UNIVERSIDAD RICARDO PALMA
FACULTAD DE INGENIERÍA

PROGRAMA DE TITULACIÓN POR TESIS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO DE ARQUITECTURA DE SEGURIDAD PERIMETRAL PARA UNA EMPRESA DEDICADA A LA ACTIVIDAD INMOBILIARIA

TESIS

PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. MONTES LARIOS JOSE MANUEL

Bach. ITURRIZAGA HERNANDEZ MANUEL ANTONIO

ASESOR: LUIS ALBERTO CUADRADO LERMA

LIMA – PERÚ

AÑO: 2015

Dedicatoria

Dedico esta tesis de manera especial a mis padres, a mis hermanos, a mí querida esposa Vanessa y a mi precioso hijo Fabrizzio, los cuales siempre han sido el motor y motivo para poder lograr cada pasó de éxito en mi vida profesional, a su vez a mis abuelos por todas las recomendaciones brindadas en el transcurso de mi vida.

Agradezco a Dios por brindarme la tenacidad y fortaleza para poder finalizar de manera exitosa la tesis, a mis colegas ingenieros por sus grandes aportes y a mis profesores que con gran ahínco brindaron una gran base de conocimientos.

Manuel Antonio Iturrizaga Hernández

Dedicatoria

Dedico esta tesis al Señor Jesucristo, quien es la fortaleza de mi vida, quien cuida siempre de mí.

Así mismo a mis padres, a mis hermanos por su comprensión y palabras de aliento en todo tiempo.

José Manuel Montes Larios

Agradecimiento

En primer lugar agradecemos a Dios por habernos dado la vida por medio de nuestros padres, pues han sido usados por Él y han sido de gran ayuda en todo momento.

Índice General

Índice de Figuras

Índice de Tablas

Resumen

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. A su vez día a día se descubren nuevas vulnerabilidades, nuevos tipos de ataques y nuevos parches que aplicar los sistemas institucionales, convirtiendo la operación de la seguridad en una tarea sumamente compleja y demandante.

El presente documento es sobre el desarrollo de la seguridad perimetral en la empresa Los Portales, vale indicar que dicha empresa es una de las más renombradas a nivel de la actividad inmobiliaria en el Perú, por ende se está considerando las amenazas de seguridad desde perspectivas diferentes para permitir de esta forma conocer algunos riesgos que puedan afectar a la institución, así como determinar el nivel de madurez de la seguridad informática, a su vez se demostrara a detalle el diseño e implementación de la solución así como el alcance económico.

Palabras clave: Seguridad Perimetral, amenazas de seguridad, seguridad informática, firewall, ataques, vulnerabilidades.

Abstract

Because Internet use is increasing, more and more companies allow their partners and suppliers access to their information systems. Therefore, it is essential to know what company resources need protection so as to control system access and the rights of users of the information system. In turn every day new vulnerabilities, new types of attacks and new patches to apply institutional systems, making the security operation in an extremely complex and demanding task are discovered.

This thesis is on the development of perimeter security at Los Portales, it indicate that the company is one of the most renowned level of real estate activity in Peru, thus being considered security threats from different perspectives to meet thus enable some risks that may affect the institution, and to determine the maturity level of computer security, in turn demonstrate in detail the design and implementation of the solution as well as the economic scope.

Keywords: perimeter security, security threats, security, firewall, attacks, vulnerability.

Introducción

Hoy en día debido a la gran facilidad que nos brindan los dispositivos electrónicos tales como: ordenadores, Smartphones, Tablets, etc; los cuales permiten el acceso a mucha información virtual. Se ha vuelto una necesidad el poder controlar los niveles de acceso a dicha información.

Ante un nuevo software o nueva tecnología, hoy en día los hackers inmediatamente empiezan a analizar las vulnerabilidades que pudieran explotar, y cuando las detectan las atacan.

A partir de aquí el nivel de seguridad decae considerablemente y se está expuesto a que cualquiera encuentre alguna vulnerabilidad en el sistema informático de la Organización.

