente a la comunidad universitaria de UPB Seccional Montería, conformada por estudiantes, docentes y administrativos. En la tabla 2 se detalla la comunidad educativa.

[55] De Moya R., Proyecto factible: una modalidad de investigación. Recuperado de:http://www.redalyc.org/pdf/410/41030203.pdf

Tabla 2. Comunidad educativa

INTEGRANTES	TAMAÑO
Estudiantes	2.306
Administrativos	169
Docentes	80
Total	2.555

Fuente: el autor.

Para la muestra de tráfico por la población universitaria, se tomaron muestras de tráfico promedio por día y por mes de estudiantes, administrativos y docentes, como se evidencia en la tabla 3. Tamaño de la muestra de tráfico.

Tabla 3. Tamaño de la muestra

MUESTRAS DE TRAFICO POR POBLACIÓN	PROMEDIO EN Mbps
Tráfico de Internet de administrativos	11,61
Tráfico de Internet de estudiantes	99,32
Tráfico de Internet de docentes	5,00
Total de tráfico promedio	**115,93**

Fuente: el autor.

La metodología se establece en cuatro momentos o etapas de la investigación que son: Planeación, ejecución, capacitación y pruebas y puesta en producción.

7.2. PLANEACIÓN

Esta primera etapa consiste en preparación, delimitación del alcance, recursos necesarios, estudio de la red actual en la UPB seccional Montería mediante levantamiento de esquema de red y conectividad, activos informáticos y de seguridad. Luego del análisis de la situación actual de la red perimetral e interna, se hará el rediseño de la red para poder implementar el gestor unificado de amenazas a la red de la institución. Finalmente para esta etapa se hará el dimensionamiento de los recursos de hardware necesarios basados en el análisis de la red para implementar el UTM.

En esta fase se plantean las siguientes preguntas las cuales son guías o rutas de trabajo:

- ¿Cuál es la topología de red?
- ¿Inventario de la red?
- ¿En qué sistema operativo está basada la red de UPB?

- ¿Cuáles son los sistemas operativos de escritorio?
- ¿Qué servicios ofrecen los servidores (DNS, Correo, WEB, aplicación, antivirus, entre otros)?
- ¿Cómo se hace el filtro de red (Firewall)?
- ¿Qué vulnerabilidades están presentes en la red LAN y WAN?

En esta fase también, se plantea las necesidades y requerimientos de la red institucional de UPB seccional Montería basada en Firewall UTM. Se plantea las siguientes preguntas guías de acción:

- ¿Cuál es la arquitectura adecuada para la red institucional basada en firewall UTM?
- ¿Qué requerimientos de hardware y software son necesarios para cumplir con las políticas de seguridad?

7.3. EJECUCIÓN

En esta etapa se evalúan las diferentes tecnologías UTM a implementar, hacer el proceso de adquisición e implementar el gestor unificado de amenazas UTM de acuerdo a los requerimientos de protección de la red institucional de UPB Seccional Montería.

La seguridad perimetral es uno de los diseños posibles de defensa de una red, basado en el establecimiento de recursos de contención, prevención y filtrado en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. Los riesgos se pueden mitigar implementando:

Guerra[56], describe un **UTM** (Unified Thread Management) como un dispositivo de red que en su funcionamiento básico incorpora las funciones de un Firewall, también integra otras funciones como conexiones físicas y lógicas, direccionamiento IP, canales VPN, permisos de navegación, escaneo de antivirus, cifrado de conexiones, filtrado de navegación, escaneo antispyware, anti spam, detección de intrusos (IDS), control a nivel de aplicaciones, la gestión del tráfico, entre otros.

Los UTM[57] no solo hacen las funcionalidades nombradas anteriormente, también hacen protección de tráfico, rendimiento, balanceo de la red y gestión de ancho de

[56] GUERRA, Cristian. Implementación de una red segura para los laboratorios del DEEE utilizando un dispositivo UTM [en línea]. Tesis de pregrado. Sangolquí: Escuela Politécnica del ejército. Departamento de Eléctrica y Electrónica, 2011. 149p. 2011. [Consultado 13 de febrero de 2016]. Disponible en Internet:http://repositorio.espe.edu.ec/handle/21000/4741

[57] Ibíd., p.19.

banda, incorporando funcionalidades que ofrecen una protección de seguridad informática más robusta.

Cabe aclarar que los componentes básicos se encuentran siempre en cualquier UTM, y los componentes avanzados se encuentran en algunos, de acuerdo al fabricante, referencias y dimensionamiento de acuerdo al volumen de tráfico, funcionalidad y seguridad a implementar.

7.4. SOLUCIÓN PROPUESTA

La solución propuesta consiste principalmente, en la implantación de un Firewall UTM; el cual sería el encargado de controlar los paquetes de entrada y de salida de la empresa, se establecerían las reglas de filtrado de la red, para que toda la empresa tanto en su red de visitantes, como en su red empresarial, estén protegidos, y así brindar la seguridad informática que requiere la empresa.

La implementación del Firewall UTM incluye un análisis y levantamiento de la red actual, una reingeniería de la estructura de la red LAN y de servidores de la UPB Seccional Montería, posterior a un análisis detallado de la situación inicial de la misma y así poder aplicar las mejoras a este diseño. Se instalará y configurará el dispositivo por Hardware o Software UTM, luego del análisis y comparación de los diferentes UTM que cumplan con los requerimientos y dimensionamiento de tráfico de la UPB Seccional Montería.

Las características de seguridad a implementar son:

- Monitoreo en tiempo real de tráfico de red.
- Balanceo y alta disponibilidad de enlaces de internet.
- Enrutamiento: Estático, OSPF, BGP Multicasting.
- Agregado de enlaces.
- Sistema de detección y prevención de intrusos (IPS).
- Posibilidad de alta disponibilidad en hardware.
- Servicios de red: DNS, DHCP, NTP.
- Soporte de IPv6.
- NAT: Destination NAT, Source NAT, Full NAT.
- Filtrado de navegación web.
- Protección antivirus y antispyware perimetral.
- Control de aplicaciones.
- Protección anti spam y antivirus de correo.
- Cifrado de correo electrónico.
- VPN site-to-site: IPSec y SSL.
- Acceso remoto vía VPN SSl, IPSec, PPTP, L2TP/IPsec.
- Web Application Firewall (Firewall de aplicaciones web).
- Protección contra amenazas avanzadas.

Se analizará las diferentes tecnologías UTM a implementar, teniendo en cuenta los líderes del mercado según el cuadrante de Gartner; como son: Fortinet, SonicWall, Sophos, Palo Alto Networks, Pfsense, entre otros.

El alcance de esta propuesta de solución es para la red institucional de UPB Montería, cubriendo la protección de las diferentes subredes administrativas y académicas, roles de servidores, conexiones físicas y lógicas, reglas de Firewall, direccionamiento IP, canales VPN, permisos de navegación, escaneo de antivirus, cifrado, filtrado de navegación, escaneo antispyware, control a nivel de aplicaciones, control de tráfico de red, etc.

Se plantean las siguientes preguntas guía de acción:

- ¿Cuáles es el UTM adecuado para los requerimientos de la red institucional de UPB Seccional Montería?
- ¿El UTM a implementar cumple las características de seguridad requeridas a implementar?
- ¿El UTM está al alcance de los recursos financieros de la institución?

7.5. CAPACITACIÓN Y PRUEBAS

En esta etapa se realiza la capacitación para el administrador de la red para la administración del UTM, se realizan las pruebas de amenazas, vulnerabilidades, escaneo de virus, malware, gestión de tráfico, control de aplicaciones y contenidos Web, simulaciones, análisis de tráfico, entre otros.

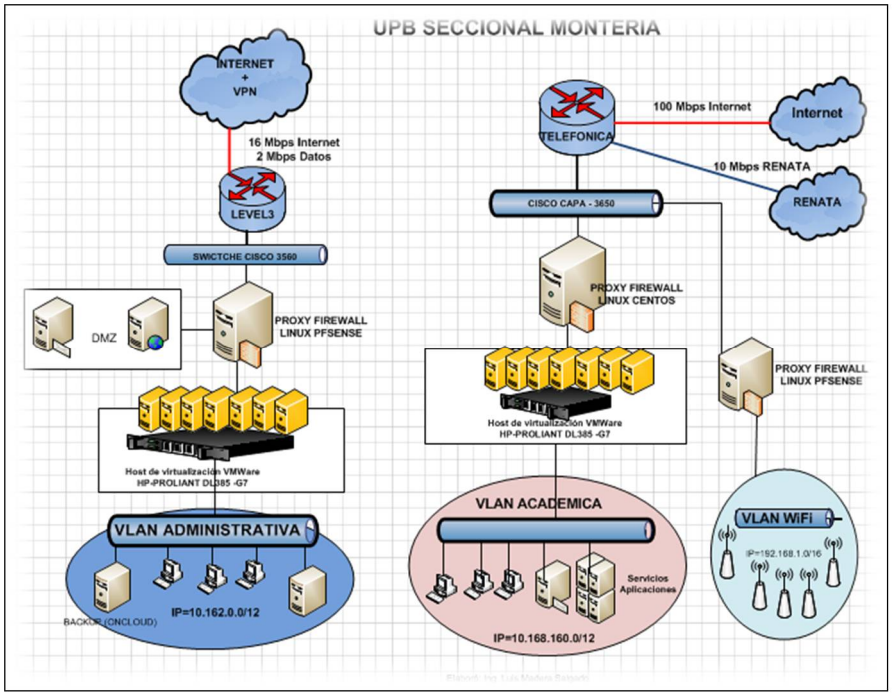
7.6. PUESTA EN PRODUCCIÓN

En esta etapa se presenta los resultados con acta de entrega, documentación y puesta en producción de la solución.

8. IDENTIFICACIÓN DE LA INFRAESTRUCTURA ACTUAL DE LA RED INSTITUCIONAL DE UPB SECCIONAL MONTERÍA Y ANÁLISIS DE VULNERABILIDADES

La red LAN y WAN actual de la UPB seccional Montería, está configurada con tres VLAN (Administrativa, académica y WiFi) y una zona desmilitarizada con elementos activos y pasivos de conectividad a internet y la red Intranet; la zona desmilitarizada nos permite la interconexión entre la WAN y la red LAN a través de servidores de correo, proxy y WEB, Switche Cisco de capa 3 y capa2 y enrutadores de salida a Internet por cada uno de los proveedores del servicio de Internet ISP. (Ver Figura 11). Esquema de conectividad y Servidores de UPB seccional Montería.

Figura 11. Esquema de conectividad de UPB Montería



Fuente: el autor

La conectividad y red corporativa consta de Enrutadores de borde interconectados a Internet y a la VPN de conexión al canal de datos corporativo para acceso al ERP remoto y centralizado en la sede principal UPB Medellín.

La conexión WAN se hace por medio de Fibra óptica proveída por los ISP (Proveedor de Servicios de Internet).

La conexión de la red interna LAN y la VPN se realiza a través de Switches Cisco de capa 3 que separan lógicamente las diferentes VLAN (Administrativa, académica y WiFi).

La red corporativa presenta una complejidad en la administración, debido a que se encuentra separada en las dos principales VLAN y con conexión a Internet por diferente ISP.

Las conexiones de los hosts se hace en cada VLAN a través de Proxy/Firewall de Red a nivel lógico; Linux CentOS para la red académica, Linux PfSense para la red administrativa y WiFi.

A través de los Proxy y firewall de Red los hosts tienen acceso a los servicios Web locales, los servicios de Internet y los accesos remostos a través de la VPN al ERP.

Los servicios Web locales están alojados en dos grandes servidores Físicos de 7ª. Generación y uno de 8ª. Generación. Estos servidores alijan los servicios virtualizados a través del software de virtualización VMWare Sphere.

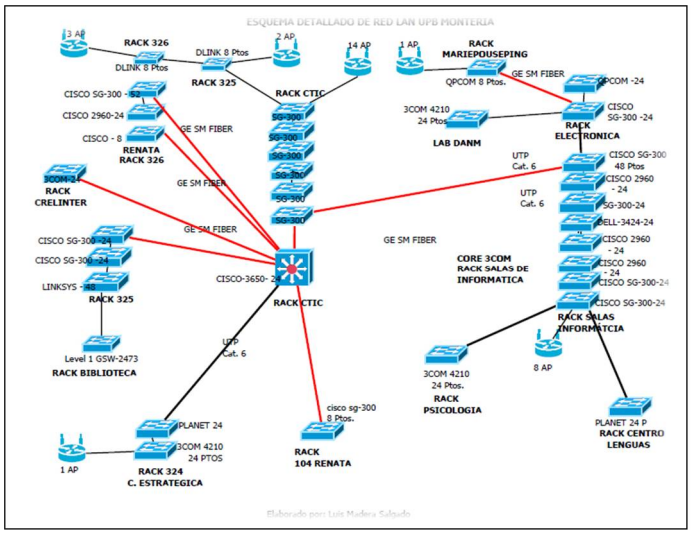
La conexión hacia los 550 puntos de red corporativa se realiza a través de Switches de capa 2 en su mayoría Cisco; distribuidos en diferentes Gabinetes Racks e interconectados por el backbone o enlaces principales por medio de fibra óptica multimodo.

La red de cableado interna es estructurada con cable UTP, categoría 6 en su mayoría, con algunos segmentos en categoría 5e. Cuenta con un área de Data Center y Rack de datos principal y 9 racks de datos adicionales de interconexión LAN.

La Red corporativa presenta una zona desmilitarizada para los servicios que necesitan publicación Web, como son: servicios Web y los proxy/firewall de cada subred.

La siguiente Figura 12. Muestra el esquema detallado de la red LAN de UPB Seccional Montería.

Figura 12. Esquema detallado de la red LAN UPB Montería



Fuente: el autor.

La red LAN está diseñada con Switches de capa 2 y 3, medio de transmisión de fibra óptica y cable UTP categoría 6 para la interconexión de 550 puntos de red. Para la red WiFi se dispone de AP de categoría 802.11n administrados a través de una controladora Ruckus con las funciones de gestión centralizada de los AP, distribución de carga de usuarios entre AP y roaming de usuarios entre APs.

La infraestructura de servidores de red está basada en Sistema Operativo Linux en las distribuciones de CentOS versión 7 y PfSense con Firewall lógico de red.

La infraestructura de usuarios finales es Windows 7, 8 y 10 con arquitectura de 32 y 64 bits.

Los servicios que se ofrecen a través de servidores virtualizados con VMWare es de Proxy, Firewall, Servidor WEB, DNS, Servidor de Antivirus, servidores de control de licencias para software de laboratorios, Servidor de aplicaciones Web, servidor de Bases de Datos, Servidor de envíos masivos de correos, servidor de backup, servidor de plataforma Moodle.

Los servidores proxy/Firewall Linux CentOS y PfSense (**filtrado de paquetes y firewall**) se basa en **Netfilter**; que es la infraestructura tanto del núcleo como de las herramientas de usuario. El proxy se basa en Squid y el firewall en Iptables, ambas herramientas de Linux. El principio de Netfilter es sencillo; consiste en toma de decisiones acerca de cómo debe fluir un paquete. Para ello Netfilter suministra una herramienta sencilla llamada **iptables,** que se puede ejecutar desde la línea de comandos. Mediante Netfilter se hace tres tareas: **NAT** (Network Address

Translation), desmenuzadora y filtro, permite a los administradores esconder los anfitriones de ambos lados del router, de modo que los dos permanecen ignorados de la existencia del otro. Mediante Netfilter, el NAT puede ser: SNAT, NAT fuente, DNAT, NAT destino y Masquerading (Mascarada).

El filtrado en Netfilter se fundamenta en cadenas, que son listas de reglas que actúan sobre un paquete que fluye por el sistema. Hay cinco cadenas predefinidas: PREROUTING, FORDWARD, POSTROUTING, INPUT y OUTPUT.

8.1. EXPLORACIÓN DE LA RED CON NMAP

La aplicación Network Mapper, más conocida como Nmap, es una herramienta que nos permite realizar exploración de puertos desde sistemas Linux. Esta herramienta permite descubrir información de los servicios y sistemas encontrados, así como reconocimiento de huellas identificativas de los sistemas escaneados. Seguidamente se realizará la exploración de nuestro servidor Proxy de la red, utilizaremos el siguiente comando. Para facilidad se utilizará la herramienta gráfica **Zenmap** de uso libre.

Se escanea el Proxy/Firewall de la red académica con el siguiente comando:

Nmap –sS –O –A -Pn -T4 190.66.1.53

Los parámetros indican lo siguiente[58]:

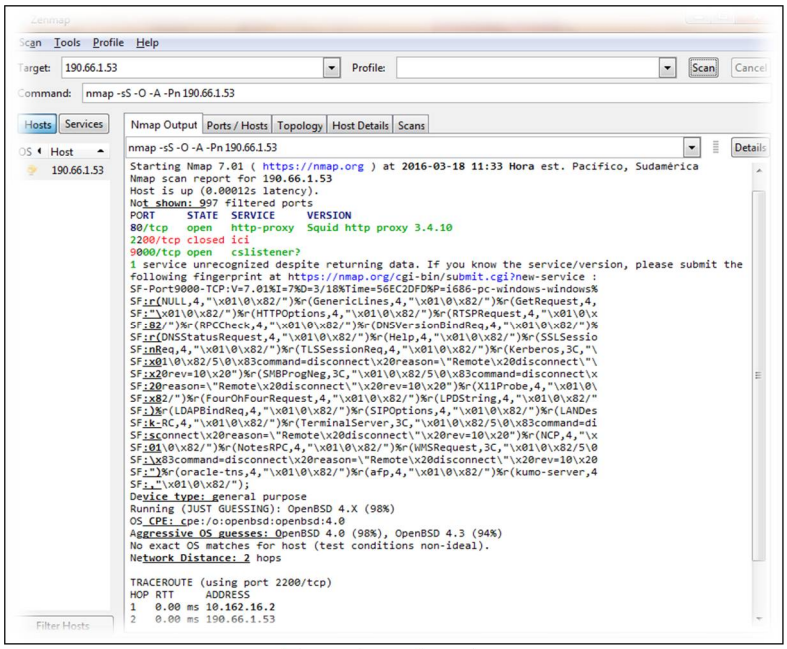
- **O**; la cual hace una predicción del sistema operativo que se está usando.
- **sS**; utiliza una exploración de puertos TCP silencios basada en el envío de paquetes TCP/SYN.
- **Pn**; no utiliza ping para descubrimiento.
- **A**; Permite la detección del sistema operativo.
- **T4**; permite una ejecución más rápida.

Análisis:

Se muestra los puertos 80 y 9000 abiertos; el puerto 80 es normal para los servicios web ofrecido, pero el 9.000 se anuncia como una vulnerabilidad por ser un puerto no conocido, debido a necesidades del servicio de transmisiones radiales se encuentra habilitado para el servicio de audio Streaming Shoucast para la emisora Frecuencia Bolivariana de UPB Montería. Situación que hay que evaluar como mecanismo de seguridad. Ver Figura 13 y 14 de los resultados de escaneo.

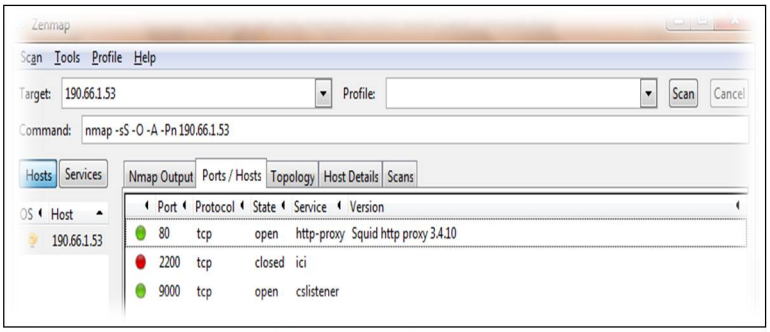
[58] Nmap.org [en línea]. [Consultado marzo 15 de 2016]. En Internet: https://nmap.org

Figura 13. Escaneo de la Red



Fuente: el autor

Figura 14. Escaneo de la Red

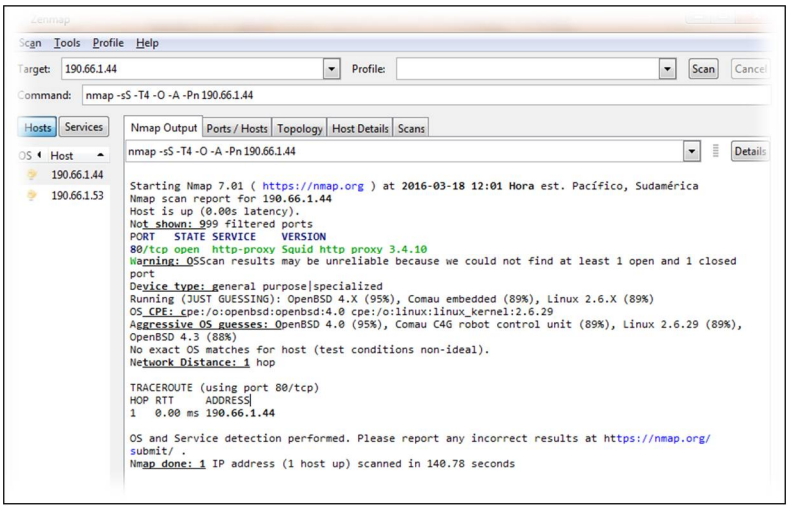


Fuente: el autor

Escaneo para el Proxy/Firewall de Red inalámbrica:

En la Figura 15, se visualiza el escaneo del Firewall de red WiFi presentando solo en servicio el puerto 80.

Figura 15. Escaneo de Firewall de Red WiFi

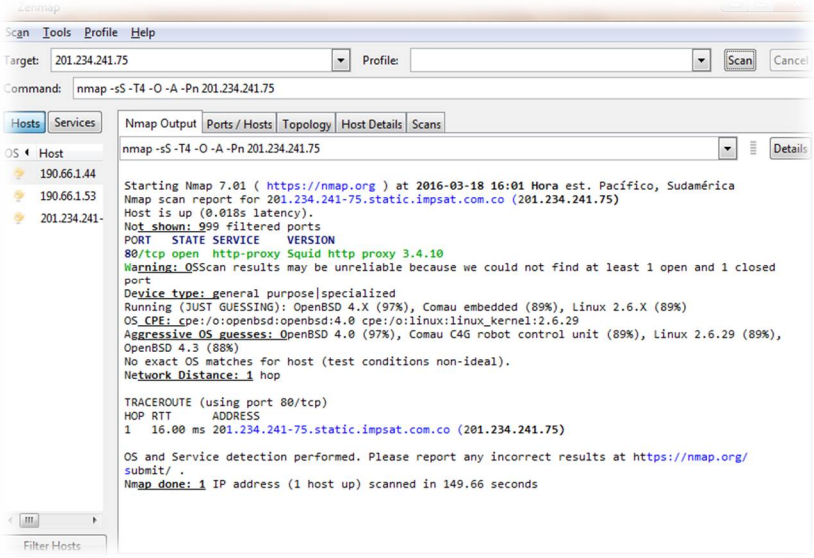


Fuente: el autor

Escaneo del firewall de red Administrativa.

En la Figura 16, se visualiza el escaneo del Firewall de red Administrativa presentando solo en servicio el puerto 80.

Figura 16. Escaneo de Firewall de Red Administrativa

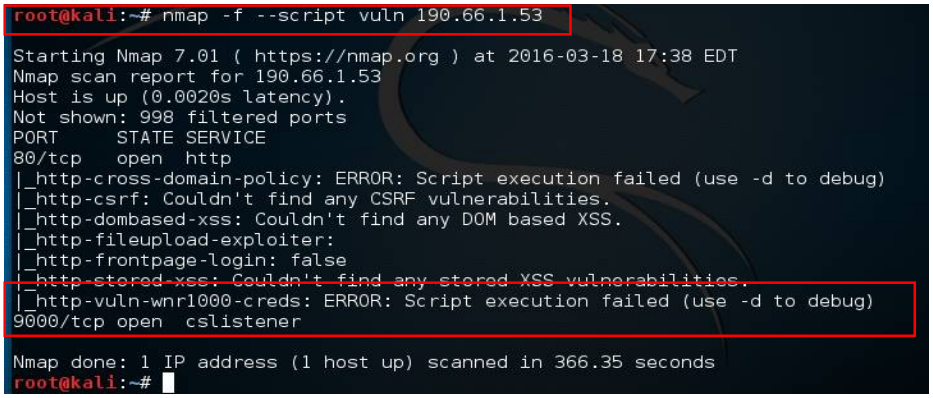


Fuente: el autor

8.2. ANÁLISIS DE VULNERABILIDAD DE LA RED

8.2.1 Análisis con Nmap de Kali-Linux. Se hará inicialmente el uso de la herramienta Nmap de Kali-Linux para el escaneo de vulnerabilidad. En la Figura 17, se detalla el escaneo de vulnerabilidad para el Proxy/firewall Académico basado en Linux CentOS. Se observa el puerto 9000 abierto y hay advertencia por ser un puerto no conocido; pero corresponde a un servicio de audio Shoucast. Además se notifica un error de ejecución de script con la vulnerabilidad wnrl1000; indica que una vulnerabilidad ha sido descubierta en WNR serie 1000 que permite a un atacante recuperar las credenciales de administrador con la interfaz del enrutador.

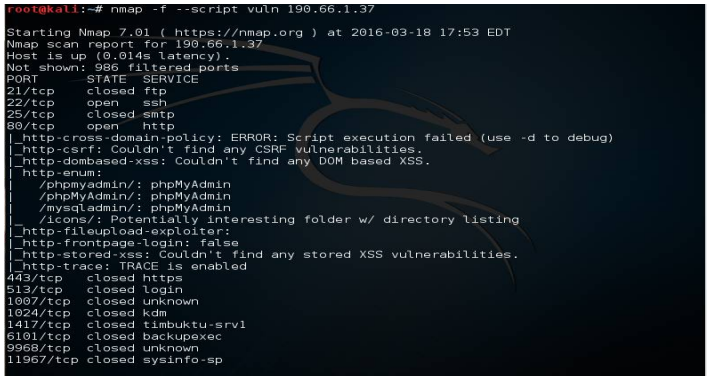
Figura 17. Vulnerabilidades de Proxy Académico



Fuente: el autor

El siguiente escaneo mostrado en la Figura 18, es sobre el Servidor Web que publica en Internet, no presenta vulnerabilidad y los puertos habilitados son los que están en servicio: 80 y 22.

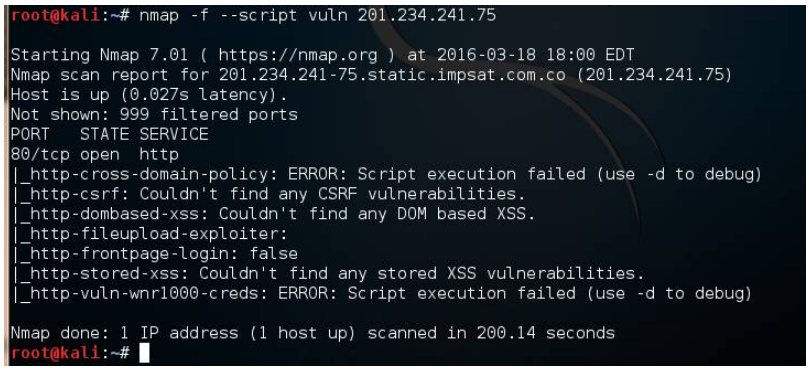
Figura 18. Vulnerabilidades de Servidor Web



Fuente: el autor

En la siguiente Figura 19, se realiza escaneo de vulnerabilidad del Proxy/Firewall PfSense para la red Administrativa, presentando vulnerabilidad de error de script wnr1000.

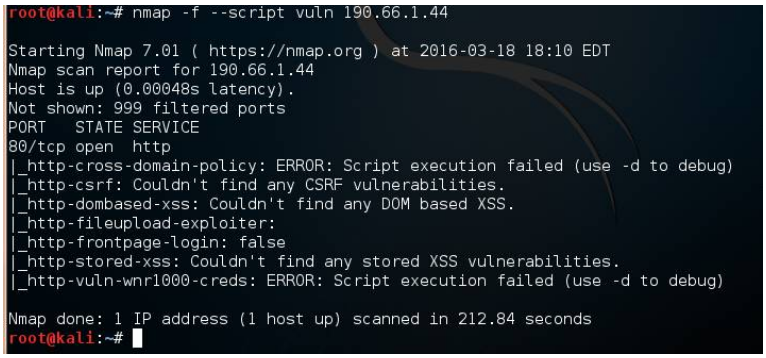
Figura 19. Vulnerabilidades de Servidor Web



Fuente: el autor

La Figura 20 siguiente presenta las vulnerabilidades del Firewall de la red WiFi.

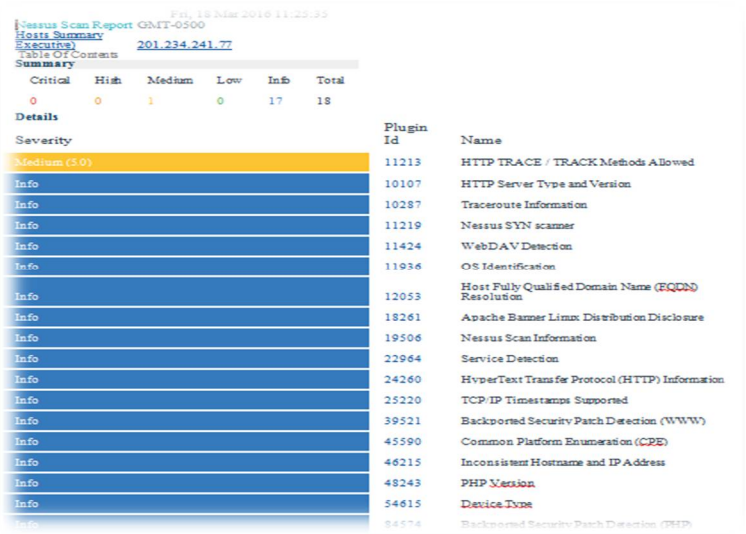
Figura 20. Vulnerabilidades del Firewall WiFi



Fuente: el autor

8.2.2 Análisis de vulnerabilidad con Nessus. En la Figura 21 siguiente se detalla el resultado de vulnerabilidades escaneadas con la herramienta Nessus para el Servidor de publicación.

Figura 21. Escaneo de vulnerabilidad con NESSUS


Nessus Scan Report GMT-0500
Hosts Summary (Executive) 201.234.241.77
Table Of Contents
Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

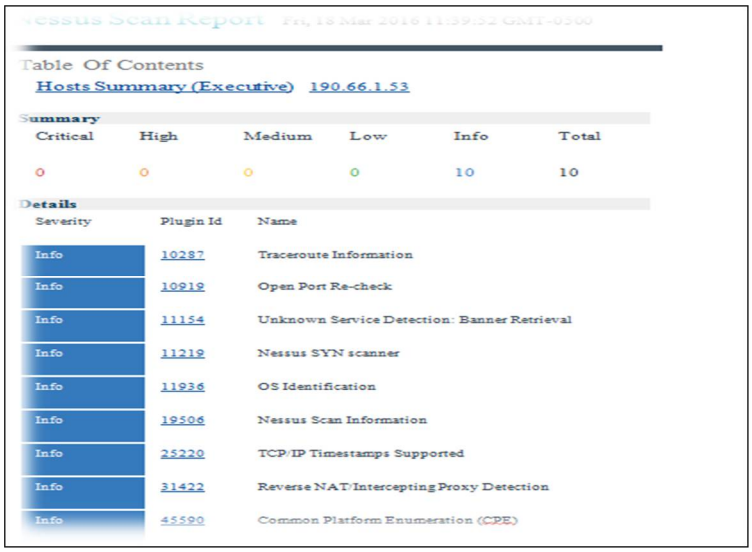
Details

Severity	Plugin Id	Name
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11424	WebDAV Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	48243	PHP Version
Info	54615	Device Type

Fuente: el autor.

En la Figura 22 siguiente se detalla el resultado de vulnerabilidades escaneadas con la herramienta Nessus para el Proxy/Firewall de la red Académica.

Figura 22. Escaneo de vulnerabilidad con NESSUS


Nessus Scan Report Fri, 18 Mar 2016 11:39:52 GMT-0500
Table Of Contents
Hosts Summary (Executive) 190.66.1.53
Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	25220	TCP/IP Timestamps Supported
Info	31422	Reverse NAT/Intercepting Proxy Detection
Info	45590	Common Platform Enumeration (CPE)

Fuente: el autor.

En la Figura 23 siguiente se detalla el resultado de vulnerabilidades escaneadas con la herramienta Nessus para el Proxy/Firewall de la red Administrativa.

Figura 23. Escaneo de vulnerabilidad con NESSUS

Fuente: el autor.

En el análisis con Nessus se realizan advertencias para tener en cuenta y una vulnerabilidad de nivel medio en el servidor Web en los métodos alojados. Para el resto de servicio se debe estar atento a la información y seguimiento.

8.2.3 Análisis de tráfico de la red administrativa. En la Tabla 4. Se resume el tráfico de red para la institución UPB seccional Montería, en el Anexo B, se encuentran las evidencias de medición.

Tabla 4. Tráfico de la red de UPB Montería.

Red	Ancho de Banda Dedicado contratado en Mbps	Entrante en Mbps	Saliente en Mbps	Promedio en Mbps
Tráfico de la Red Administrativa	16	16,61	6,61	11,61
Tráfico de la red Académica	100	60,00	56,00	58,00
Tráfico de la Red WiFi		62,05	20,58	41,32
tráfico del Canal de Datos	2	0,008724	0,003809	0,006267
Renata(Red Educativa nacional de Tecnología Avanzada)	10	5,00	5,00	10,00
Total de tráfico promedio	**128,00**	**138,67**	**83,19**	**120,93**

Fuente: el autor.

Se observa saturación del canal de la red administrativa con un ancho de banda establecido de 16 Mbps, lo que significa que se puede presentar perdida de tráfico

o lentitud en la red, además implica realizar mediciones más detalladas de procesamiento debido al firewall lógico presente en la red sobre servidores. El tráfico total de la red en promedio es de 120,93 Mbps; esto nos lleva a inferir que no hay un buen uso eficiente del ancho de banda total, debido a que las redes están separadas y no se hace balanceo de carga de la red hacia los diferentes operadores que suministran el servicio de Internet (Telefónica y Level3). Este análisis nos lleva a pensar la necesidad de implementación de un UTM que maneje el tráfico de manera más eficiente y seguro de toda la red.

La siguiente Tabla 5, se detalla los roles de servidores al servicio de la seccional; los cuales se pueden resumir en sub portales Web, Bases de Datos locales, servidor de apoyo a los procesos de enseñanza y aprendizaje (Moodle), y servidores de infraestructura de conectividad (Proxy, firewall, DNS, Radius).

Tabla 5. Listado y roles de servidores.

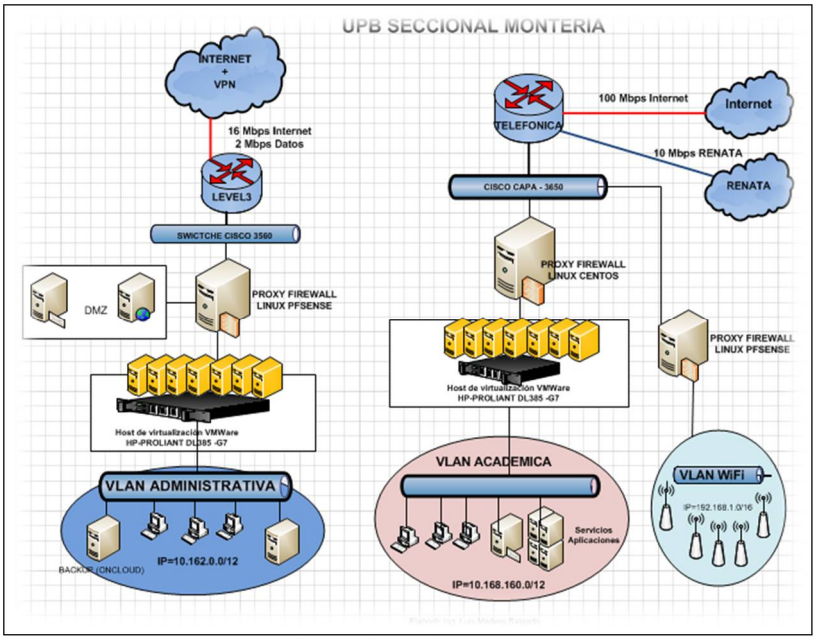
Uds	Categoria	Propietario	Ubicación Física	Descripción	Marca/Modelo
1	Hardware	Luis Madera	Montería - Data Center CTIC	Servidir Físico Proxy y Aplicaciones Web	HP Proliant / DL385 G 7
1	Hardware	Luis Madera	Montería - Data Center CTIC	Servidir Físico Proxy y Aplicaciones Web	HP Proliant / DL320E G 8
1	Software	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare BD Aplicativos	Centos 7 - VmWare Sphere 5.5
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Consultorio médico	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado - Repositorio	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Consultorio Jurídico	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - eventos	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Antivirus	WINDOWS SERVER 2012
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Revista Generos	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - moddle viejo	Centos 6.5
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Firewall Proxy Académico	PfSense 2.2.6
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Portafolio	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Firewall Proxy WiFi	PfSense 2.2.6
1	Bases de Datos	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare BD Radius	Centos 6.5
1	Bases de Datos	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare BD Formación Cont	Centos 7
1	Bases de Datos	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare Licencias de autocad	Centos 6.5
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare BD BIBLIOTECA -SIABUC	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare BD Mercadeo	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Subportal	Centos 6.5
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - moddle	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Procesos	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - DNS	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Control de versiones desarrol	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Antivirus Administrativo	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Correos masivos	Centos 6.5
1	Software	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Desarrollo	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Firewall Proxy Administrativo	Centos 7
1	Bases de Datos	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare -BD Postgre	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Subportal	Centos 7
1	Servicio	Luis Madera	Montería - Data Center CTIC	Servidor Virtualizado VmWare - Servidor OpenVPN	Centos 7

Fuente: el autor

9. REDISEÑO TOPOLÓGICO DE LA RED DE UPB MONTERÍA

La red actual de UPB seccional Montería, presenta una segmentación física para la red Administrativa, Académica y de red inalámbrica. El tráfico administrativo se direcciona a Internet y al canal de datos a través del operador de servicios de Internet Level3 con un ancho de banda dedicado de 16 Mbps para Internet y 2 Mbps para el canal de datos. El tráfico de la red académica e inalámbrica es direccionado a través del proveedor del servicio de Internet Telefónica con un ancho de banda dedicado de 100 Mbps, adicionalmente suministra 10 Mbps de la red RENATA (Red Educativa Nacional de Tecnología Avanzada). En la siguiente Figura 24 se puede observar el diseño actual de la red, con un grado de complejidad para la administración, debido a que el tráfico se cursa por diferentes firewall lógicos y segmentos físicos. Esto puede causar problemas de vulnerabilidad de la red por la dificultad de no tener centralizada la gestión de la red y monitoreo de amenazas de la red.

Figura 24. Diseño de la Red actualmente en UPB Montería

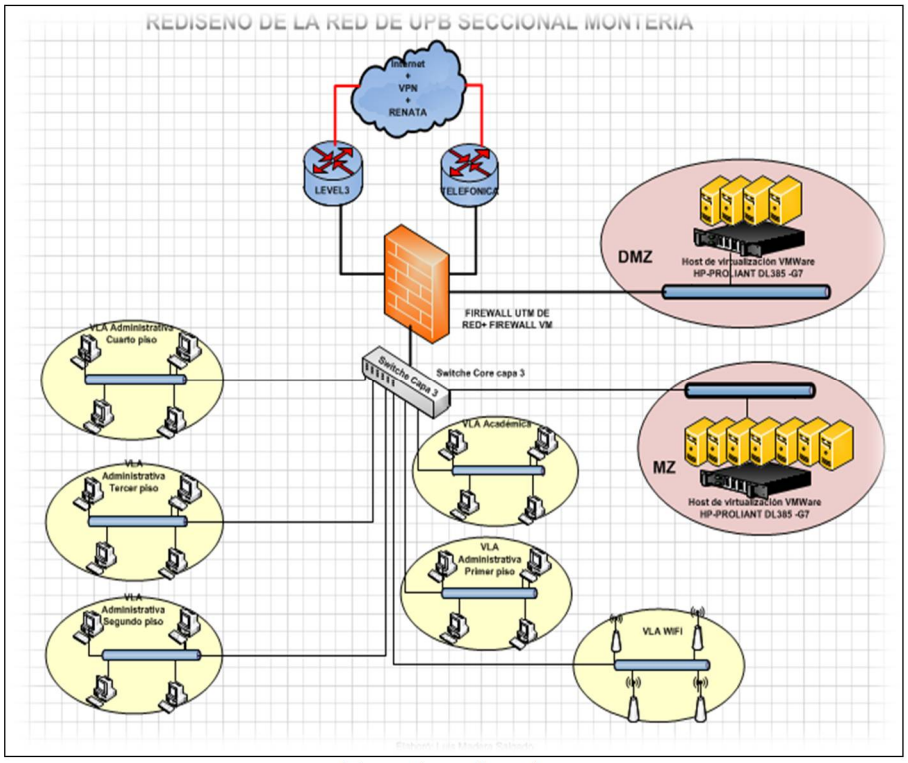


Fuente: el autor

Para hacer una implementación adecuada y eficiente del Firewall de última generación UTM, se propone el siguiente esquema de Red para la UPB Seccional Montería, con el fin de facilitar la gestión centralizada de amenazas y monitoreo eficiente de la Red. Se define una zona desmilitarizada para los servidores que necesitan hacer publicación a Internet, la zona militarizada para servidores con

servicios internos como bases de datos, servidor de aplicaciones, entre otros. La red administrativa se debe segmentar en VLAN por piso, la red académica e inalámbrica en sus VLAN correspondientes. El tráfico de las diferentes VLAN se direcciona a través del Switche Core de capa 3 hacia el Firewall perimetral de protección de la red entrante y saliente. En la Figura 25, se propone el rediseño de la red.