Los riesgos han evolucionado y ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas maliciosas, accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Es así que para asegurar la operatividad de un negocio a nivel de recursos informáticos así como de ancho de banda, se ha vuelto inherente el uso de dispositivos que fortalezcan la seguridad de las políticas de la empresa.

Hoy en día el núcleo de todo negocio radica en la información que define a la empresa, por ende la prioridad que se da al resguardo de dicha información es vital.

Por ende el siguiente estudio tiene como finalidad brindar un esquema de Seguridad Perimetral para la empresa Los Portales, empresa líder en el ámbito inmobiliario ,dicho diseño tiene como finalidad proteger la red interna y dar buen uso de sus recursos a nivel de ancho de Banda.

CAPITULO I: LA SEGURIDAD INFORMATICA

1.1 Descripción de la realidad problemática

Los Portales con el transcurrir de los años ha empezado a crecer en gran manera por todo el país por ende la información con la que cuenta y maneja también lo hizo, pues al tener mayor alcance, las oportunidades laborales aumentaron, por consiguiente se obtiene más usuarios empleando más información la cual es parte importante y es uno de los activos de la empresa.

La seguridad perimetral [1] en una red de datos es de vital importancia para proteger la integridad, confidencialidad y autenticidad de la información, si no se aplicarían normas de seguridad en el perímetro de la red existiría un riesgo que en cualquier momento podría ser aprovechado generando consecuencias muy graves en este caso para Los Portales que ahora en adelante llamaremos la empresa.

La empresa actualmente cuenta con una topología de red la cual en este momento ya no cubre del todo con las necesidades que tiene y requiere.

Es muy importante conocer a fondo todo el esquema y los componentes de la red de datos, a partir de lo cual, deberían implementar los controles necesarios para bloquear o filtrar los accesos desde las redes no confiables hacia la red privada. Todo esto conlleva a la elaboración de un esquema de seguridad perimetral que debe ser muy bien analizado y evaluado, ya que una mala planeación puede llevar a la saturación de los recursos de red y afectar al negocio.

La seguridad perimetral en cualquier red de datos está conformada por componentes de hardware y software, entre los cuales podemos destacar:

- Ruteadores
- Firewall
- IDS (Intrusion Detection System) o IPS (Intrusion Prevention System)

- Antivirus
- Antispam

1.1.1 Delimitaciones

1.1.1.1 Delimitación Espacial

Esta tesis está enfocada en la empresa Los Portales, empresa líder de la actividad inmobiliaria del Perú conformada por la alianza estratégico entre LP Holding (Grupo Raffo) e ICA de México. Más de 50 años de experiencia en el mercado nacional con cuatro unidades de negocio.

1.1.1.1.2 Delimitación temporal

Esta investigación es de actualidad, por cuanto esta solución está siendo implementada.

1.2 Definición del problema de investigación

1.2.1 Problema principal

- La empresa no cuenta con una arquitectura consistente que brinde seguridad perimetral la cual pueda garantizar la integridad de la información tanto interna como externa.

1.2.2 Problemas secundarios

- Se podrá determinar qué solución por medio de un análisis el tipo de topología de Seguridad Perimetral que se aplicará.
- De qué manera se podrá diagnosticar las necesidades del cliente nivel de seguridad perimetral.
- Con un estudio detallado se podrá determinar las tecnologías que apliquen a las necesidades específicas del cliente.

1.3 Objetivos de la investigación

- En los objetivos de la investigación se cuenta con dos tipos, general y especifico, se detallan a continuación:

1.3.1 Objetivos generales

- Desarrollar una arquitectura consistente que brinde seguridad perimetral garantizando la integridad de la información tanto interna como externa de la empresa orientada al rubro inmobiliario.

1.3.2 Objetivos específicos

- Analizar y definir las necesidades de seguridad perimetral, en base a los resultados obtenidos del análisis de riesgo actual.
- Diseñar el esquema de seguridad definiendo políticas de seguridad, mecanismos de defensa, dispositivos de seguridad, software y hardware a utilizarse usando la información resultante del análisis previo sobre las necesidades de seguridad perimetral para la red.
- Estudiar las tecnologías que cubran las necesidades específicas del cliente.