Figura 25. Rediseño de la Red de UPB Montería



Fuente: el autor

En la Figura 25. Rediseño de la red, se incluye el Switche de capa3 administrable, de tal forma que debe permitir configurar las VLAN necesarias para la red. Esta arquitectura facilita el cumplimiento de las políticas de seguridad, el rendimiento de la red y simplicidad de la misma. Como filtro de la red se plantea el Firewall UTM a implementar. El firewall bastión garantiza en un alto porcentaje que los ataques que se sufran de manera externa serán contenidos y repelidos; pero lo más importante alertará al administrador de estos ataques, para tomar acciones de correctivas.

Una vez que se ha definido las políticas y el propósito del firewall, estamos listos para profundizar técnicamente el ambiente del firewall, para lo cual debemos tener en cuenta algo clave, que es la "**Simplicidad**". De tal forma, que se debe tener claro los siguientes requerimientos:

- Filtrado de entrada
- Control de salida
- Cifrado
- Protección contra virus
- Control de Errores.
- Control de uso de aplicativos web
- Sistema de detección y Prevención de intrusiones IPS.

Se implementarán reglas de filtrado de paquetes diseñadas, de acuerdo a la nueva topología y políticas de seguridad. Se mantendrá un control total sobre los protocolos y puertos que se estén ejecutando sobre la red corporativa de UPB Montería.

La red queda conformada por VLANs y zona desmilitarizada con los servicios Web, correo, DNS y servicios de directorio. La zona desmilitarizada es una red que permite el tráfico entre Internet dentro o fuera de la Intranet y al mismo tiempo mantiene la seguridad en la propia Internet.

La conectividad entre los switches de capa 3 se realiza también a través de una VLAN entre ellos. Estos Switches dan un el control de acceso seguro de red, basado en el estándar 802.1x. Además permiten la autenticación de los dispositivos conectados mediante la dirección MAC. Estos switches de capa 3 soportan la definición de redes virtuales (VLANs), y posibilitan la comunicación entre las diversas VLANs, sin necesidad de utilizar un router externo.

Como la red LAN es bastante grande, implementamos los switches de capa 3 para la segmentación de la red, haciéndola más eficiente y segura; estos switches permiten la unión de segmentos de diferentes "*Dominios de Broadcast*". Además la implementación típica de un switche de capa 3 es más escalable que un router, pues éste último utiliza las técnicas de enrutamiento a nivel 3 y repaso a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del switche, aplicando enrutamiento donde sea necesario.

9.1. ESQUEMA DE ASIGNACIÓN IP EN LA SECCIONAL UPB MONTERÍA

Se toma como referencia la red 10.0.0.0/8, que de acuerdo con las recomendaciones para asignación es el mapa a escoger cuando se realiza una segmentación. Ver la Tabla 6. Distribución de IP UPB Montería.

Tabla 6. Distribución de IP UPB Montería

Distribución UPB Montería					
Ciudad	**Campus**	**Mapa**	**Mascara**	**Redes**	**Hosts por subred**
Montería	Principal	10.160.0.0/12	255.240.0.0	16	1.048.574

Fuente: el autor.

Para una segmentación que se adapte a mejores prácticas es necesario no utilizar el primer ni el último segmento, por ende, la tabla anterior excluye dichos rangos. Con el propósito de mantener uniformidad en la asignación de direcciones IP se establecen las siguientes condiciones para la seccional UPB Montería:

- El primer *byte* es fijo, con un valor de 10 (diez en base decimal).
- Se establece el segundo *byte* de la asignación para diferenciar categorías de servicios y equipos.
- El tercer *byte* diferencia ubicaciones o propósitos.
- El último *byte* corresponde a cada usuario final.

Segundo Byte. El segundo *byte* da espacio a dieciséis (16) mapas clase A, de los cuales no se debe usar el primero ni el último, quedando espacio para catorce (14) mapas usables. Para garantizar uniformidad en los campus, este *byte* debe separarse por categorías, que permiten rápidamente establecer el propósito de cada equipo en la red. Permitiendo además una aproximación desde el punto de vista de prioridades de tráfico y/o seguridad, ver la tabla 7. Segundo Byte.

Tercer Byte (Asignación de Reglas de Firewall o VLANs). El tercer *byte* permite separar categorías de equipos, bien sea por su ubicación o por su propósito dentro de la red, otorgando una mayor libertad en la asignación de recursos al administrador de la seccional. Esta separación tiene como propósito permitir un mejor manejo en grupos de seguridad o separación entre *VLAN*, así como una identificación rápida en estructuras de auditoria.

Tabla 7. Segundo Byte

Segundo Byte		
Segmento	**Función para cada segmento**	**Montería**
0	No usado	10.160.0.0
1	Infraestructura de red	10.161.0.0
2	Servidores institucionales	10.162.0.0
3	Servidores de grupos de estudio o dependencias pequeñas	10.163.0.0
4	Servicios de comunicación IP	10.164.0.0
5	Infraestructura de Impresión (servidores e impresoras)	10.165.0.0
6	Equipos de usuarios identificados	10.166.0.0
7	Equipos de usuarios desconocidos (zonas con alta rotación de personal)	10.167.0.0
8	Salas de cómputo	10.168.0.0
9	Controladores de Wireless	10.169.0.0
10	Auditorios, zonas públicas y eventos	10.170.0.0
11	Convenios con externos	10.171.0.0
12	Inteligencia de edificios (CCTV, Control de Acceso, monitoreo ambiental)	10.172.0.0
13	IPTV	10.173.0.0
14	Reserva por definir	10.174.0.0
15	No usado	10.176.0.0

Fuente: el autor.

Teniendo en cuenta que en algunos casos se facilita el separar por bloques, pisos, aulas, u otros criterios de acuerdo a la seccional, se segmenta el tercer *byte* dejando espacio a múltiples categorizaciones. Cada uno de los "mapas" presentes en la Tabla 8. Tercer Byte*,* permite visualizar un segmento de red que se puede asignar bien sea a una VLAN *o a reglas de* firewall*.*

Los principios de diseño de *multilayer networks* indican que la labor de la capa *distribución* es congregar los enlaces hacía el *core* y cuartos de cableado de cada edificio. Por esa razón se establecen direcciones para la infraestructura de red tanto en el segundo como en el tercer *byte*, permitiendo a cada administrador de red establecer su propia estructura nemotécnica para los equipos activos.

Tabla 8. Tercer Byte

Tercer Byte						
Función Tercer Byte	**Valor Inicial Byte**	**Mascara 255.255.192.0**	**Mascara 255.255.248.0**	**Mascara 255.255.252.0**	**Mapas Clase C incluidos**	**IP incluidas**
No usado: Dirección de red.	0		10.x.0.0/21		8	2048
Core Layer	8			10.x.8.0/22	4	1024
Distribution Layer	12			10.x.12.0/22	4	1024
Access Layer (edge, usuarios)	16		10.x.16.0/21		8	2048
Wireless Access Points	24		10.x.24.0/21		8	2048
Separación por nivel de información	32	10.x.32.0/19			32	8192
Información Crítica	36			10.x.36.0/22	4	1024
Información Confidencial	40			10.x.40.0/22	4	1024
Información Privada	44			10.x.44.0/22	4	1024
Información de Uso Interno	48		10.x.48.0/21		8	2048
Información Pública	56		10.x.56.0/21		8	2048
Separación por Unidades Organizacionales	64	10.x.64.0/19			32	8192
Separación por Bloques	96	10.x.96.0/19			32	8192
Separación por grupos académicos	128	10.x.128.0/19			32	8192
Separación por aula	160	10.x.160.0/19			32	8192
Reserva, por definir	192	10.x.192.0/19			32	8192
Conexiones no autorizadas a puntos libres en el cableado	224		10.x.224.0/21		8	2048
Equipos aislados de otras redes	232		10.x.232.0/21		8	2048
Servicios sin firewall	240		10.x.240.0/21		8	2048
No usado: Dirección de broadcast	248		10.x.248.0/21		8	2048

Fuente: el autor.

No es permitido asignar a un equipo direcciones que pertenezcan a otra categoría. En caso de presentarse nuevas categorías no contempladas se recurrirá en primera instancia a los segmentos de “reserva”, en última instancia se recortará uno de los segmentos más amplios.

Cuarto Byte. El último byte distingue a un usuario de otro, dentro de cada dependencia. Para zonas con múltiples grupos de usuarios adscritos a la misma dependencia, se puede segmentar también este valor según la necesidad.
Se sugiere que a las instalaciones temporales le sean asignadas direcciones a partir del 200, de tal forma que la dirección IP acarreé información adicional del estado o derechos de seguridad del usuario.

Disponibilidad de Direcciones. Teniendo en cuenta la segmentación realizada, para cada una de las treinta y dos (32) dependencias que se pueden diferenciar en este esquema, se dispone de doscientas cincuenta y cinco (255) por dependencia.

9.2. ELABORACIÓN DE REQUERIMIENTOS

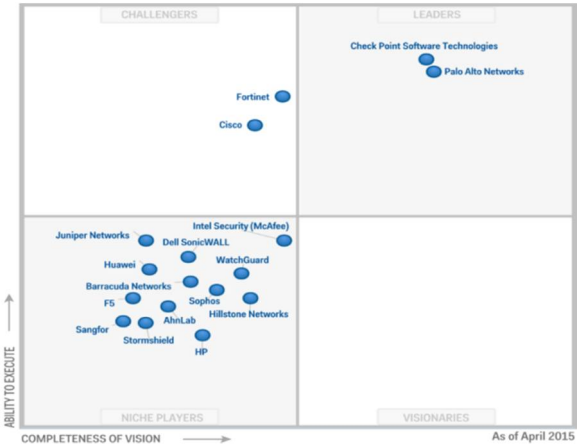
En el Anexo C, se detalla los requerimientos de seguridad, dimensionamiento de tráfico y especificaciones básicas y avanzadas necesarias para la implementación del UTM para la Universidad Pontificia Bolivariana Seccional Montería. Se envía la Invitación a Presentar Oferta (IPO) a diferentes proveedores de tecnologías Palo Alto Networks, Fortinet y SonicWALL.

10. ANÁLISIS DE DIFERENTES TECNOLOGÍAS FIREWALL UTM

Tomando como referencia el análisis de tecnologías Firewall del 2015 presentado en el cuadrante de Gartner[59] (Empresa consultora y de investigación de tecnologías de la información con sede en Stanford Connecticut, Estados Unidos), Se observa cuáles son las tecnologías que están como líderes del sector en lo referente a firewall de próxima generación para empresas. Según lo analizado en Gartner menos de un 40% de las empresas con conexión a Internet tienen en cuenta los Firewall de próxima generación. Según lo analizado por Gartner para el año 2018 esta cifra aumentará en un 85% debido a que las empresas se están dando cuenta de los beneficios de implementación para aplicaciones y el control de los usuarios.

Según Gartner el mercado de los Firewall sigue evolucionando en productos de nueva generación, con nuevas características para mejorar el cumplimiento de las políticas (aplicaciones y usuarios), detectar nuevas amenazas mediante los sistemas de prevención de intrusiones (IPS), el uso de las VPN (Redes privadas virtuales), manejo de servicios web o transferencias de datos seguros o cifrados mediante la utilización del protocolo Secure Sockets Layer (SSL), que en gran medida están en las funcionalidades de los Firewalls. Sin embargo, los Firewall de próxima generación no integran todas las funcionalidades de seguridad de red en un solo equipo o todo en uno como los productos UTM; equipos o tecnología adecuada para pequeñas y medianas empresas. En la Figura 26 siguiente, observamos los firewall empresariales que se encuentran en el cuadrante Mágico de Gartner.

Figura 26. Cuadrante Mágico de Gartner para Firewalls



Fuente: Gartner, (Abril de 2015).

[59] Cuadrante Mágico para Firewalls de Red Empresarial. Recuperado de: https://www.gartner.com/doc/reprints?id=1-2DVI0YW&ct=150422&st=sb

Los Líderes: en este cuadrante están las empresas que crean productos que cumplen con las demandas de las empresas; incluyendo una amplia gama de modelos, soportes de virtualización, capacidad de gestión, reportes y administración a diferentes niveles y simplificación de aplicación de políticas y reglas. Los que están en este cuadrante son los líderes que ofrecen nuevas aplicaciones de seguridad y suministran un buen soporte para evitar vulnerabilidades en sus productos de seguridad.

Los Desafiantes: en este cuadrante están las empresas que han alcanzado un número de clientes importantes pero que no son los líderes en cuanto a las innovaciones o Firewall de próxima generación. Las empresas ubicadas en este cuadrante ofrecen productos con buenos precios debido a la fortaleza de sus números de clientes y su estabilidad.

Los Visionarios: las empresas ubicadas en este cuadrante ofrecen aplicaciones correctas para estar en el mercado, pero les falta número de ventas, estrategias para ventas o factores financieros para competir con los líderes o desafiantes. Las tecnologías ofrecidas por estas empresas tienen productos de nueva generación pero no son fuertes en la capacidad de soporte de redes.

Los jugadores de nicho: en este cuadrante se presentan las empresas con Firewall corporativo, con productos para oficinas que están entrando al mercado.

Gartner incluye las empresas de firewall que cumplen los criterios de Capacidad de competición en el mercado de los firewall, que esas empresas integran listas de ventas, que las empresas productoras tienen presencia a nivel corporativo, la inclusión de sus productos luego del análisis de especialistas de Gartner, que hayan vendido más de diez millones de dólares en sus productos en los últimos años.

Las empresas integradas el cuadrante mágico del mercado de Firewall son las siguientes:

- Check Point Software Technologies
- Intel Security (McAfee)
- AhnLab
- Barracuda Networks
- Cisco
- Dell SonicWALLF5
- Fortinet
- Hillstone Networks
- HP
- Huawei
- Juniper Networks
- Palo Alto Networks

- Sangfor
- Sophos
- Stormshield
- WatchGuard

10.1. ANÁLISIS DE FIREWALL PALO ALTO NETWORKS

La tecnología de Firewall de Palo Alto Neworks[60] es uno de los líderes del mercado según el cuadrante de Gartner, por lo tanto se toma como el primer firewall a evaluar. Se analizará la Serie PA-3000, una de los productos que más se ajusta a nuestros requerimientos de seguridad de aplicaciones, usuarios, contenidos y el desempeño adecuado al requerimiento de nuestro tráfico.

PA-3060. Ofrece las siguientes características:

- Rendimiento de firewall a 4 Gbps (con función App-ID1)
- Rendimiento de la prevención de amenazas a 2 Gbps
- Rendimiento de VPN basada en IPSec a 500 Mbps
- 500.000 sesiones máximas
- 50.000 nuevas sesiones por segundo
- 2.000 interfaces de túnel/túneles de VPN basada en IPSec
- 2.000 usuarios VPN SSL
- 10 enrutadores virtuales
- 1/6 sistemas virtuales (base/máx.2)
- 40 zonas de seguridad
- 5.000 políticas como máximo

La tecnología de Palo Alto Networks se destaca por las siguientes funcionalidades: Detección y decodificación de protocolos de aplicaciones; el firewall decodifica las aplicaciones codificada en la capa de socket seguro SSL, si la regla de política está definida para permitir el tráfico, este se codifica nuevamente y se transmite hacia su destino. Ejemplo Facebook.com

Filtrado URL: basado en listas negras actualizadas el firewall puede restringir o dejar pasar URLs según las reglas definidas de filtrado, pero adicionalmente se puede personalizar las reglas de filtrado de URLs permitiendo accesos a sitios restringidos a usuarios con contraseñas.

Descifrado de protocolos de aplicaciones y firmas de aplicaciones: con el descifrado de aplicaciones el firewall puede establecer si se está aplicando conexiones seguras o no y puede aplicar firmas o certificados digitales para aplicaciones seguras.

[60] Palo Alto Networks. Disponible en Internet: https://www.paloaltonetworks.es/products/platforms/firewalls/pa-3000/overview.html

Análisis heurísticos o de comportamiento: cuando se combina las técnicas de identificación de aplicaciones con descifrado de protocolos y firmas digitales es posibles bloquear múltiples amenazas y además tener un buen control de uso de aplicaciones web.

Prevención de amenazas: El firewall realiza la detección y bloqueos de amenazas, virus, spyware o exploits mediante la utilización de un motor de bases de datos de prevención en tiempo real. Es decir el equipo ofrece gran velocidad de procesamiento que no afecta los tiempos de respuestas aun haciendo el análisis de datos de manera granular.

Visibilidad y control de los usuarios: La tecnología de Palo Alto Networks permite hacer control de uso de aplicaciones, debido que es compatible con la mayoría de los directorios activos conocidos, haciendo control por lo tanto, desde grupos de usuarios configurados en los directorios activos.

Visibilidad y control de contenidos**:** permite hacer control de navegación o bloqueo de contenidos en tiempo real sumando las funcionalidades de control citadas anteriormente. De esta forma se bloquean amenazas al controlar transferencias de archivos y el bloqueo de páginas web no relacionadas con el trabajo.

Aplicación Centralizada de comandos (ACC): presenta una interfaz gráfica que facilita la configuración, la gestión de seguridad y el monitoreo del tráfico de la red de una manera eficiente.

Control y filtrado de archivos y datos**:** los administradores de TI o de seguridad informática pueden aplicar políticas para reducción de riesgos asociados a transferencias de archivos, por tipo de archivos, transferencias de tramas de datos confidenciales y control de transferencias.

Conectividad Segura: cumple las funcionalidades de túneles SSL, VPN extremo a extremo de usuarios y VPN site-to-site; para establecimiento de conexiones seguras con validación de usuario y contraseñas.

La tecnología de Palo Alto Network cuenta con la protección total para IPv6.

Gestión de informes e registros: posee un generador de reportes de análisis de amenazas y vulnerabilidades en tiempo real, facilitando la gestión unificada de amenazas.

Controles basados en políticas: La tecnología Palo Alto Networks permite establecer políticas basado en aplicaciones, que permiten la aplicabilidad de las políticas para los siguientes controles:

- Denegar acceso a la red de determinados tipos de aplicaciones, como por ejemplo peer-to-peer y servicios proxy.

- Permitir accesos a usuarios como se establece en directorio activo.

- Aplicar políticas de uso de aplicaciones Web mail y de mensajería instantánea; inspeccionando virus, spyware y exploits de vulnerabilidades, todo en una sola norma de política.

- Identificar transferencias de información confidencial y bloquear, permitir o enviar alertas acerca de quienes transfieren los datos.

- Aplicar políticas de filtrado Web, además informándole al usuario sobre la opción de continuar navegando en un sitio no seguro.

- Aplicar reglas de filtrado de cortafuegos basadas en el puertos entrantes y salientes combinadas con reglas de filtrado basadas en aplicaciones para facilitar la transición a cortafuegos de última generación.

10.2. ANÁLISIS DE FIREWALL FORTINET

Fortinet[61]. Es otro de los líderes en el mercado de soluciones de seguridad de Firewall UTM, proporciona una amplia protección contra amenazas, es una Appliance de alto rendimiento y simplifica la infraestructura de seguridad para la empresa.

Modelo UTM de Fortinet. La tecnología Fortinet integra una gama de funcionalidades, reduciendo costos a un buen desempeño de protección. Sus funcionalidades corren sobre su sistema operativo FortiOS. FortiOS 5.0 (última versión de FortiOS), introduce nuevas mejoras e innovaciones. Las principales funcionalidades a destacar son:

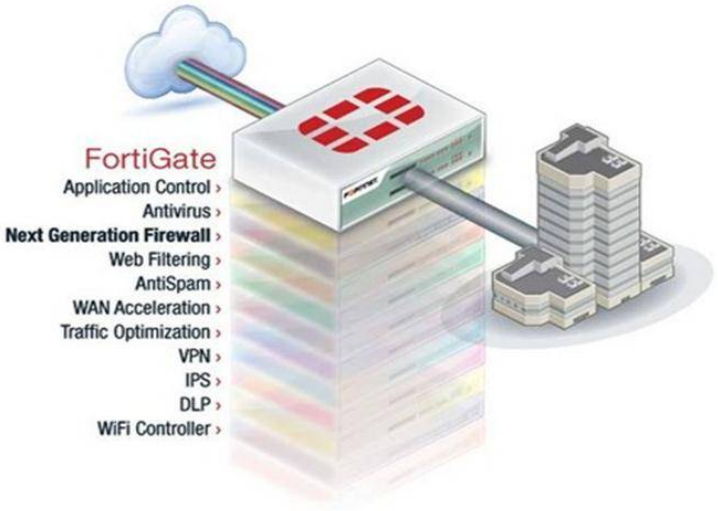
Incorpora un nuevo sistema avanzado anti-malware, nuevo motor heurístico de comportamiento y servicio de antivirus con soporte en la nube.

Mayor control para asegurar dispositivos móviles propios o personales.

Mayor eficiencia con ajustes de políticas basadas en roles para usuarios, ubicación y perfiles de aplicación. La Figura 27, muestra un UTM Fortinet con sus características.

[61] Fortinet. Seguridad y Servicios. Disponible en Internet: www.fortinet.com

Figura 27. UTM Fortinet



Fuente: Fortinet, (2016)

Tecnología y plataformas de Fortinet. Esta tecnología incluye todas las funcionalidades que ofrecen los UTM de nueva generación. El FortiGate se distingue según su capacidad de manejo tráfico y dimensionamiento para la pequeña, mediana y gran empresa. Así, los modelos 30D y 90D son destinados para la pequeña empresa, los modelos 100 y 200 son destinados para la mediana empresa, los modelos 300 y 500 son destinados para sucursales de empresa, desde las series 600 a 900 incorporan velocidades en el orden de 51 Gbps y puertos de 10 Gbps, desde estas series son los Firewall de nueva generación, los modelos 3000 y 5000 son destinados para la gran empresa y Data Center.

La versión FortiGuard ofrece una gran protección de amenazas soportada por grupos de investigación de Fortinet a nivel mundial, incluyendo las funcionalidades de los Firewall de nueva generación, es decir filtrado de puertos, filtrado de aplicaciones y accesos de aplicaciones por perfiles o grupos de usuarios, además las protecciones contra virus, malware, spam, entre otros.

La funcionalidad FortiASICs; permite ejecutar las funciones de seguridad acelerando el procesamiento, ofreciendo de esta forma un desempeño óptimo en manejo de ancho de banda.

Los firewall Fortinet incorporan un sistema operativo llamado FortiOS, que permite hacer todas las funciones de seguridad y redes de una manera centralizada.

Fortinet ofrece también una plataforma en la nube, para la gestión de políticas de seguridad y configuración centralizada, con una capacidad de gestión de 10.000 dispositivos Fortinet. Esta funcionalidad se conoce como FortiManager, FortiAnalyzer y FortiCloud.

La gama de soluciones de Fortinet son: protección de amenazas avanzadas basas en Sandbox o cajas de arena, protección de aplicaciones web, protección de correo electrónico, protección de DDoS, controlador de descubrimiento de aplicaciones, gestión de identidad de usuarios y control de tráfico LAN y WAN.

10.3. CHECK POINT

Check Point Software Technologies Ltda.[62]. Es una empresa proveedora de soluciones de seguridad IT, conocida por sus productos de Firewall de Nueva Generación y VPN.

El Check Point 5600 es un UTM de nueva generación ofrece las funcionalidades de todos los firewall de este tipo, Es un dispositivo optimizado contra amenazas en tiempo real. Con gran capacidad de procesamiento y almacenamiento.

Incorpora un servicio de protección de amenazas basado también en Sandbox y una de sus principales características es la extracción de datos para análisis y entrega limpia de datos a usuarios sin afectar la transferencia de información al usuario final. Es decir, si por ejemplo un correo tiene adjunto un archivo contaminado, este no es bloqueado, sino limpiado y marcado para informar al usuario, pero se realiza la entrega del archivo limpio al usuario final sin afectar los servicios de información o de transferencia o manejo de archivos.

La serie UTM 5600 es un Appliance a la mediana empresa de las amenazas conocidas y desconocidas o de día cero, protección de virus, Bot, emulación de Sandbox o caja de arena y tecnología de extracción de amenazas.

En la siguiente Tabla 9, se detallan las funcionalidades de los Firewalls Check Point NGTP para prevenir amenazas conocidas y los Firewalls NGTX para prevenir las amenazas conocidas y ataques de día cero.

[62] Check Point Software Technologies Ltda. Disponible en internet: http://www.checkpoint.com/products-solutions/threat-prevention/index.html.

Tabla 9. Funciones de TGP y NGTX

	TGTP Prevención de amenazas conocidas	**NGTX** Prevención de amenazas conocidas y ataques del día cero
Firewall	✓	✓
VPN (IPSec)	✓	✓
IPS	✓	✓
Control de Aplicaciones	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Filtrado URL	✓	✓
SandBlast Threat Emulation	×	✓
SandBlast Threat Extraction	×	✓

Fuente: Check Point, (2016)

11. IMPLEMENTAR UN FIREWALL UTM (INIFIED THREAT MANAGEMENT) DE NUEVA GENERACIÓN DE ACUERDO AL ANÁLISIS DE LA TECNOLOGÍA Y VIABILIDAD ECONÓMICA MÁS ADECUADA PARA UPB

En la siguiente Tabla 10, se puede visualizar un resumen comparativo de especificaciones técnicas entre las tres tecnologías de Firewall empresarial que se ajustan a las necesidades de tráfico y seguridad de UPB Montería. Se puede observar que la tecnología de Firewall de nueva generación de Palo Alto Network y Fortinet ofrece toda la gama de servicios de nueva generación incorporados en un mismo equipo o Appliance, es decir incorporan todas las funcionalidades sin necesidad de solicitud de adición de servicios con negociaciones adicionales.

Tabla 10. Comparación entre Firewall de gama media

Características	***Check Point 5600 NGDP***	***Palo Alto LA 3060***	***Fortinet 1200D***
Rendimiento	1,5 Gbps	4 Gbps	3.6 Gbps
IPS Rendimiento (por defecto / Perfil recomendado)	4 / 1 Gbps	4 / 2 Gbps	11 / 6.8 Gbps
Sesiones Concurrentes	3.2 M	500.000	11.000
Máximo de Sesiones por segundo	50 K	50 K	290 K
VLANs	1024	4096	1024 / 512
Firewall	x	x	x
Autenticación por perfil	x	x	x
IPSec VPN	x	500 Mbps	48 Gbps
Advanced Networking y agrupamiento	x	x	X
Mobile Access	x	x	x
Control de Aplicaciones	x	x	x
DLP	x	x	x
Filtrado URL	O	x	x
Antivirus	O	x	x
Anti-Spam & Email Security	O	x	x
Anti-Bot	O	x	x
Administración de políticas de red	x	x	x
Información de accesos de usuarios y estado	x	x	x
Monitoreo	O	x	x
Directorio de Usuarios	x	x	O
Reportes	O	x	x
Administración de políticas de usuario final.	O	5 K	100 K

Fuente: El autor.

Observación: X: cumple la funcionalidad, O: es opcional y se debe contratar el servicio adicional.

11.1. CRITERIOS DE EVALUACIÓN

La evaluación de propuestas tecnológicas se basará en los siguientes criterios:

- Cumplimiento de los requisitos.
- Oferta de valor de la solución.
- Capacidad del proveedor para cumplir o superar los requisitos establecidos en el presente documento.
- Conveniencia del sistema y/o esquema propuesto por el oferente.
- Conveniencia de las sugerencias y recomendaciones de modificación al esquema planteado.
- Presentación de la oferta cumpliendo con el diligenciamiento de los requisitos propuestos y presupuesto.
- Tiempo de implementación.
- Experiencia del proveedor en proyectos similares. Para ello deberá describir brevemente, el objeto del proyecto, la empresa y el contacto avalado para corroborar la información.

Teniendo en cuenta los criterios de evaluación para la UPB seccional Montería; institución educativa sin ánimo de lucros, que encaja en la gama empresarial media por su dimensionamiento de tráfico y número de usuarios y su proyección de crecimiento, procedemos a evaluar tecnologías de firewall UTM de nueva generación destinados a empresas de gama media y que están por lo menos 4 años en el cuadrante de Gartner como soluciones de protección de TI. A partir de un tráfico promedio de datos de entrada y salida de 120 Mbps medido para nuestra institución actualmente, comparamos las diferentes tecnologías de Firewall de nueva generación como son:

- Palo Alto Networks UTM 3060.
- Check Point 5600.
- Fortinet 1200D.

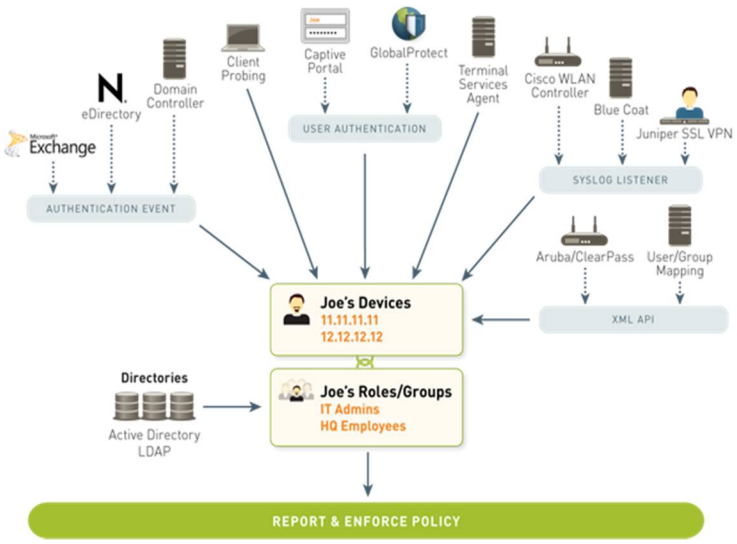
La solución tecnología propuesta por Palo Alto Networks con el **Firewall UTM 3060 de nueva generación** para mediana empresa es la que más características técnicas favorables y funcionalidades de seguridad se ajusta a nuestros requerimientos. Además suministra la solución virtual en VMWARE para protección de servidores virtualizados. Soporta todas las especificaciones y funcionalidades explicadas a continuación.

Los firewalls normales aplican políticas de filtrado basados en puertos y protocolos. Pero con el uso masivo de aplicaciones Web y algunas redes sociales incorporadas

a la empresa, se puede presentar técnicas de evasión de firewall usando túneles de aplicativos que pueden esconder ataques incluso en tráficos cifrados. Por lo tanto, para el administrador de seguridad no puede ejecutar los controles o políticas de filtrado de manera eficiente. La tecnología del Firewall de Palo Alto Networks facilita el control y visibilidad sobre todo el tráfico IP que corre la red, permitiendo identificar las aplicaciones funcionando sobre los puertos, no solo por la detección de los puertos utilizados sino también por la codificación utilizada y técnicas de evasión, ofrece protecciones de ataques escondidos en aplicaciones web en tiempo real, ofrece un ambiente gráfico de gestión de políticas, monitoreo y visualización del comportamiento de la red y ofrece un rendimiento en velocidad de protección en múltiples gigabit sin afectar el funcionamiento de los servicios de red.

Con la funcionalidad de App-ID o identificadores de aplicaciones, puede decodificar los protocolos y codificación utilizada para el análisis o inspección de amenazas y según el cumplimiento de las política de filtrado de usuarios y aplicaciones se deja que siga su curso. (Ver la Figura 28).

Figura 28. APP-ID

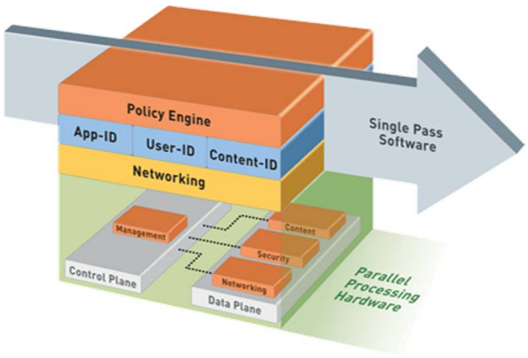


Fuente: Palo Alto Networks, (2016)

Palo Alto Networks[63]. Permite aplicar políticas personalizadas de bloqueo de aplicaciones y de manera granular a través de las funcionalidades de descifrado de protocolos, firmas de aplicaciones, análisis heurístico o de comportamiento de técnicas evasivas incorporadas en algunas aplicaciones web; esta combinación de técnicas de prevención ejercen una protección eficiente en tiempo real de posibles ataques a la red. (Ver Figura 29).

[63] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

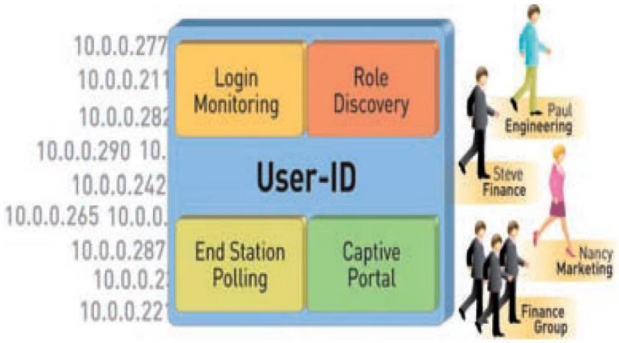
Figura 29. APP-ID



Fuente: Palo Alto Networks, (2016)

La prevención de amenazas se lleva a cabo en tiempo real, permite la visibilidad y control de usuarios cruzando reglas de filtrado por grupos de usuarios y aplicaciones permitidas, el sistema de prevención de amenazas es compatible con los directorios activos configurados. (Ver Figura 30).

Figura 30. User-ID



Fuente: Palo Alto Networks, (2016)

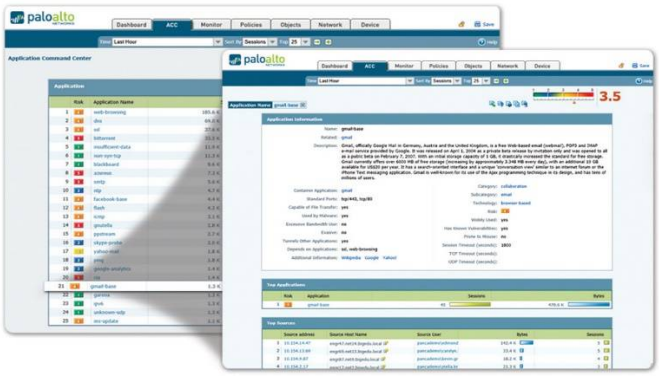
La visibilidad y control de contenidos de la tecnología Palo Alto Networks permite detectar y bloquear en tiempo real amenazas y controlar la navegación por Internet de accesos no relacionados con el trabajo. La identificación de contenidos junto a la identificación de aplicaciones mejora el proceso de prevención y control. (Ver Figura 31).

Figura 31. Contenido-ID

Fuente: Palo Alto Networks, (2016)

La gráfica de centro de comandos, permite monitorear el uso y controlar el comportamiento de la red. (Ver Figura 32).

Figura 32. Centro de comandos



Fuente: Palo Alto Networks, (2016)

Los controles de políticas basados en aplicaciones permiten decidir tratar una aplicación y crear políticas de cortafuegos. (Ver Figura 33).

Figura 33. Controles basado en políticas

Fuente: Palo Alto Networks, (2016)

El modelo de Firewall de nueva generación de Palo Alto Networks PA-3060 posee el dimensionamiento de tráfico que se ajusta a las necesidades de UPB Montería; manejo de tráfico de control de aplicaciones de 4 Gbps, de 2 Gbps para tráfico con firmas digitales y control de aplicaciones, antivirus y antispyware, soporta 500.00 conexiones simultáneas y 50.000 nuevas conexiones. Posee fuente redundante para alta disponibilidad, más 8 interface 10/100/1000 base- TX, 8 de 1 Gbps SFP y 2 interfaces de 1 Gbps de red SFP.

Ofrece en la misma solución un módulo de protección con las mismas funcionalidades de protección que el físico para servicios o servidores virtualizados. Para los diferentes sistemas híper visores de virtualización.

Además de las características de protección generales, el Appliance de nueva generación realiza el reconocimiento de aplicaciones, la identificación de usuarios y el control de manera granular de los permisos.

Palo Alto Networks[64] describe un control de políticas de firewall en ambas soluciones como se describe a continuación:

- Controles por zona de seguridad.
- Controles de políticas por puerto y protocolo.
- Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
- Control de políticas por código de País (Por ejemplo: BR, USA, UK, RUS).
- Control, inspección y descripción de SSL por política para tráfico de entrada y Salida.
- Debe soportar off load de certificado en inspección de conexiones SSL de entrada.
- Debe descifrar tráfico entrante y saliente en conexiones negociadas con TLS.
- Control de inspección y descifrado de SSH por política.
- La plataforma de seguridad debe implementar espejamiento de trafico descifrando (SSL e TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras).
- Es permitido el uso de Appliance externo, específico para el descifrado de (SSL y TLS), con espejamiento de copia del tráfico descifrado tanto para el firewall, como para las soluciones de análisis.
- Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, e reg.
- Traffic shaping QoS basado en Políticas (Prioridad, Garantía y Máximo).

[64] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

- QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
- Soporte a objetos y Reglas IPV6.
- Soporte a objetos y Reglas multicast.
- Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.

La tecnología tiene la capacidad de control de aplicaciones, mediante la identificación de estas independientemente del puerto y protocolo que use. Es decir permite bloqueo o liberación de aplicaciones sin necesidad de bloqueo o liberación de puertos y protocolos. Tienen la capacidad de reconocimiento bittorrent, redes sociales de mensajería instantánea, herramientas de almacenamiento en la nube para ejercer control sobre amenazas incluidas en estas.

Posee la capacidad de verificar no solo el encabezado de paquetes, sino la carga útil o payload con el fin de detectar firmas digitales y servicios de aplicación en los puertos por default y no en puertos no seguros. Incorpora la funcionalidad de detectar técnicas evasivas descifrando el tráfico SSL y SSH con el fin de poder verificar el payload de firmas conocidas por el fabricante. Al verificar la posición en el payload de los paquetes TCP y UDP y la utilización decodificación de por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body, puede controlar técnicas de ataques evasivas escondidas en los cifrados.

Funciona bajo el protocolo IPv4 e IPv6 y puede hacer control de uso de ancho de banda basado en IP de origen, grupo de usuarios y funcionalidades del directorio activo.

La prevención de amenazas en ambas soluciones, posee protección de IPS, antivirus, anti-Spyware, firmas de prevención de intrusos IPS, manejo de excepciones por IP de origen y destino, bloqueos de vulnerabilidades, exploits conocidos, bloqueos de ataques de denegación de servicios, protege de ataques básicos como: Synflood, ICMPflood, UDPfloot, entre otros y los mecanismos de protección de la red con el análisis para anomalías de protocolos, análisis heurístico, desfragmentación de paquetes IP, re ensamblado de paquetes TCP y bloqueo de paquetes mal formados.

La tecnología realiza la inspección de archivos comprimidos de diferentes formatos como Zip, Gzip, entre otros.

El análisis de Malwares modernos en ambas soluciones permite enviar de forma automática archivos transferidos a la nube de análisis de Palo Alto y la local donde se someterá el archivo a simulaciones en un ambiente controlado. El sistema de análisis “In Cloud” o local suministra información sobre las acciones del Malware en

la máquina infectada, informaciones sobre las aplicaciones infectadas que pueden causar la propagación, detecta las aplicaciones no confiables con Malware y genera las firmas de Antivirus y Anti-spyware automáticamente, también marca las URLs no confiables utilizadas por el nuevo Malware y suministra la información necesaria sobre el usuario infectado (su dirección IP y su login de red).

Para el filtrado de URL se puede establecer políticas por tiempo u horario determinado, por ejemplo: día, mes, año, día de la semana y hora. Permite establecer políticas por usuarios, o grupos de usuarios, IPs, redes y segmentos de red de zonas seguras.

Bloquea el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de SafeSearch esté deshabilitada. En este caso informa al usuario el bloqueo dando instrucciones de como habilitar dicha función.
Se permite la identificación de usuarios con políticas basadas en la visibilidad de quien está utilizando las aplicaciones, haciendo uso de la matriz de perfiles de usuarios e identidad de aplicaciones, adicionales a la incorporación de funcionalidades del directorio activo.

Cumple con la calidad de servicios en ambas soluciones para controlar el tráfico de ancho de banda utilizado, por ejemplo cuando se utiliza aplicaciones como YouTube, ustream, entre otras. Por medio de las políticas definidas se controla el máximo ancho de banda a petición de usuarios en el uso de audio y video streaming. El control lo realiza por dirección de origen, dirección de destino, por usuarios o grupos de usuarios, por aplicaciones, por puertos, y garantías de utilización de ancho de banda garantizada, máxima y colas de prioridad.

La tecnología también permite hacer filtrado de datos por extensiones de archivos como MS Office, pdf, entre otros identificados sobre aplicaciones P2P, mensajería instantánea, etc.