1.4 Justificación e importancia

Podemos precisar que lo más relevante en esta tesis, es asegurar la integridad y privacidad de la información informática y el buen uso de los recursos adquiridos por la empresa orientada al rubro inmobiliario.

CAPITULO II: MARCO TEÓRICO

2.1 Antecedentes del estudio de investigación

Para poder hablar de seguridad perimetral es necesario mencionar algunos factores que determinaron su importancia. [2]

Así como también es necesario definir los elementos que intervienen, las diferentes tecnologías existentes para asegurar la información y los servicios de una red informática.

En la década de los 60´s los estudiantes del Tecnológico de Massachusetts fueron aquellos que iniciaron el nombre de Hacker para hacer referencia a programadores de colegio de supercomputadoras, muy distinto al significado que tiene ahora.
El departamento de defensa de los Estados Unidos crea ARPANET la cual ganó popularidad en investigación y en círculos académicos para el intercambio electrónico de información, hoy mejor conocida como Internet.

Ken Thompson desarrolla el sistema operativo Unix, conocido como la herramienta del “hacker amistoso” por las bondades que ofrece, herramientas sumamente accesibles que cuentan con ayuda y mejora constante.

Dennis Ritchie desarrolla el lenguaje de programación C, el cual es el más popular entre todos los lenguajes usados por la comunidad de Hackers.

En los 70’s el protocolo Telnet fue desarrollado por Bolt, Beranek, y Newman, la cual era una extensión pública de Arpanet. Bajo el punto de vista de varios investigadores de seguridad, Telnet es el protocolo más inseguro de las redes públicas.

Apple fue fundada por Steve Jobs y Steve Wozniak y de esta manera se empezó con el mercadeo de las computadoras personales.

Fue creado USENET, era uno de los más populares foros para el intercambio de ideas en computación, redes y Cracking.

En los años 80´s IBM por medio de su microprocesador Intel desarrolló y comercializó la PC, de esta forma la PC pasó a ser de uso en el hogar y oficinas.

Vint Cerf desarrolló el protocolo TCP la cual es dividida en dos partes.

Durante 9 días de hackeo ininterrumpido, fue atrapada por las autoridades La Brigada 414, quienes interrumpieron en Los Álamos, organización que realiza investigación en armas nucleares.

Los primeros grupos de Hackers fueron la legión de destrucción y el club de caos que comenzaron atacando sobre las vulnerabilidades en computadoras y redes de datos.

En el año 1986 el acto de fraude y abuso de computadoras ,fue llevado a votación por el congreso de los Estados Unidos, luego de ello se puso tras las rejas a Robert Morris tras desatar el Gusano Morris a más de 6000 computadoras vulnerables en Internet.

Durante los 90´s ARPANET es consolidada como la red de redes es decir Internet.

El entorno gráfico del navegador Web es creado y con esto da inicio a una acelerada demanda a Internet.

Un grupo de estafadores transfieren ilegalmente 10 millones de dólares a varias cuentas de la base de datos central Citibank, siendo el líder de este grupo capturado por la INTERPOL.

Kevin Mitnick fue quien entró a varios sistemas corporativos, robando todo desde información personal de celebridades hasta más de 20,000 números de tarjetas de crédito y código fuente propietario, fue sentenciado a 5 años de prisión.

Los fraudes de todos los tipos empiezan a salir a la luz, no solo realizaban sus hazañas sino que también las compartían e intercambiaban ideas e información, en Defcon convención anual.

2000

En mayo se detectó el virus I Love You, causó daños por más de 10.000 millones de dólares en el mundo entero.

2004

El 3 de mayo un nuevo virus, Sasser, atacó Italia infectando decenas de miles de ordenadores. Afectó gravemente el funcionamiento de Correos y Ferrocarriles.

2005

En febrero un ataque a Bank of América afectó a 1,2 millones de cuentas dio comienzo a la escalada. Desde entonces, bancos, tiendas, universidades, aseguradoras y centros sanitarios se han convertido en el blanco favorito de los atacantes. En junio Citigroup veía cómo accedían a los datos de 3,9 millones de ficheros.