Permite la creación de políticas de geolocalización, permitiendo el bloqueo de tráfico de determinado país o países, permite visualizar los logs del tráfico originado o con destino a determinado país, la interfaz gráfica permite crear políticas de regiones geográficas.

La tecnología Palo Alto soporta todos los mecanismos de cifrados normalizados para el establecimiento de VPN en ambas soluciones (Física y para ambientes virtualizados), además ofrece interoperabilidad con VPNs de diferentes fabricantes como Cisco, Fortinet, Check Point, entre otros.

La consola de administración y monitoreo en ambiente gráfico permite hacer una gestión de seguridad eficiente y centralizada, con accesos vía SSH y HTTPS. Permite hacer todas las funciones de configuración, reglas de filtrado o aplicación

de políticas, monitoreos de logs, herramientas de investigación de logs, Debugging, captura de paquetes entre otros.

11.2. ESTUDIO FINANCIERO

Se requiere adquirir el activo de hardware FIREWALL UTM de nueva generación para su implementación e instalación en el área de Data Center de la UPB Seccional Montería. En la tabla 11 se detallaran los costos de instalación de la tecnología Palo Alto PA-3060 propuesta.

En la Tabla 12, se compara los costos de instalación para las tres tecnologías analizadas. La más económica es Check Point pero no detalla la protección de servidores virtualizados y exige adiciones económicas al contrato de implementación y soporte, Fortinet no es factible económicamente, los costos de implementación se desfasan del presupuesto previsto. Se propone implementar Palo Alto Networks PA-3060 por su factibilidad económica, incluye el módulo de protección de virtualización o de servidores virtualizados, el VM-300 sin ningún costo adicional en la propuesta planteada, ofrece mejores especificaciones técnicas de protección, mejor dimensionamiento de manejo de tráfico de la red actual y en crecimiento para los próximos 5 años y no hay exclusión en el soporte.

Tabla 11. Costos de implementación PA-3060

DESCRIPCIÓN	CANTIDAD	VALOR PALO ALTO PA-3060
HARDWARE.		
Palo Alto Network PA-3060.	1	U$ 35.521
SFP+ SR 10GigE Transceptor (PA-7000 series, PA-5060, PA-5050, PA-3060).	2	U$ 2.960
SOFTWARE.		
Suscripción por 1 año de Prevención de amenazas PA-3060.	1	U$ 7.104
Suscripción por 1 año de PANDB filtrado URL, PA-3060.	1	U$ 7.104
Palo Alto Networks VM-300.	1	U$ 5.320
Suscripción por 1 año de Prevención de amenazas VM-300.	1	U$ 1.064
Instalación.	1	U$ 8.574
Mantenimiento o Soporte.	1 año	U$ 8.646
Mantenimiento o Soporte por el proveedor.	1 año	U$ 3.088
Capacitación.	4 horas	Incluida
Project Management.	5 días	Incluida
Subtotal:		U$ 79.382
IVA.		U$ 12.701
Costo Total:		**U$ 92.083**

Fuente: El autor.

Tabla 12. Análisis de costos de diferente Firewall

TECNOLOGÍA	VALOR EN DOLLAR U$
VALOR PALO ALTO PA-3060	**92.083**
VALOR CHECK POINT 5600	**74.992**
UTM Fortigate-1200D	**159.611**

Fuente: El autor.

12. IMPLEMENTACIÓN DEL FIREWALL PALO ALTO NETWOR PA-3060

Para la implementación del Firewall seleccionado y adquirido luego del análisis técnico y financiero, se elabora un plan de trabajo con una durabilidad de 45 días considerando los siguientes destalles de implementación como se evidencia en la siguiente tabla 13 del cronograma de actividades elaborado conjuntamente con el proveedor de Palo Alto Networks[65]:

Tabla 13. Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	TRABAJO	NOMBRE DE RECURSOS
IMPLEMENTACIÓN PALO ALTO	**48.25 días**	**196.75 hrs**	
INICIO	**1.75 días**	**2.5 hrs**	
Presentación de equipo de trabajo	0.25 días	1 hr	COMITE PROYECTO[50%]
Revisión de alcance, compromisos, supuestos	1 día	0.5 hrs	COMITE PROYECTO[6%]
Elaboración y firma de acta de inicio	0.5 días	1 hr	PM[13%],Sponsor[13%]
PLANEACION	**17.5 días**	**15.5 hrs**	
Identificación de recursos	0.5 días	1 hr	PM[25%]
Elaboración y firma de acta de inicio	0.5 días	8 hrs	PM,Sponsor
Elaboración de Cronograma	12 días	2 hrs	PM[2%]
Revisión de Cronograma	4 días	4 hrs	COMITE PROYECTO[13%]
Aprobación de cronograma	0.5 días	0.5 hrs	COMITE PROYECTO[13%]
EJECUCION	**42.6 días**	**160.75 hrs**	
Levantamiento de Requerimientos	17 días	6 hrs	Líder Técnico[4%]
Levantamiento de Información	17 días	6 hrs	Líder Técnico[4%]
Elaboración HLD	**5.5 días**	**14 hrs**	
Consolidar información para configuración	2 días	8 hrs	Líder Técnico[50%]
Arquitectura de solución	2 días	2 hrs	Líder Técnico[13%]
Presentación documento topologia, información de configuración	1 día	2 hrs	Líder Técnico[25%]
Ajustes HLD	0.5 días	2 hrs	Líder Técnico[50%]
HITO - Aprobación HLD	0 días	0 hrs	COMITE PROYECTO

Continúa

[65] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

NOMBRE DE LA TAREA	DURACIÓN	TRABAJO	NOMBRE DE RECURSOS
Elaboración LLD - Perimetral	**6.5 días**	**26 hrs**	
Elaboración de plantilla	4 días	15 hrs	Líder Técnico[47%]
Elaboración Minuto grama	1 día	1 hr	Líder Técnico[13%]
Laboratorio	2 días	8 hrs	Líder Técnico[50%]
Presentación de Plantilla de configuración	0.5 días	2 hrs	Líder Técnico[50%]
HITO - LLD Aprobado	0 días	0 hrs	Líder Técnico
Instalación Física Appliance	**0.7 días**	**2.3 hrs**	
Raqueado	0.5 días	2 hrs	Sponsor[50%]
Alimentación	0.1 días	0.15 hrs	Sponsor[19%]
Verif disponibilidad Conexión interfaces	0.1 días	0.15 hrs	Sponsor[19%]
HITO - Servidor Instalado	0 días	0 hrs	Sponsor
Configuración Firewall Físico	**0.75 días**	**6.15 hrs**	
Aplicación plantilla Appliance	0.5 días	4 hrs	Líder Técnico
Conexión	0.25 días	0.15 hrs	Líder Técnico[8%]
Pruebas de conectividad	0.25 días	2 hrs	Líder Técnico
HITO - Appliance configurado	0 días	0 hrs	Líder Técnico
Ventana 1	**6.2 días**	**11 hrs**	
Gestión de Cambio	2 días	6 hrs	PM[19%],Sponsor[19%]
Presentación ventana a Administradores	0.25 días	1 hr	Líder Técnico[50%]
Ventana	0.5 días	2 hrs	Líder Técnico[50%]
Verificaciones y pruebas	0.25 días	2 hrs	Administradores servicio
Elaboración LLD - FW Servidores	**8.5 días**	**22 hrs**	
Identificar requerimientos y configuración de conectividad FW Virtual	2 días	4 hrs	Líder Técnico[25%]
Elaboración de plantilla	4 días	8 hrs	Líder Técnico[25%]
Laboratorio	2 días	8 hrs	Líder Técnico[50%]
Presentación de Plantilla de configuración	0.5 días	2 hrs	Líder Técnico[50%]
HITO - LLD Aprobado	0 días	0 hrs	Líder Técnico
Instalación Firewall Servidores	**11 días**	**18 hrs**	
Configuración Máquina virtual	4 días	2 hrs	Sponsor[6%]
Instalación Firewall Virtual	2 días	16 hrs	Líder Técnico
HITO - Firewall virtual listo para integrar	0 días	0 hrs	Líder Técnico
Entrega de documentación	0.15 días	0.3 hrs	
Transferencia de conocimiento	1 día	7 hrs	

Continúa

NOMBRE DE LA TAREA	DURACIÓN	TRABAJO	NOMBRE DE RECURSOS
Ventana 2	**6.75 días**	**42 hrs**	
Gestión de Cambio	2 días	32 hrs	PM,Sponsor
Presentación ventana a Administradores	0.25 días	2 hrs	Líder Técnico
Tareas de preproducción	0.25 días	2 hrs	Líder Técnico
Ventana	0.5 días	4 hrs	Líder Técnico
Verificaciones y pruebas	0.25 días	2 hrs	Administradores servicio
Transferencia de conocimiento	**1.15 días**	**7.3 hrs**	
Entrega de documentación	0.15 días	0.3 hrs	
Transferencia de conocimiento	1 día	7 hrs	
CONTROL Y SEGUIMIENTO	45 días	10 hrs	
Reuniones de seguimiento	45 días	10 hrs	
CIERRE	3 días	8 hrs	
Documentación de Cierre	2 días	6 hrs	
Reunión de Cierre	1 día	2 hrs	

Fuente: El autor

12.1 REQUERIIENTOS

El firewall Appliance requiere de los siguientes elementos de instalación: alimentación: 100-240VAC (50-60Hz), corriente máxima: 2A@100VAC, espacio en Rack: -1U, 19” standard rack (1.75”H x 17”D x 17”W), conectividad: Cableado UTP necesario, temperatura de operación: 32 to 122 F, 0 to 50 C, temperatura no operacional: -4 to 158 F, -20 to 70 C.

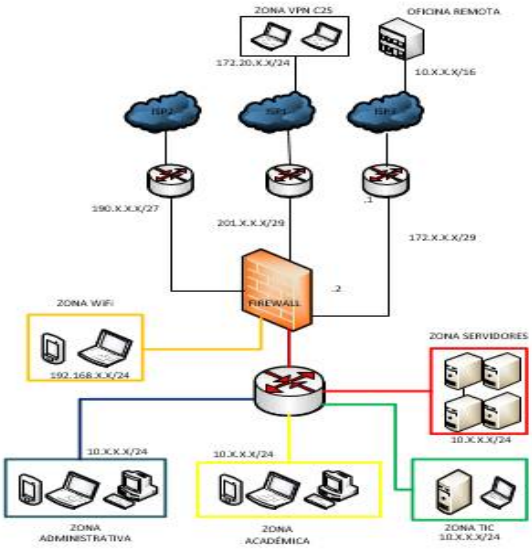
12.2 DISEÑO Y ARQUITECTURA DE LA SOLUCIÓN

La solución de seguridad de firewall adquirida por la Universidad Pontifica Bolivariana seccional Montería consta de un equipo NGFW Palo Alto PA-3060 y un VM-300. El dispositivo PA-3060 queda configurado como Gateway de las redes de la sede Montería, mientas que la máquina virtual VM-300 está como respaldo en caso de un fallo físico del PA-3060.

12.3 DISEÑO LÓGICO

A continuación en la figura 34, se presenta el diagrama de red lógico final del firewall que se debe implementar en la infraestructura de red de la UPB seccional Montería, desde la perspectiva del firewall:

Figura 34. Diseño Topológico

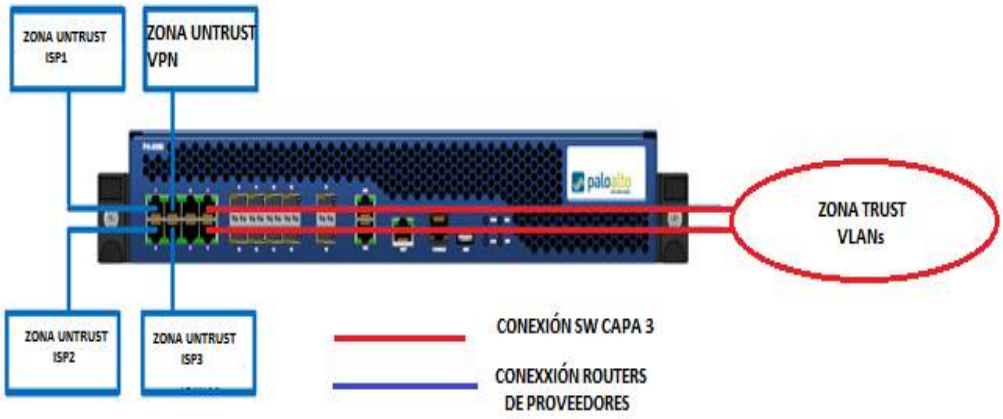


Fuente: El autor

12.4 DIAGRAMA DE CONEXIONES

A continuación se presenta el diagrama de conexiones físicas desde la perspectiva del Firewall Palo Alto. Básicamente se compone de interfaces tipo Trunk las cuales en su mayoría sirven de default Gateway de las diferentes redes, de esta manera el Firewall ejerce un control sobre los paquetes en tránsito en las diferentes zonas. Ver figura 35.

Figura 35. Diagrama de conexiones



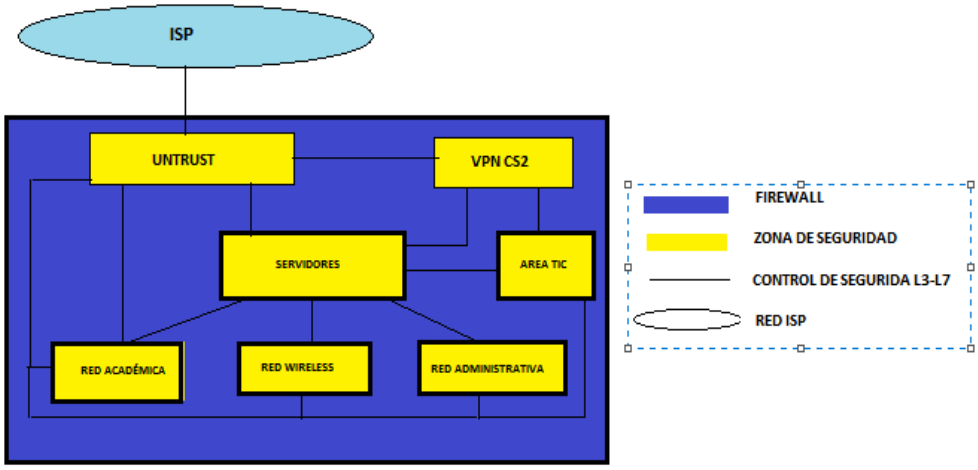
Fuente: El autor

12.5 ARQUITECTURA DE SEGURIDAD

Según como lo explica Palo Alto Networks[66]; para la implementación se han creado varias zonas dependiendo del tráfico a manejar en cada una de ellas. La caracterización del tráfico por zonas permite a los firewall de nueva generación establecer controles en capa de transporte, en capa de aplicación del modelo OSI y a su vez controles por usuarios. Posterior a la validación de esos controles el firewall desempeña validaciones más específicas del tráfico como lo es el IPS y el filtrado de URL para la prevención de amenazas y el uso inadecuado de la red. A continuación se muestra gráficamente la distribución de zonas de seguridad entre los diferentes Firewalls virtuales, de esta manera ilustramos los puntos de control que se mantienen en el firewall de forma que sea entendible para su administración.

A continuación en la figura 36 se pueden apreciar las diferentes zonas de seguridad provistas en el firewall:

Figura 36. Arquitectura de seguridad



Fuente: El autor

12.6 PERFILES DE SEGURIDAD

Por medio de los perfiles de seguridad el Firewall Palo Alto realiza inspecciones sobre el tráfico en búsqueda de intrusos (IPS), malware (virus-spyware, sandbox) y accesos no deseados a sitios web (Filtro URL).

[66] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

A continuación encontramos el detalle de cada uno de los perfiles de seguridad aplicados para tráfico inter-zonas según recomendaciones de Palo Alto Networks[67]:

Antivirus: Se crea un perfil llamado AV_Profile, este perfil usa la configuración por defecto de Palo Alto para detener virus en la red. Se recomienda mantenerlo tal cual como está configurado y aplicado a todas las reglas del equipo.

Anti-spyware: Se crea un perfil llamado AS_Profile, este perfil resetea las conexiones que se detecten como spyware. Se recomienda mantenerlo tal cual como está configurado y aplicado a todas las reglas del equipo.

Vulnerabilidad: Se crea un nuevo perfil llamado Vuln_Profile, este perfil reinicia la conexión del lado del servidor y del cliente cuando se identifica una vulnerabilidad alta o critica, de lo contrario se generará una alerta, según recomendaciones del fabricante. Se recomienda mantenerlo tal cual como está configurado y aplicado a todas las reglas del equipo.

Filtrado de URL: Se crea el perfil URL_Profile según lo verificado por la UPB Montería.

File blocking: Se crea el perfil VISIBILIDAD, el cual genera un log por cada fichero que ve pasar.

Análisis Wildfire: Se crea un perfil WF para que se realice el envío de todos los ejecutables no registrados previamente a la nube y sean analizados. Esto según la guía de buenas prácticas.

Data Filtering: Se crea el perfil DF_Profile, para la identificación de archivos que tengan números de tarjetas de crédito, según recomendaciones del fabricante. Se recomienda mantenerlo tal cual como está configurado y aplicado a todas las reglas del equipo.

12.7 RECOMENDACIONES GENERALES

Durante la administración de la solución se debe tener en cuenta que durante la creación de las reglas de seguridad en el firewall Palo Alto se debe optar por relacionar las aplicaciones en vez de los servicios o protocolos según Palo Alto Networks[68]:

- Se recomienda al administrador realizar una migración paulatina de todas las reglas de acceso externo (Remote desktop, teamviewer, logmeein, etc.) hacia conexiones VPN Client to Site.

[67] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp
[68] PALOALTO NETWORKS. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

- Limitar los accesos entre y hacia las zonas de servidores, a las aplicaciones requeridas.
- Generación de reportes periódicos de tráfico y amenazas por parte del administrador donde se pueda identificar consumos de ancho de banda anormales, prevenir la saturación de los recursos de red y mitigar las amenazas.
- Los certificados digitales que emplea la plataforma se han creado con una expiración de 3 años, por tanto es importante que previo a esta fecha de caducidad este certificado sea cambiado por un nuevo certificado.
- Estar atentos a los comunicados y alertas de Palo Alto sobre actualización en sus firmas y vulnerabilidades de plataformas, es muy importante estar atentos a estos comunicados y tomar los correctivos respectivos de ser necesarios.

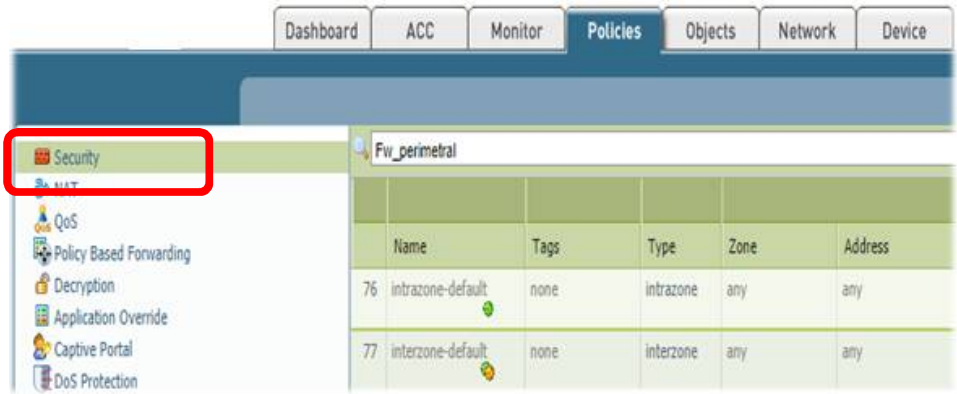
12.8 CREACIÓN DE REGLAS DE SEGURIDAD

Previamente a la creación de las reglas de seguridad se deben conocer los puntos finales del tráfico y las zonas de seguridad que interactúan. Se pueden agrupar usuarios, grupos de usuarios, puntos finales, IP, subredes, rangos de IP y zonas que requieran de las mismas aplicaciones o servicios.

A continuación se describen las recomendaciones para la creación de reglas de seguridad elaboradas para la institución:

Para la creación de las reglas de seguridad se debe acceder a la pestaña **“POLICIES”** y al vínculo **“security”**, luego agregar una nueva regla con el vínculo **“Add”**. Ver figura 37.