2007

En abril hackers atacaron páginas de varias instituciones de Estonia. Las autoridades acusaron de la agresión a los servicios secretos rusos pero los expertos estimaron que se realizó a nivel global.

2008

A finales de año se detectó el virus Conficker que para abril de 2009 infectó más de 12 millones de ordenadores afectando los sistemas de buques de la Armada y el Parlamento del Reino Unido.

2009

El 8 de abril The Wall Street Journal informó de que hackers rusos y chinos atacaron ordenadores que controlan las redes eléctricas en territorio estadounidense probablemente para introducir programas que podrían producir cortes en caso de una crisis o una guerra.

El 21 de abril el periódico The Wall Street Journal comunicó que ciberdelincuentes consiguieron violar el sistema informático del Pentágono y robaron la información sobre el F-35 Lightning II. Según los expertos, los datos se podrían utilizar para elaborar sistemas de defensa contra el avión.

El 21 de diciembre la televisión Fox News informó de que el FBI comenzó a investigar el robo de decenas de millones de dólares a Citigroup y que las sospechas del crimen recaían sobre hackers rusos.

2010

En septiembre las autoridades estadounidenses acusaron a más de 60 personas de un ataque informático contra la banca que permitió robar al menos 3 millones de dólares en EEUU y 9,5 millones en el Reino Unido. El virus que usaron los delincuentes, Zeus, probablemente fue creado en Rusia.

En noviembre y diciembre Anonymous organizó una serie de ataques DDoS contra compañías y organizaciones que se oponían a la actividad de Wikileaks, en particular PayPal, Visa y MasterCard.

2011

En junio el grupo bancario Citigroup informó de un ataque a una base de datos de tarjetas en Norteamérica que afectó a 360.000 personas.

En marzo, piratas violaron la red informática de RSA, sucursal de la empresa EMC, obteniendo información sobre la tecnología SecurID que se utiliza para proteger redes de ordenadores en el mundo entero.

2012

El 22 de mayo se supo que Anonymous logró acceder al servidor del Ministerio de Justicia de EEUU donde estaban almacenados datos sobre todos los crímenes cometidos en territorio estadounidense.

La noche del 28 de noviembre una organización iraní de hackers, Parastoo, atacó uno de los servidores del OIEA y publicó las direcciones de correo de cien empleados exigiendo que firmaran una petición para investigar la actividad nuclear de Israel.

El 21 de diciembre consiguieron acceder al sistema de la operadora india de tarjetas prepago Visa y MasterCard y sacaron 5 millones de dólares en 4.500 cajeros automáticos. Hasta el 19 de febrero de 2013, y después de atacar también a una operadora estadounidense, se apropiaron de 40 millones de dólares realizando 36.000 transacciones.

2013

El 14 de abril, el día de las elecciones presidenciales en Venezuela, hackers desconocidos agredieron la cuenta de Twitter de Nicolás Maduro informando sobre supuestos fraudes.

En junio el FBI y Microsoft realizaron una operación conjunta para desmantelar una de las mayores redes de cibercrimen que infectó unos 1.000 ordenadores para cometer fraudes por más de 500 millones de dólares.

El 26 de julio un ciberataque afectó los sitios de doce instituciones públicas y la Bolsa de Venezuela. De la agresión se responsabilizaron Anonymous Venezuela y a Venezuela Hackers.

El 29 de julio Anonymous violaron las páginas del presidente y varias instituciones de Perú.

El 8 de noviembre quedaron vulneradas las páginas del presidente y el jefe del Ejecutivo de Singapur después de que las autoridades del país anunciaran medidas contra el grupo de hackers Anonymous.

2014

El 10 de julio The New York Times informó que piratas chinos atacaron en marzo el archivo de la Oficina de Administración de Personal de EEUU obteniendo datos sobre funcionarios que solicitaron información clasificada.

En 2015, la empresa especializada en seguros de salud Blue Cross ostentaba el dudoso honor de contar con el ataque más notable hasta el momento: 11 millones de archivos, muchos relacionados con sus pacientes, quedaron al descubierto.

2.2 Bases teóricas

En esta sección se va a tratar todo lo relacionado a conceptos bases sobre seguridad informática, desde la definición de Información hasta, seguridad perimetral y componentes.

2.2.1 Definición de Información

La información está constituida por un grupo de datos ya supervisados y ordenados, estos sirven para construir un mensaje. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Por lo tanto, viéndola de otra manera nos indica que la información es un recurso que otorga significado o sentido a la realidad, ya que mediante códigos y conjuntos de datos, da origen a los modelos de pensamiento humano.

Existe tipos de información, por ejemplo las que deben o pueden ser de conocimiento público, pues puede ser visualizada por cualquier persona ;y también aquella que debe ser privada y solo puede ser visualizada por un grupo selecto de personas, es en ésta que se debe de realizar esfuerzos para protegerla pues este tipo de información es:

- Critica: Indispensable para garantizar la continuidad operativa de la organización.
- Valiosa: Para la Organización es un activo corporativo con valor.
- Sensitiva: Debe ser conocida solo por las personas que necesitan la información.

Es imprescindible garantizar estos tres aspectos en cuanto a la información que maneja:

- Disponibilidad: Que siempre esté disponible cuando se la necesita.
- Integridad: La información siempre debe ser autentica y completa.
- Confidencialidad: La información debe ser solo vista por aquellas personas que cuenten con los privilegios y sean las autorizadas para hacerlo.

2.2.2 Concepto de seguridad Informática

La seguridad informática nació alrededor de los años 80 como una necesidad de evitar y contrarrestar los efectos que producen los ataques informáticos.

En vista que esto cobró a tener más importancia, pues la información era usada más a menudo por los sistemas informáticos y esta a su vez era más privilegiada y llegaba a convertirse en un activo de una Organización, es ahí cuando la seguridad informática crece ya que la necesidad de proteger información era muy importante pues podría afectar al negocio de una Organización.

Hoy en día la mayoría de organizaciones procesan datos los cuales usan en su día a día para el desarrollo del negocio en diversos dispositivos informáticos, entidades del entorno privado y público manejan información muy sensible, por ejemplo, el registro de una universidad maneja todos los datos de los estudiantes, ¿Qué sucedería si esos datos son alterados o eliminados por un hacker?, pues en ambos casos serían escenarios terribles para aquella casa de estudios, es aquí pues la importancia de la seguridad informática.

2.2.2.1 Amenazas Informática

Hoy en día los más grandes ataques son de carácter financiero, donde existe el robo sistemático de cantidades millonarias de dinero, producidas muchas veces por virus en los sistemas informáticos, y/o el acceso no autorizado a información, entre otros.

La manera en que estos ataques hayan llegado a tener acceso al sistema informático, implica que la red misma posea vulnerabilidad, la acción a tomar es implementar esquemas de seguridad, es decir una solución que en corto o

largo plazo sea completa y crezca continuamente conforme al nivel de protección y datos de la organización.

De este modo las organizaciones cada día están dando más importancia a la inversión en tecnologías de seguridad a decir verdad esto representa un gasto elevado que a la final da resultados intangibles y normalmente estos enormes presupuestos no convencen del todo a las personas que toman las decisiones de inversión, pero a la larga por medio de reportes mundiales sobre seguridad y estadísticas de organizaciones afectadas por ataques informáticos, dan gracias de poder tener implementados medios o políticas de seguridad en la red y no haber sido parte delos afectados.

Si bien es cierto nunca se puede llegar cubrir el 100%, pero con un esquema bien implementado y políticas de seguridad bien definidas se puede llegar fácilmente hasta un 99%.

2.2.2.2 Tipos de ataques Informáticos

Ataques, vienen a ser todas aquellas acciones que cometen una violación de seguridad de nuestra red y que estas afecten la confidencialidad, integridad o disponibilidad de la información alojada en ella.