Figura 37. Creación de reglas de seguridad



Fuente: Autor

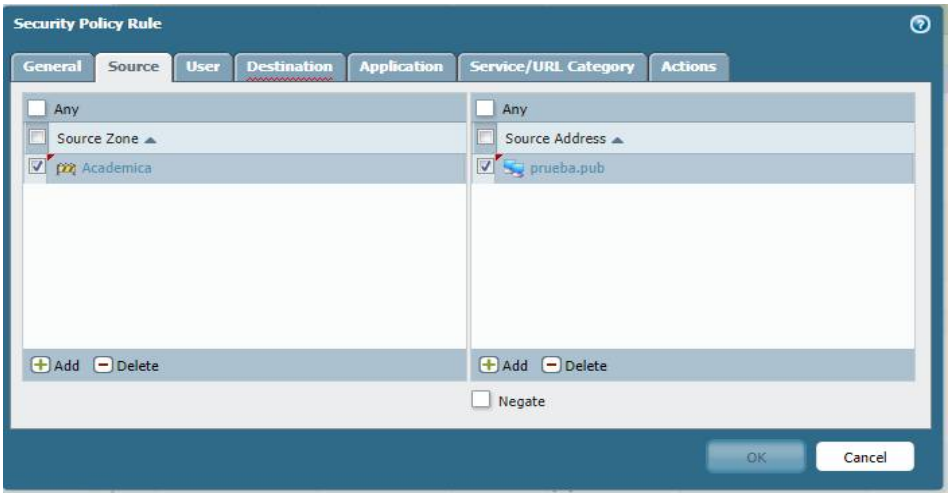
En la pestaña “**General**” agregar un nombre que describa brevemente el propósito de la regla, agregar una descripción detallada y por ultimo una etiqueta “**Tag**” que permitirá diferenciar el tipo de reglas (Por ejemplo: “Internet, DMZ, Usuarios”). Ver figura 38.

Figura 38. Pestaña General

Fuente: Autor

La pestaña “**Source**” permite ingresar a la regla el origen u orígenes del tráfico. Se debe tener en cuenta limitar el tráfico de origen a las zonas y puntos finales (**end points**) evitando seleccionar las opciones “**Any**”. Ver figura 39.

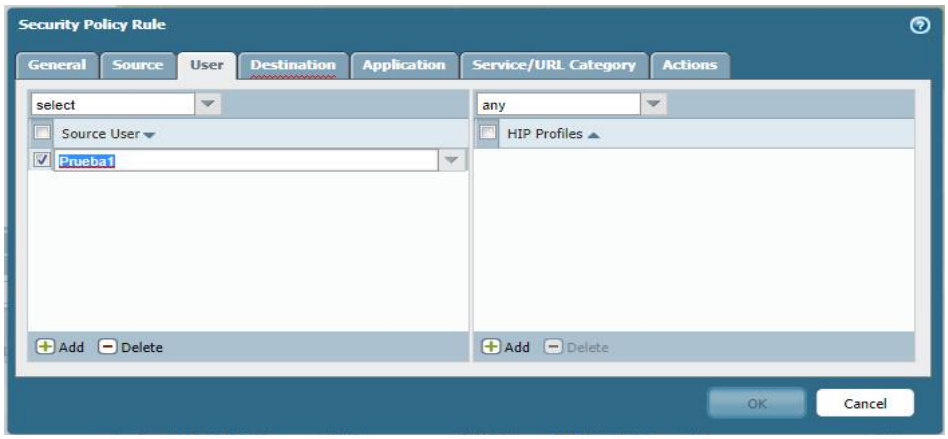
Figura 39. Pestaña Source



Fuente: Autor

Para un control más granular es posible agregar a la regla de seguridad usuarios o grupos de usuarios de un directorio. Para ello seleccionar “**select**” de la lista desplegable y agregar los usuarios a la regla. Ver figura 40.

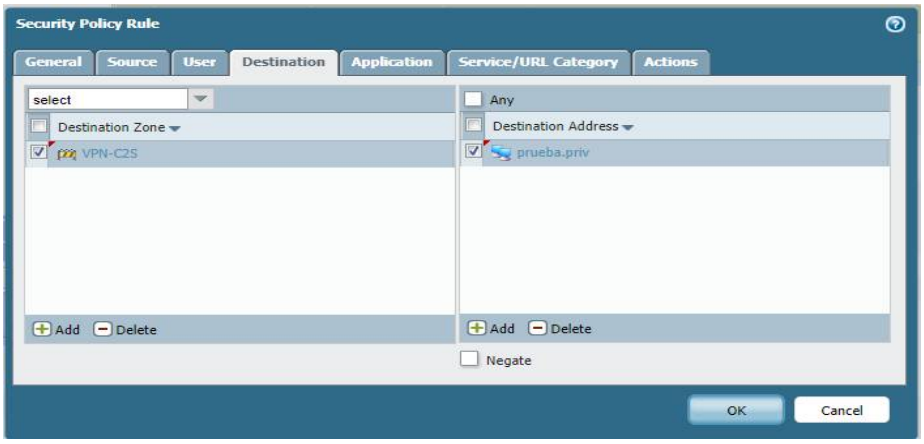
Figura 40. Pestaña User



Fuente: Autor

Al igual que la pestaña "**Source**", la pestaña "**Destination**" debe limitarse al punto o puntos finales de la comunicación deseada, evitando en lo posible seleccionar "**Any**". Dentro de la lista desplegable también es posible el empleo de **multicast** para las aplicaciones que lo requieran. Ver figura 41.

Figura 41. Pestaña Destination



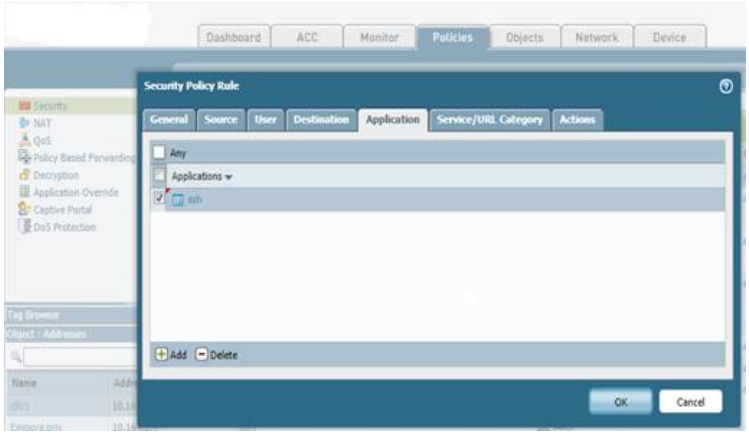
Fuente: Autor

La pestaña de aplicaciones nos permitirá agregar las aplicaciones, grupos de aplicaciones o filtros de aplicaciones que se desean permitir. Al igual que para describir los puntos finales de la comunicación, para las aplicaciones se recomienda permitir las aplicaciones estrictamente necesarias evitando el uso de la opción **"Any".**

El uso de la opción **"Any"** se debe limitar a resolución de problemas y como primera medida para permitir e identificar el tráfico de aplicaciones desconocidas, una vez

se identifica la aplicación se debe permitir su uso exclusivo en la regla. Ver figura 42.

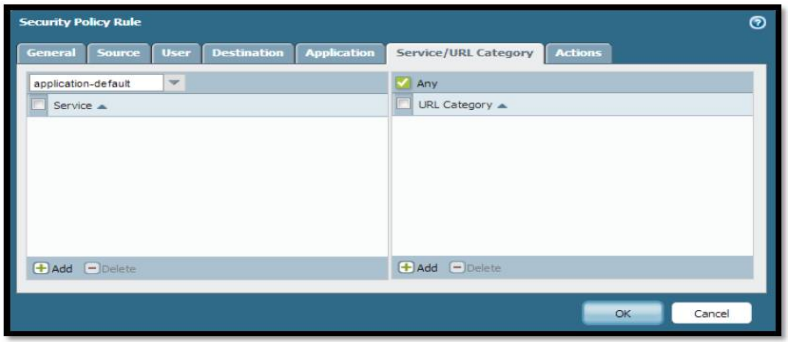
Figura 42. Pestaña Aplication



Fuente: Autor

La pestaña "***Service/URL Category***" permite ingresar los puertos por los cuales las aplicaciones se comunican y limitar los destinos a URL específicas. Se recomienda que en lo posible se haga uso de la opción "***application-default***" dentro de la lista desplegable, para permitir exclusivamente los puertos estándar por aplicación. Ver figura 43.

Figura 43. Pestaña Service/URL category

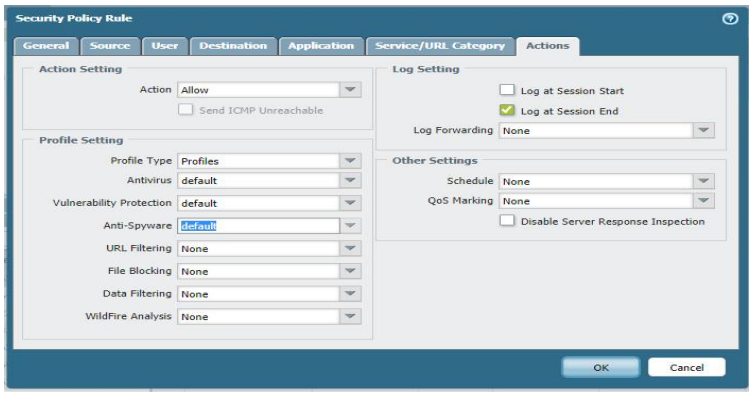


Fuente: Autor

Las acciones a tomar con el tráfico descrito en la regla de seguridad se seleccionan aquí. Se debe seleccionar si se quiere permitir o denegar el tráfico. Se recomienda la selección **"Log at Session End"** exclusivamente y solo seleccionar **"Log at Session Start"** para realizar troubleshooting.

En esta pestaña también podemos incluir los perfiles de seguridad deseados, programar los horarios en que la regla está activa, uso de calidad de servicio (QoS) y deshabilitar la inspección de la respuesta **"Disable Server Response Inspection"**. Esta última opción se recomienda habilitar para comunicaciones donde el destino es confiable. Ver figura 44.

Figura 44. Pestaña Action



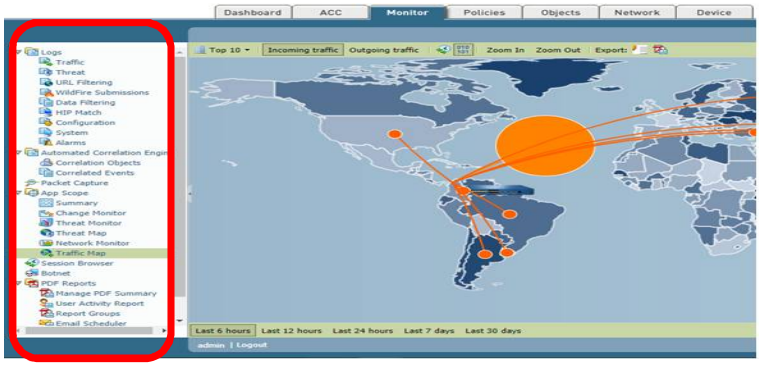
Fuente: Autor

12.9 MONITOREO DE SERVIDORES

La protección para los servidores (web, bases de datos, etc.) en una organización no solo se limita a la creación de reglas de seguridad descritas previamente. Se debe tener un monitoreo constante de los log de Tráfico y Amenazas con el fin de identificar a tiempo las posible brechas de seguridad que puedan estar siendo usadas con propósitos criminales.

La pestaña **"Monitor"**, permite la extracción de la información requerida por el administrador de seguridad para identificar las amenazas latentes en la red. Ver figura 45.

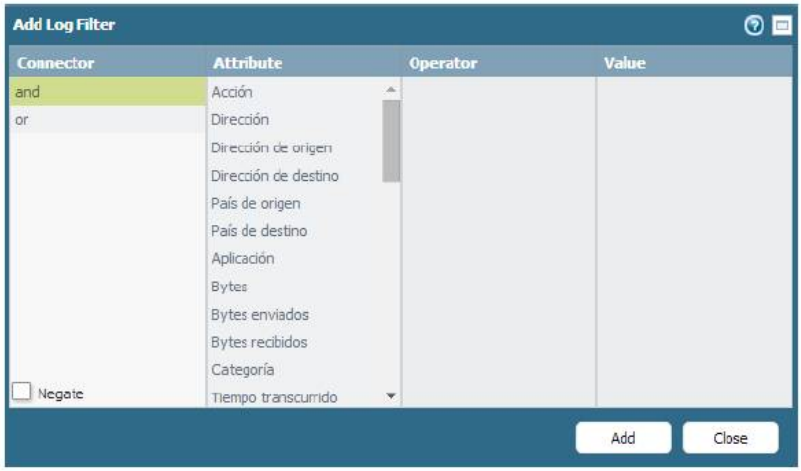
Figura 45. Monitoreo de la red



Fuente: Autor

Para realizar el filtrado en el log de Tráfico o amenazas, se deben añadir mediante el botón con símbolo de suma (+), los filtros que describan los puntos finales del tráfico que se quiere monitorear. Por ejemplo se puede agregar la IP destino de un servidor web para validar el tráfico entrante desde internet. Ver figura 46.

Figura 46. Filtrado de log de tráfico



Fuente: Autor

13. PROPUESTA DE POLÍTICAS Y REGLAS DE FILTRADO PARA EL GESTOR UNIFICADO DE AMENAZAS, CON BASE A LOS HALLAZGOS O NOTIFICACIONES DE LOS REPORTES GENERADOS POR EL UTM

Se plantea el mejoramiento de las reglas de filtrado actuales limitadas por la tecnología usada hasta el momento por las siguientes reglas factibles de implementar con la implementación del firewall Palo Alto Network PA-3060 y VM-300 como se listan a continuación:

- Denegar el acceso a la red a determinados tipos de aplicaciones, como peer-to-peer o (Proxy bypass) y servicios proxy externos.
- Asignar aplicaciones a los grupos de usuarios tal como se definen en el directorio activo lógico para nuestros usuarios. (Acceso solo al sistema financiero, de gestión humana y académico al personal administrativo con perfiles de usuario y contraseña asignado).
- Se permitirá solo la plataforma de correo Outlook corporativo para el personal administrativo, office 365 para estudiantes y académicos y la mensajería instantánea Skype empresarial para personal administrativo bajo el control de acceso con las cuentas de usuarios del directorio activo lógico.
- Para el personal administrativo funcional (Tesorería, registro, liquidaciones, cartera y contabilidad) se restringe el acceso a redes sociales.
- Solo al personal de la red académica se le permitirá acceso a las redes sociales conocidas y manejo de multimedia por YouTube a contenidos permitidos.
- Identificar la transferencia de información confidencial y bloquear, permitir o enviar alertas acerca de quién transfiere los datos.
- Bloquear las páginas de listas negras que incorpora la BD de Palo Alto networks y aplicar el filtrado de URL que bloqueen el acceso a páginas no relacionadas con el trabajo del personal administrativo, supervisar las páginas cuestionables y “controlar” el acceso a otras dándole al usuario la opción de continuar después de una advertencia inicial.
- Archivos binarios. Se debe bloquear la descarga en la red administrativa de archivos ejecutables con extensiones: .bat, .com, .exe, .sys, .vbs.
- Archivos multimedia. Se debe bloquear la descarga de archivos relacionados con audio y video para la red administrativa funcional: .aiff, .avi, .dif, .divx, .mov, .movie, .mp3, .mpeg, .mpv2, .ogg, .qt, .wav, .wma, .wmf, .wmv.
- Archivos comprimidos. Se debe bloquear a la red administrativa funcional la descarga de archivos comprimidos conteniendo otros archivos como: .bin, .bz2, .cab, .cdr, .dmg, .gz, .hqx, .rar, .sit, .sea, .tgz, .zip.
- Crear normas de cortafuegos basadas en el puerto entrante y saliente combinadas con normas basadas en aplicaciones para facilitar la transición a un cortafuego de última generación. Aceptar los puertos: 8080, 443, 53, 80,22, 993,995.
- Permitir solo el acceso remoto al personal del CTIC a través de SSH, FTP y RDP.

14. RESULTADOS E IMPACTO ESPERADO

14.1 RESULTADOS ESPERADOS

La red corporativa de UPB seccional Montería, presenta un grado de complejidad para la administración y control de seguridad, debido a que está diseñada en infraestructuras separadas de conectividad para la red académica y administrativa, adicionalmente no se hace un buen manejo de los ancho de banda contratados porque no hay la infraestructura adecuada de un UTM que realice funciones de seguridad a alto nivel y de balanceo o distribución de tráfico para un mejor rendimiento de la red. Por lo tanto luego del análisis tecnológico de tecnologías de seguridad y la viabilidad económica se propone a la alta dirección la implementación de Firewall UTM de nueva generación como mecanismo de seguridad de la red corporativa y de servicios virtualizados de UPB Seccional Montería.

Resultado 1: Informe ejecutivo de viabilidad técnico-económica, ver anexo E; que permita a la alta dirección tener conciencia en las necesidades de protección de las tecnologías de Información, el Sistema de Información de la institución y la protección de los datos a través de la implementación de Firewall UTM de nueva generación propuesta (Palo Alto Networks PA-3060).

Formular un precedente a la alta dirección con respecto a los hallazgos encontrados, producto de las pruebas de seguridad ejecutadas con un UTM en demostración, donde se evidencian 1.880 incidentes críticos escaneados durante una semana de prueba, según se evidencia en el anexo D, como son: actividades maliciosas de la red, respuestas maliciosas de DNS, acceso a sitios conocidos con Malware, virus, Phishing contra correos, Bots, entre otros. Esto demuestra la necesidad urgente de implementación de un Firewall de nueva generación para la seguridad informática perimetral y de servidores virtualizados.

Luego de la implementación del Firewall Palo alto PA-3060, se evidencian resultados positivos de control y uso eficiente de tráfico de red interno y externo, control y prevención de amenazas, bloqueos de páginas maliciosas y no permitidas, bloqueos de malware, virus, bots de niveles de amenazas críticos, altos, medios y bajos, como evidencian en el anexo F.

El tráfico de red mejora su velocidad de descarga en promedio por encima del 50%, el mayor tráfico hacia de la red es desde la inalámbrica en 13.4GB por día y alcanza picos hasta 706GB por mes, le sigue el tráfico desde la red académica hacia Internet con picos de 5.5GB y tráfico hacia servidor Moodle de 606 MB.

En el mismo anexo F. Se evidencia vulnerabilidades al mes de 73.87KB, de escaneo de hosts de 50.97KB, de Spyware de 1.29KB, de virus 110KB, que son controlados y bloqueados.

Resultado 2: Formulación o modificación de las políticas de seguridad informática de la institución. Con directrices consulta, socialización e implementación de procedimientos de prevención y mitigación de los riesgos informáticos.

Resultado 3: Procedimientos de seguridad a partir de las políticas establecidas. No basta con implementar un dispositivo tecnológico de seguridad informática, sino la formulación de procedimientos de seguridad en cumplimiento de las políticas establecidas.

14.2 IMPACTO ESPERADO

Concientizar a la empresa sobre la necesidad de establecer mecanismos de protección y prevención de posibles ataques informático a nuestra red, con el riesgo de pérdida de información, pérdida de la confidencialidad e integridad de la información y riesgo en la continuidad del negocio.

La necesidad urgente de implementación del Firewall de nueva generación. Con la tecnología Palo Alto Networks se puede alcanzar las mayores fortalezas de seguridad, debido que cumple con todas las funcionalidades de seguridad de la información y los elementos para prevención contra ataques informáticos.

Mayor control sobre aplicaciones. Los mayores ataques informático actualmente se realiza a través de software, también es donde más se detecta huecos de seguridad.

Mayor eficiencia en el manejo de ancho de banda de la red; puesto que se puede controlar el tráfico a través de matrices de perfiles usuarios, identidad de aplicaciones y filtrado de contenidos, entre otros.
Cumplir con los requerimientos de ley en la protección de los datos personales y confidencialidad de la información.

Con la implementación de la tecnología de seguridad se proyecta tener mitigado los riesgos de seguridad informática y alcanzar una utilización para la seccional durante los próximos 5 años.

CONCLUSIONES

Se logró implementar el Firewall UTM de nueva generación para UPB seccional Montería de acuerdo al análisis de la tecnología y viabilidad económica más adecuada para UPB seccional Montería.

Para la implementación se logró luego identificar la infraestructura de la red institucional de la UPB Montería y el análisis de vulnerabilidades de la red. La red de UPB Montería solo estaba segmentada a nivel físico en tres segmentos de red (Administrativa, académica y de WiFi); este tipo de segmentación afectaba el rendimiento de la red por el exceso de broadcast por segmento y de difícil control de tráfico y filtrado de contenidos de la red y de puertos. De acuerdo a las fundamentaciones teóricas y recomendaciones de uso de las mejores prácticas en seguridad informática, se logró segmentar la red de datos institucional en VLAN de acuerdo a áreas funcionales y pisos de la institución; logrando un mejor desempeño de la red de datos, menos inundaciones de broadcast, por lo tanto un mejor rendimiento de ancho de banda y mejor seguridad de red por el uso adecuado de las VLAN. De esta manera se preparó la red de datos para que en la implementación de un Firewall de nueva generación se pueda aplicar correctamente las reglas de filtrado no solo basadas en puertos, sino también en filtrados de contenidos y perfiles de tráfico de acuerdo a perfiles de usuarios.

Con la implementación del Firewall propuesto de tecnología Palo Alto Network PA-3060 se logró minimizar los riesgos de las vulnerabilidades halladas y reportadas por el UTM, se mejoró el rendimiento de la red como se visualiza en los anexos, se logró el control de virus y amenazas, mejoró la alta disponibilidad del tráfico de Internet por la funcionalidad de balanceo de carga (En conexión con dos proveedores, se enruta el tráfico por uno de los dos operadores en caso de fallos de un operador de conectividad de Internet) y en definitiva se garantiza la disponibilidad, la confidencialidad y la integridad de los datos para el sistema de información de UPB seccional Montería.

Se logró aplicar las propuesta de políticas de reglas de filtrado con base a las notificaciones de los reportes generados por el UTM. Una vez implementadas las reglas de filtrado hay un mejor control de páginas web y contenidos web no permitidos para estudiantes, mejorando la disponibilidad y desempeño de la red por el control de virus, spam y malware de red destinada a salas de informática, laboratorios y Wifi.

RECOMENDACIONES

Se recomienda mantener el pago de soporte de actualización y mantenimiento para el Firewall PA-3060 anualmente al fabricante y canal de soporte de Palo Alto Network, para garantizar las actuaciones o parches en línea de prevenciones contra nuevas amenazas y vulnerabilidades.

Se recomienda tener personal dedicado solo a la seguridad informática, debido a los requerimientos de administración y monitoreo constante de la red para minimizar de mejor manera los riesgos.

Se debe capacitar el personal de infraestructura y seguridad informática en la nueva tecnología de Firewall de nueva generación adquirida.

BIBLIOGRAFÍA

CABALLERO, María; CILLEROS, Diego y SHAMSAIFAR, Abtin. El libro del Hacker. Madrid: Ediciones Anaya Multimedia, 2015. 534p. ISBN: 978-84-415-3600-5.

CASTELLANOS, Tache y GÓMEZ, Lucero. Seguridad en redes telemáticas. McGraw-Hill, Madrid: 2006. 549p.

GARCÍA, Jean; FERNÁNDEZ, Yago; MARTÍNEZ, Rubén; OCHOA, Ángel y RAMOS, Antonio. Hacking y seguridad en internet. Bogotá: Ediciones de la U, 2013. 586p. ISBN: 978-958-762-080-1.

HERRERA, Jordi; GARCÍA, Joaquín y PERRAMÓN, Xavier. Aspectos Avanzados de Seguridad en Redes [en línea]. Barcelona: Universidad Abierta de Cataluña, 2004. 292p. Jul. 2004.

WEBGRAFÍA

ALCALDÍA DE BOGOTÁ. Ley 527 de 1999 nivel nacional. Diario Oficial 43.673 del 21 de agosto de 1999 [en línea]. 2017. [Consultado mayo 15 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. 16 p.

…….. Ley 1273 de 2009 nivel nacional. Diario Oficial 47.223 de enero 5 de 2009 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. 5 p.

..... Ley 1581 de 2012 Nivel Nacional. Diario Oficial 48587 de octubre 18 de 2012 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. 15 p.

CHECK POINT. Threat-prevention [en línea]. 2016. [Consultado 5 de mayo de 2016]. Disponible en Internet: http://www.checkpoint.com/products-solutions/threat-prevention/index.html.

DELL. SonicWALL Security Products [en línea]. 2016. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://www.sonicwall.com/us/en/

DE MOYA, Renie. Proyecto factible: una modalidad de investigación [en línea]. 2002. Venezuela. Universidad Pedagógica Experimental Libertador. [Consultado 5 de abril de 2016]. Disponible en Internet: http://www.redalyc.org/pdf/410/41030203.pdf

ENDIAN – UTM [en línea]. 2016. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://www.endian.com/

FLÓREZ R., Wilmar; ARBOLEDA S., Carlos y CADAVID A., John. Solución Integral de seguridad para las pymes Mediante un UTM [en línea]. Medellín. jun. 2012. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

GARTNER. Cuadrante Mágico para Firewalls de Red Empresarial [en línea]. 2015. [Consultado 9 de abril de 2016]. Disponible en Internet: https://www.gartner.com/doc/reprints?id=1-2DVI0YW&ct=150422&st=sb

GUERRA, Cristian. Implementación de una red segura para los laboratorios del DEEE utilizando un dispositivo UTM [en línea]. Tesis de pregrado. Sangolquí: Escuela Politécnica del ejército. Departamento de Eléctrica y Electrónica, 2011. 149p. 2011. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://repositorio.espe.edu.ec/handle/21000/4741

HERRERA, Jordi; GARCÍA, Joaquín y PERRAMÓN, Xavier. Aspectos Avanzados de Seguridad en Redes [en línea]. Barcelona: Universidad Abierta de Cataluña, 2004. 292p. Jul. 2004. [Consultado 3 de marzo de 2016]. Disponible en Internet: http://es.slideshare.net/josealbertonohnoh/aspectos-avanzados-de-seguridad-en-redes-43161221?qid=a0f83c71-b443-4158-ade5-599ebef6bc7d&v=&b=&from_search=22

ISO 27000.ES:2013. El portal de ISO 27001 en español. 2013. [Consultado 14 de mayo de 2016]. Disponible en Internet: http://www.iso27000.es/sgsi.html.

KIOSKEA.NET. Firewall [en línea]. Junio de 2014. [Consultado 14 de marzo de 2016]. Disponible en Internet: http://es.ccm.net/contents/proteccion-2675306562#590

Línuxsecurity.com. [en línea]. 2016. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://www.linuxsecurity.com/

PARRAGA NÚÑEZ, Víctor. Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de ingeniería de sistemas computacionales. Tesis de pregrado [en línea]. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas, 2014. 259p. Dic. 2014. [Consultado 13 de febrero de 2016]. Disponible en Internet: http://repositorio.ug.edu.ec/bitstream/redug/6672/1/TesisCompleta-536-2014.pdf

PALO ALTO NETWORKS. Firewall PA-3000 [en línea]. [Consultado 5 de mayo de 2016]. Disponible en Internet: https://www.paloaltonetworks.es/products/platforms/firewalls/pa-3000/overview.html

PALO ALTO NETWORKS. Firewall PA-3060 [en línea]. 2016. [Consultado 5 de MAYO de 2016]. Disponible en Internet: http://www.paloguard.com/Firewall-PA-3060.asp

SECRETARÍA DEL SENADO. Congreso de la República. Colombia. Ley estatutaria 1621 de 2013. Diario Oficial No. 48.764 de 17 de abril de 2013 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html.

……. Congreso de la República. Colombia. Ley estatutaria 1266 de 2008. Diario Oficial No. 47.219 de 31 de diciembre de 2008 [en línea]. 2017. [Consultado mayo 31 de 2017]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. 18 p.

TechTarget. SearchNetworking [en línea]. 2009. [Consultado 18 de marzo de 2016]. Disponible en Internet: http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security

ANEXOS

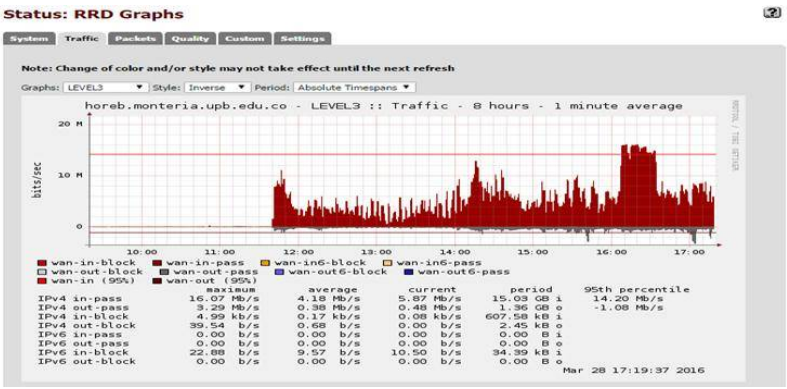
Anexo A. Autorización.

Se elabora carta de autorización para solicitar a la institución la ejecución del proyecto

Anexo B. Mediciones de Tráfico de RED de UPB Montería.

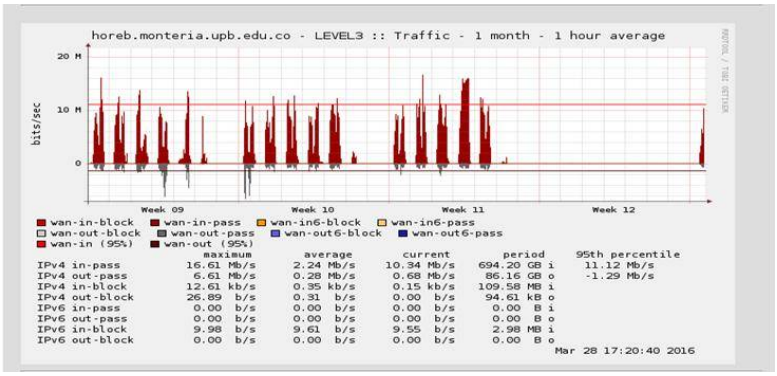
Para la red administrativa se tiene un ancho de banda de canal dedicado de 16 Mbps para acceso a Internet y un canal de datos de 2 Mbps para acceso al ERP ubicado en la sede principal UPB Medellín. Los siguientes Gráficos 1 y 2 muestran el tráfico entrante y saliente diario y mensual.

Gráfico 1. Tráfico red administrativa diario



Fuente: el autor

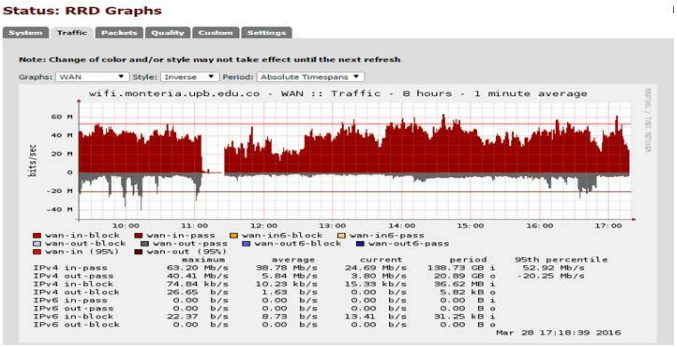
Gráfico 2. Tráfico red administrativa mensual



Fuente: el autor

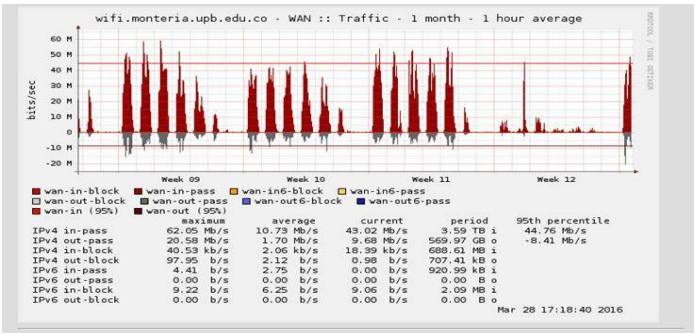
Para la red Académica y WiFi se comparte un canal dedicado de 100 Mbps. El siguiente Gráfico 3 presenta la estadística para la red inalámbrica diario y el Gráfico 4 presenta el tráfico promedio mensual.

Gráfico 3. Trafico de red inalámbrica diario



Fuente: el autor.

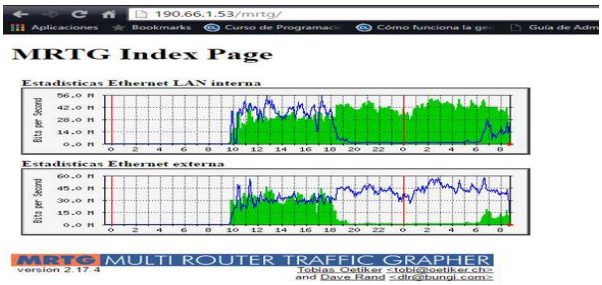
Gráfico 4. Trafico de red inalámbrica mensual



Fuente: el autor

En el siguiente Gráfico 5 se presenta el promedio de tráfico de la red académica con un ancho de banda de 100 Mbps Compartido con la red inalámbrica.

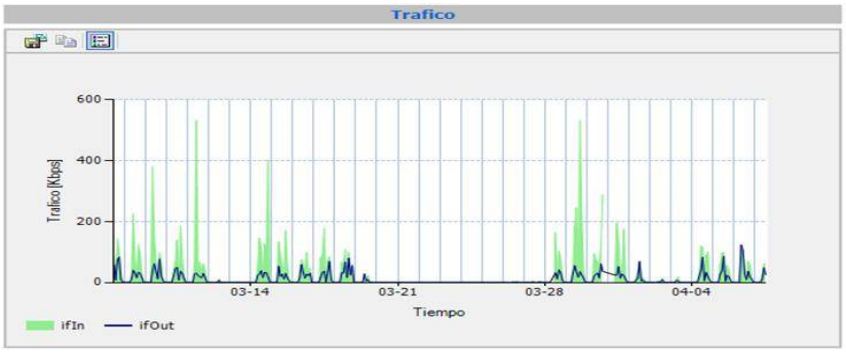
Gráfico 5. Trafico de red Académica mensual



Fuente: el autor

En los Gráficos 6 y 7 siguiente se presenta el promedio mensual de tráfico de red en Kbps del canal de datos de 2 Mbps dispuesto para el tráfico hacia el ERP ubicado en UPB Medellín y de acceso solo al personal administrativo.

Gráfico 6. Trafico del canal de datos mensual



Fuente: el autor

Gráfico 7. Trafico del canal de datos mensual

Valores tipicos	ifOut [Kbps]	ifIn [Kbps]
Valor máximo	123,31	531,62
Valor mínimo	0,12	0,08
Último valor	16,71	31,44
Valor promedio	3,81	8,72
Percentile 95	21,01	48,58

Fuente: el autor

Anexo C. Invitación a Presentar Oferta.

OBJETIVO

La Universidad Pontificia Bolivariana Seccional Montería invita a presentar oferta para la implementación de firewall UTM en la prestación de servicios de seguridad perimetral de nuestra seccional.

COBERTURA Y PARTICIPACIÓN

La cobertura prevista de esta IPO y cualquier acuerdo resultante de esta convocatoria, será para el uso de todos los departamentos de la UPB Seccional Montería.

La UPB Seccional Montería se reserva el derecho de no celebrar ningún contrato, añadir y/o eliminar elementos, o cambiar cualquier elemento de la cobertura y la participación en cualquier momento sin previo aviso y sin ninguna responsabilidad u obligación de ningún tipo o cantidad.

CONDICIONES GENERALES Y PARTICULARES

La UPB Seccional Montería está interesada en recibir ofertas para el suministro de una solución integral de Seguridad, que permita proteger el perímetro y los servidores (físicos y virtuales), en una arquitectura de protección por capas, que no solo asegure estas dos zonas indicadas, sino entre servidores virtuales entre sí. Las ofertas deberán ser presentadas en modalidad de inversión y de servicio a 1 o 3 años.

Las propuestas deberán incluir el diseño de la arquitectura adecuada para la UPB Seccional Montería, el suministro de los equipos necesarios, la instalación, la configuración del equipo de seguridad, así como los equipos complementarios para una integración adecuada LAN, así como la puesta en funcionamiento, soporte y mantenimiento de la solución para:

DIMENSIONAMIENTO	CANTIDAD	SOLUCIÓN
Usuarios de la institución actuales	2.500	
Red LAN	550 puntos	
Promedio de conexiones WiFi	800 conexiones	
Velocidad de Internet actual	118 Mbps	
Velocidad de Internet proyectada a 1 año	180 Mbps	
Años de servicio y garantía	1 a 3 años	
Usuarios a conectarse por VPN	30	
Bloqueo de correos basura	Si	

REQUISITOS PARA LA EVALUACIÓN Y POSTERIOR ADJUDICACIÓN

La arquitectura debe incluir: Cuadro 1. Requisitos de obligatorio cumplimiento y funciones adicionales deseadas.

FUNCIÓN ESPECÍFICA, DE OBLIGATORIO CUMPLIMIENTO	FUNCIÓN DESEADA, COTIZADA COMO ADICIONAL	CUMPLE S/N
Firewall UTM de Nueva Generación de Perímetro, tipo Appliance		
Firewall de Nueva Generación de Servidores, Virtual o lógico		
Deberán indicar consumos energéticos de los equipos incluidos en la solución		
El fabricante debe ser Líder del cuadrante mágico de Gartner para Firewalls de Nueva Generación, o del cuadrante 1 de NSS Labs; al menos durante los dos últimos años. Anexar soportes.		
La solución no debe poseer vulnerabilidades conocidas durante el último año que hayan implicado que la arquitectura ha podido ser vulnerada.		
Se requiere Firewall, VPN, Gateway Antivirus de red, IPS, Filtrado de Contenido, Control de aplicaciones, identificación de usuarios a través de directorio activo u OpenLDAP. Si la solución se diseña en uno solo o múltiples equipos, tiene que ejecutar todas las funcionalidades al mismo tiempo, sin degradación del servicio. Indicar también modo de procesamiento del equipo, ejemplo si trabaja con procesadores separados para diferentes componentes.		
El equipo debe ser accesible a través de SSH/interfaz Web HTTPS/SSL		
La herramienta debe ser capaz de realizar backup/restore de la configuración		
Interfaces requeridas: *Cantidad de puertos requeridos (Ethernet, ópticos, etc.)*		
Debe soportar mínimo *30* Vlans por interface. En cualquier caso, indicar cuanto es el máximo soportado por puerto.		
Throughput con firewall y módulo de aplicaciones activo mayor o igual a *x* Gbps		
Throughput para VPNs al menos 60 Gbps		
Al menos *x* de sesiones concurrentes		
Debe incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino.		
Debe permitir crear controles de acceso por aplicaciones/servicios/protocolos predefinidos. El fabricante deberá indicar cuantos soporta como máximo.		

FUNCIÓN ESPECÍFICA, DE OBLIGATORIO CUMPLIMIENTO	FUNCIÓN DESEADA, COTIZADA COMO ADICIONAL	CUMPLE S/N
Debe tener la opción de negar los parámetros de origen o destino, es decir, que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.		
La comunicación entre los servidores de administración y los gateways, (si no está incluido en el mismo equipo) debe ser cifrada y autenticada.		
Filtro de Contenido		
Debe ser basado en URL y categorías, integrado al hardware o como modulo adicional		
Debe tener la capacidad de bloquear granular mente sitios		
Debe incluir un mecanismo para negar o permitir URLs específicos, que no están definidos en una categoría, y que podrán ser utilizados en la definición de nuevas reglas		
Debe permitir la creación de excepciones		
El fabricante deberá indicar por escrito cuantos sitios web está en capacidad de filtrar, y cuantas categorías, sobre los equipos diseñados para la presente IPO.		
Control de Aplicaciones		
Debe ser capaz de identificar, permitir o bloquear aplicaciones, así como monitorear el uso que se hace por bytes, sesión y usuario. El fabricante deberá indicar el número máximo de aplicaciones soportadas.		
Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con directorio activo o LDAP.		
Debe proveer control granular para aplicaciones, especialmente redes sociales y torrent file. En caso de no reconocer la aplicación, el fabricante deberá suministrar una remediación en un tiempo inferior a 24 horas, o suministrar un mecanismo que permita tomar acciones sobre esta.		
La solución debe integrar reglas de filtrado de URL o con módulo de control de aplicaciones basado en firmas y/o decodificadores		
Debe tener la capacidad de hacer un análisis avanzado que incluya, tráfico por sitios, graficas, estadísticas, y análisis centralizado de comportamiento de aplicaciones		
Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales y grupos de usuarios.		
Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.		

FUNCIÓN ESPECÍFICA, DE OBLIGATORIO CUMPLIMIENTO	FUNCIÓN DESEADA, COTIZADA COMO ADICIONAL	CUMPLE S/N
Debe ser posible integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en: usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas		
La solución debe controlar el ancho de banda de las aplicaciones por regla/usuario, prioridad, segmento y/o aplicación. También por horarios de uso y/o redirección a páginas personalizadas que informen las políticas de uso de la *UPB Seccional Montería*		
Debe ser posible usar al menos las siguientes cuatro acciones en una regla de control de aplicaciones y filtrado de URL: bloquear, monitorear, informar al usuario y preguntar al usuario.		
GATEWAY ANTIVIRUS		
Debe realizar scan de virus y bloquearlos en al menos los siguientes protocolos: POP3, FTP, SMTP y HTTP.		
El antivirus debe soportar descargas continuas, de manera que se comience a enviar el archivo escaneado antes de realizar el scan completo del archivo y de esta manera evitar timeouts cuando se realizan scans sobre archivos grandes.		
Debe soportar el escaneo por dirección, es decir que el Gateway sea capaz de detectar y escanear archivos que se mueven en una dirección particular, por ejemplo de redes externas o cuando cruza una DMZ.		
El módulo de Antivirus & antimalware debe hacer escaneo en tiempo real tanto de antivirus como de malware. Y vulnerabilidades conocidas y nuevas		
Debe ser capaz de detectar malware y ataques de día cero (no conocidos) en base a una plataforma de sandbox (Caja de Arena)		
Debe hacer inspección sobre tráfico encriptado SSL.		
Debe hacer control de tráfico IPV4 e IPV6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y URL específicas		
ACCESO MOVIL / VPN		
La *UPB Seccional Montería* cuenta con aplicaciones altamente sensibles al retardo, por eso se requieren VPNs IPSec. Si el oferente la propone tipo SSL, el retardo será medido, y en caso de no cumplir con un valor mínimo que permita la ejecución de la aplicación correctamente, deberá ser modificada durante la implementación a VPN IPSec.		
Debe soportar conexiones VPN site to site, y client to site.		
Al menos 60 usuarios concurrentes tipo client to site, y al menos 50 sesiones concurrentes site to site.		

FUNCIÓN ESPECÍFICA, DE OBLIGATORIO CUMPLIMIENTO	FUNCIÓN DESEADA, COTIZADA COMO ADICIONAL	CUMPLE S/N
Deberá suministrar facilidades para la conexión VPN para clientes con sistemas operativos: Windows Xp, Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits), Mac OS 10.6 en adelante, Linux; también para móviles Android, iOS, Windows phone, etc.		
Deberá permitir crear reglas para tráfico VPN (SSL / IPSEC)		
Deberá soportar autenticación de usuario por base de datos local, integración con Directorio Activo u Open LDAP.		
FUNCIONES AVANZADAS		
Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red.		
Debe soportar priorización de trafico según clases, para permitir trafico crítico sobre el que no lo es		
Debe incluir balanceo de carga de Gateway con sincronización de estados, sin necesidad de usar un balanceador externo.		
Administración de la solución		
Debe proveer el mecanismo o funcionalidad de distribuir y aplicar nuevas versiones de software para los gateways de la solución.		
Los logs de los equipos deben poder correlacionarse.		
Debe tener la funcionalidad de Administración de Logs integrada en el mismo dispositivo de seguridad, en el caso de que no sea posible, debe redirigirse a un equipo externo, o indicar como lo haría, sin incrementar el costo de la solución.		
Debe automáticamente unificar eventos de IPS, y tener un análisis forense completo de los eventos		
Debe poder generar y enviar reportes sin afectar al tráfico real y sin la necesidad de un equipo de terceros.		
Los reportes deberán incluir la capacidad de proporcionar un resumen gráfico de aplicaciones utilizadas, y amenazas encontradas diariamente.		
Deberá tener la capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con respecto al pasado.		

FUNCIÓN ESPECÍFICA, DE OBLIGATORIO CUMPLIMIENTO	FUNCIÓN DESEADA, COTIZADA COMO ADICIONAL	CUMPLE S/N
El equipo deberá proporcionar los siguientes conjuntos de reportes: - Utilización de ancho de banda de entrada y salida por aplicación. - Reporte de malware día cero detectado como benigno o maligno. - Comparativo diario/semanal de aplicaciones corriendo en la red que pudieran incrementar o disminuir su utilización. - Utilización (en bytes) por aplicación. - Origen y destino del tráfico por aplicación-usuario - Eventos / ataques por: origen, categoría, amenaza, protocolo, nivel de riesgo de la red. - Principales aplicaciones que circulan por el firewall		

LA IMPLEMENTACIÓN DE LA SOLUCIÓN DEBERÁ SER POR FASES, ASÍ:

Los objetivos que deberán cumplirse con el diseño son:

- Firewall para controlar el tráfico desde y hacia la red internas y externas de la UPB Seccional Montería.
- Acceso seguro para todo tipo de dispositivo que requiera conexión a la UPB Seccional Montería desde redes externas; lo cual incluye equipos Windows, MAC, Linux hasta móviles Android, IOS y Windows phone.
- La solución debe permitir la integración con el Directorio Activo para adquirir las identidades de los usuarios de la UPB Seccional Montería.
- La solución debe permitir el uso de una página de autenticación, para todos aquellos dispositivos que no puedan integrarse contra el Dominio de la *UPB Seccional Montería*, para controlar el acceso a Internet, y aplicativos internos de la entidad.
- La solución debe contar con la capacidad de implementar medidas que eviten riesgos de suplantación, para computadores de usuarios críticos (ej. Financiero, contabilidad, Recursos Humanos).
- La solución debe estar dimensionada para 2500 usuarios, con un crecimiento estimado del *3*% anual, durante los próximos *5* años, contados a partir de 2016. En caso de que el diseño del oferente arroje que este supuesto debe ser mejorado, deberá justificarlo.
- Deberá permitir el control, sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal).
- Deberá incluir protección contra ataques de negación de servicios.
- Control de host diferentes a Windows.
- Deberá incluir solución Anti - Botnets.

- Escalamiento a futuro para protección avanzada de bases de datos, en cumplimiento de la ley 1581 de 2012.

En cuanto al IPS deberá cumplir lo siguiente:

- Deberá incluir un módulo de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en internet y bloqueo de archivos por tipo.
- Deberá estar basado en los siguientes mecanismos de protección: firmas de exploit, anomalías de protocolo, detección basada en comportamiento y controles para aplicaciones.
- Deberá incluir protección contra virus en contenido HTML, software espía y gusanos.
- Deberá incluir Protección contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos.
- Deberá escanear virus en HTTP, HTTPS, SMTP, POP3, IMAP como mínimo.
- Deberá permitir la inspección en archivos comprimidos.
- Deberá soportar bloqueo de archivos por tipo, indicando el máximo permitido por el fabricante.
- La actualización de firmas de ataques deberá ser diaria, semanal y de emergencia.
- Deberá proteger implementaciones de VoIP, soportando H323 v2/3/4 (incluido h.225 v.2/3/3 y h.254 v3/5/7), SIP, MGCP y SCCP.
- Deberá soportar excepciones de red basadas en origen, destino, servicio o una combinación de las 3.
- Deberá contar con la opción de realizar análisis, detección y bloqueo de malware de día cero vía revisión de archivos en caja de arena (SANDBOX) y facilitar remediación inmediata.
- Contará con un mecanismo para activar o administrar nuevas firmas de forma automática, después de un proceso de actualización.
- Tendrá la capacidad de capturar paquetes para protecciones específicas, con el ánimo de realizar propósitos forenses posteriores.
- Tendrá mecanismos anti-evasión para controlar trafico P2P.
- La licencia debe ser para usuarios ilimitados de firewall e ilimitadas direcciones IP.
- El oferente deberá incluir procedimientos alternos cuando se pierde la gestión remota.
- El oferente deberá especificar **por escrito** si cumple o no lo solicitado en el cuadro 1.
- El oferente deberá cumplir con una implementación por fases como la especificada anteriormente.

Además, deberá responder por escrito lo siguiente:

La solución de seguridad requerida debe cumplir para los protocolos ipv4, ipv6, ipv4 más ipv6. El oferente debe indicar para cada ítem solicitado si soporta cada uno de ellos. Dentro de la implementación, el proveedor deberá considerar que servicios como voz, videoconferencia y/o streaming, presenten alta calidad, por ello los equipos incluidos en la solución deberán soportar esquemas de QoS, y el oferente estará incluyendo dichas configuraciones dentro del proyecto.

La entrega de propuestas debe realizarse en las fechas indicadas y vía electrónica. Cualquier inquietud puede hacerse vía correo electrónico a **TODOS** los contactos indicados en la IPO, y por ese mismo medio será resuelta. Propuestas que no incluyan los costos en el formato propuesto para presupuesto, y las respuestas al cuadro 1 no serán consideradas en la adjudicación del proyecto.

Capacitación		
Project Management		
Otros costos (especifique cuales)		
Subtotal:		
IVA:		
Costo Total:		

Las categorías de costo solicitadas son:

Hardware: Listado, descripción y registro del costo de cada parte de hardware requerida.

Software: Listado, descripción y registro de las licencias, sistemas operativos, desarrollo de portal, implementación de la solución integrada a una autenticación con directorio activo, entre otros, que estén asociados a la solución.

Instalación: Todo lo requerido con la instalación y puesta en operación de la solución diseñada en la presente IPO. Incluida la configuración en equipos pertenecientes a *UPB Seccional Montería*, y se requieran para integrar la solución a la LAN.

Mantenimiento: Todo costo asociado con la operación y mantenimiento de la propuesta entregada.

Documentación: Si existen tarifas asociadas a la documentación técnica

Capacitación: Si existen tarifas asociadas con el entrenamiento del personal de *UPB Seccional Montería* para la operación de la solución propuesta.

PM: Si existen costos asociados con la solución propuesta, deberán ser incluidos en este ítem.

El oferente puede presentar su oferta indicando el costo asociado por cada una de las fases planteadas en las condiciones generales, sin modificar el formato anterior de presupuesto. Es decir, deberá aplicar el formato por cada fase y por todo el proyecto. Deberá especificar el costo total después de impuestos, y al momento de emitir la Orden de compra se hará con la TRM que tenga asociada dicho día.

11.2 Modelo Servicio:

Presentar todos los costos asociados al proyecto de forma independiente, es decir, un valor por servicio tipo recurrente mensual, y un valor por instalación, que se pagara una única vez en relación al presente diseño y posterior implementación. Además, como varían los costos del servicio finalizada cada fase de implementación, especificada en las condiciones generales de la presente IPO.
Si existe algún servicio de valor agregado, y tiene cobro por aparte, este deberá indicarse también.

CRITERIOS DE EVALUACIÓN

La evaluación se basará en los siguientes criterios:

- Cumplimiento de los requisitos obligatorios.
- Oferta de valor de la solución.
- Capacidad del proveedor para cumplir o superar los requisitos establecidos en el presente documento.
- Conveniencia del sistema y/o esquema propuesto por el oferente.
- Conveniencia de las sugerencias y recomendaciones de modificación al esquema planteado.
- Presentación de la oferta cumpliendo con el diligenciamiento de los requisitos (cuadros 1 y 2) y presupuesto.
- Tiempo de implementación.
- Experiencia del proveedor en proyectos similares. Para ello deberá describir brevemente, el objeto del proyecto, la empresa y el contacto avalado para corroborar la información.

El propósito de esta convocatoria es identificar al proveedor que presente la mejor oferta de valor de seguridad que demanda la época actual. El proveedor en cuestión deberá tener el interés de trabajar con la UPB Seccional Montería, la capacidad técnica y operativa para presentar una solución de alto nivel de calidad e implementarla en el mejor tiempo posible; y la fortaleza financiera que permitan llevar a feliz término el suministro de una solución empresarial para la UPB Seccional Montería.

Anexo D. Pruebas de Vulnerabilidades con UTM Check Point.

El siguiente reporte presenta el informe de vulnerabilidades encontradas en la red con el UTM en demostración de Check Point:

Fuente: el autor

Anexo E. Evidencias de Resultados e Impacto Esperado.

ACTIVIDAD DE LA RED POR DÍA

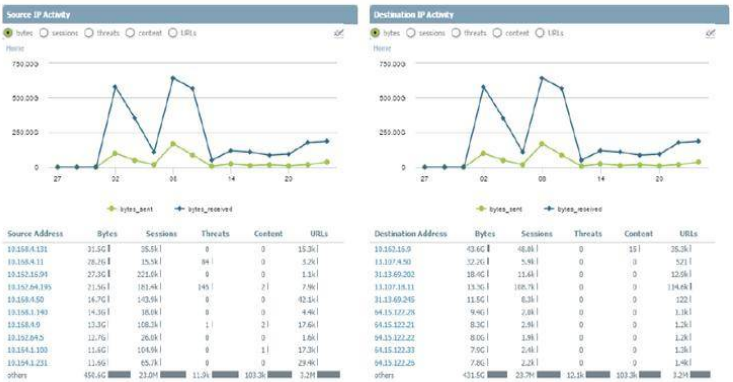
Rule	Bytes	Sessions	Threats	Content	URLs
Wireless-Untrust	13.4G	81.9k	34	790	39.7k
Salida a Internet_99	5.4G	3.8k	334	14	882
Administrativa-Untrust	1.0G	18.5k	2	2	5.6k
Academica-Untrust	631.4M	5.6k	0	20	1.0k
Moodle	606.4M	4.4k	0	4.1k	4.3k
Zenu	293.3M	2.9k	0	47	1.6k
Servidores-Untrust	116.7M	34.2k	0	2	1.3k
Tavor	113.4M	613	0	0	615
CTIC-Untrust	42.7M	509	0	0	289
Wireless-Servidores-1	2.6M	15.0k	0	0	0
others	9.9M	10.3k	4	0	893

Fuente: el autor

ACTIVIDAD DE LA RED POR MES:

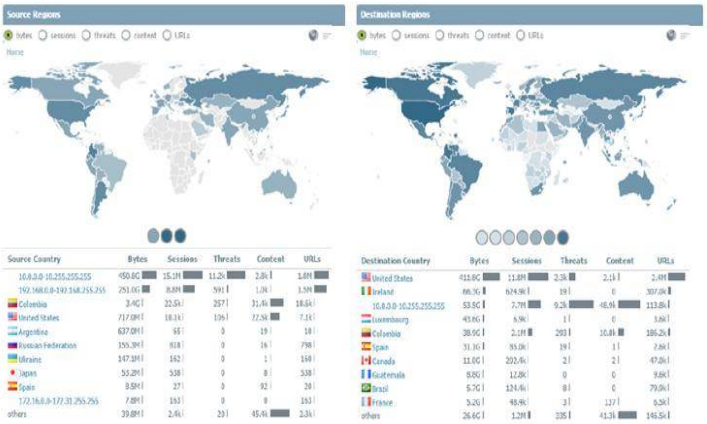
Fuente: el autor

ACTIVIDAD DE LA RED POR MES:



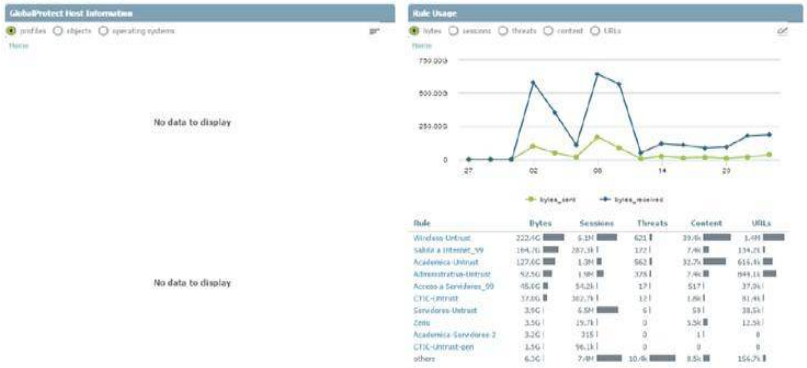
Fuente: el autor

ACTIVIDAD DE LA RED POR MES:



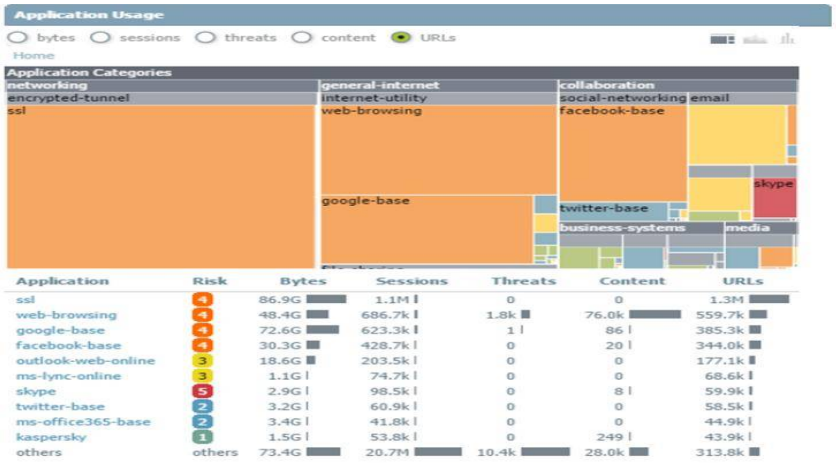
Fuente: el autor

ACTIVIDAD DE LA RED POR MES:



Fuente: el autor

TRAFICO POR MES:



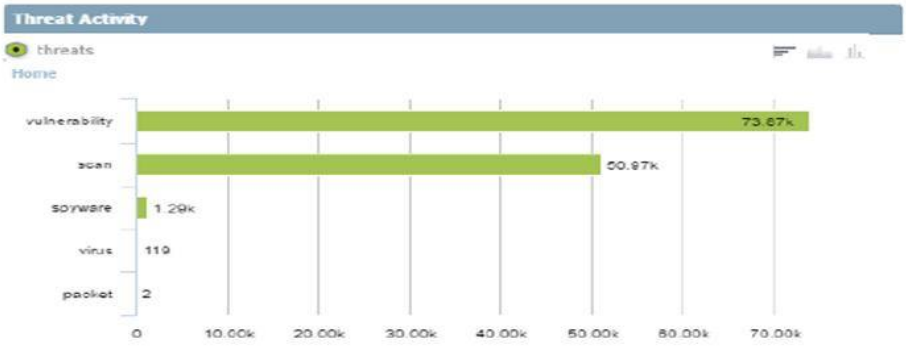
Fuente: el autor

REPORTE DE ENRUTAMIENTO:

Rule	Bytes	Sessions	Threats	Content	URLs
Wireless-Untrust	227.2G	6.2M	661	40.2k	1.4M
Salida a Internet_99	165.2G	289.3k	172	7.4k	135.5k
Academica-Untrust	128.9G	1.4M	583	33.3k	634.5k
Administrativa-Untrust	93.7G	1.9M	379	7.4k	852.0k
Acceso a Servidores_99	45.8G	55.0k	17	517	38.6k
CTIC-Untrust	37.0G	303.4k	12	1.8k	81.8k
Servidores-Untrust	3.9G	6.5M	6	59	38.6k
Zenu	3.5G	19.8k	0	5.5k	12.6k
Academica-Servidores-2	3.2G	329	0	2	0
CTIC-Untrust-gen	1.5G	96.3k	0	0	0
others	6.3G	7.5M	10.4k	8.5k	158.3k

Fuente: el autor

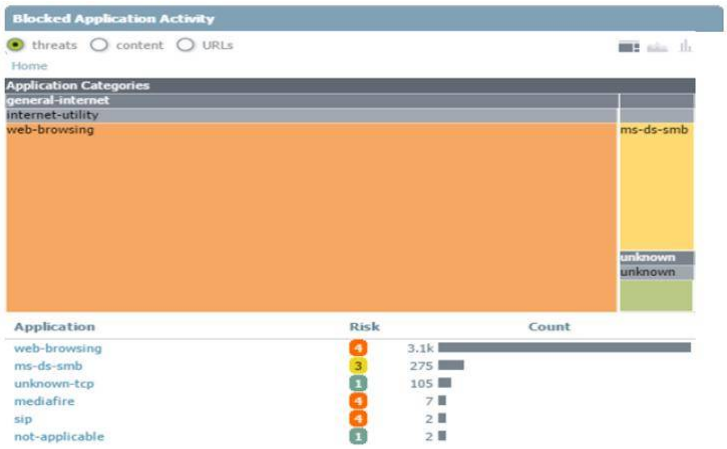
REPORTES DE ATAQUES:



Threat Name	ID	Severity	Threat	Threat Ca	Count
SCAN: Host Sweep	8002	medium	scan	scan	50.6k
HTTP OPTIONS Method	30520	informa	vulnerab	info-leak	30.5k
Javascript WSF or HTA File Sent in Email	39003	informa	vulnerab	code-execu	22.9k
Microsoft Office File with Macros Detected	39154	informa	vulnerab	code-execu	2.8k
Unknown HTTP Request Method Found	39822	informa	vulnerab	protocol-ar	2.5k
HTTP Non RFC-Compliant Response Found	32880	informa	vulnerab	info-leak	2.1k
JavaScript Obfuscation Detected	31825	low	vulnerab	code-execu	2.1k
Suspicious Abnormal HTTP Response Found	38870	low	vulnerab	protocol-ar	1.8k
WordPress Login Brute Force Attempt	40044	critical	vulnerab	brute-force	1.7k
Suspicious HTTP Response Found	39869	low	vulnerab	protocol-ar	1.5k
others	others	others	others		7.8k

Fuente: el autor

REPORTE DE BLOQUEOS DE APLICACIÓN:



Fuente: el autor

REPORTE DE BLOQUEO DE ATAQUES:

Fuente: el autor

MEDICIÓN DE VELOCIDAD DE LA RED:

Fuente: el autor