Estas acciones se pueden clasificar de genéricamente según los efectos causados:

- Intercepción: Esto es cuando se desvía la información a otro punto el cual no es el destinatario original.
- Modificación: Sucede cuando algún individuo no autorizado consigue acceso a algún tipo de información como por ejemplo a una base de datos y este es capaz de manipularla.
- Suplantación: Esto es conocido como "phishing" [3] y consiste en crear portales exactos a otros y de esta manera engañar a los usuarios para que den información confidencial, generalmente se albergan en servidores remotos a los que se ha tenido acceso no autorizado, mayormente son los portales bancarios clonados los que son usados

para cometer fraude y estafar a sus usuarios. Un claro ejemplo lo tenemos en la figura 2.1.

Figura 2.1: Ejemplo de Phishing

Fuente: www.bloginspanish.wordpress.com

- Autentificación: Cuando un ataque suplanta a una persona con autorización.
- Explotación de errores: Sucede cuando se encuentran vulnerabilidades en los S.O, protocolos de red o aplicaciones.
- Ataques de denegación de servicio (DoS) [4]: Este tipo de ataque consiste en saturar un servidor con peticiones falsas hasta dejarlo fuera de servicio.

La red de cualquier organización está expuesta a todos estos tipos de ataques, tanto de usuarios internos como de externos, se podría decir que el mayor peligro se encuentra en los usuarios internos, debido a que estos se encuentran dentro la organización tienen accesos y privilegios y por

consiguiente están dentro del perímetro de seguridad de la red, esto quiere decir que no tienen restricción alguna en cuanto a la seguridad perimetral.

Actualmente los ataques internos a nivel mundial son los que producen más daño que los externos y son más frecuentes.

Figura 2.2: Finalidad de los ataques informáticos

Fuente: http://starterdaily.com

2.2.2.2.1 Ataques Internos

Se considera como una amenaza interna a los trabajadores tanto como a los administradores de red de la misma, pues tienen el poder total sobre la red ya que ellos conocen usuarios y claves con todos los privilegios, en teoría los administradores deben tener un concepto de ética mucho mayor que los demás usuarios, pero mundialmente es pues en las empresas han habido casos de ataques internos por parte de administradores que han sido despedidos o simplemente no están satisfechos con algún aspecto de la empresa, es por eso que se han convertido en sujeto de amenaza para la red.

Actualmente existe una técnica de ataque interno que está trayendo bastantes problemas en el ámbito de la seguridad informática, esta es la ingeniería social.

2.2.2.2.2 Ingeniería Social

Es una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir lo que nos interese de un tercero por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos. Las acciones

realizadas suelen aprovecharse de engaños, tretas y artimañas para lograr que un usuario autorizado revele información que, de alguna forma, compromete al sistema.

En el mundo de la seguridad de la información, es utilizado, entre otros, para dos fines específicos:

- Primero: El usuario es tentado a realizar una acción necesaria para dañar el sistema: este es el caso en donde el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto o abrir la página web recomendada que terminará dañando el sistema.
- Segundo: El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del phishing, en donde el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza.

Si bien podríamos entrar en particularidades de cada caso, es fundamental comprender que no hay tecnología capaz de protegernos contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque. La Ingeniería Social no pasa de moda, se perfecciona y sólo tiene nuestra imaginación como límite.

2.2.2.2.3 Ataques externos

Este tipo de ataque es más amplio y genérico, debido a que cualquier red puede ser víctima de ataques provenientes de afuera sin importar el tipo de red que sea o si contiene información crítica en sus servidores.

Son más fáciles de detectar y repeler ya que con solo revisar los logs del firewall o de otras herramientas de seguridad, se puede saber desde donde se realizó el ataque, el tipo de ataque y a que parte de la red se quiso afectar.

2.2.2.2.3.1 Ataques de virus informáticos

Se define como programas que contienen código malicioso que al ejecutarlos de diferentes maneras, estos desarrollan un comportamiento anormal en el computador, existen varios tipos:

- Bombas lógicas: Diseñados para activarse ante la ocurrencia de un determinado evento.
- Troyanos: Suelen propagarse como parte de programas de uso común y se activan cuando los mismos se ejecutan.
- Gusanos: Se auto duplican causando diversos efectos.
- Keyloggers: Son aplicaciones destinadas a registrar todas las teclas que el usuario aplasta en su computador.

Estos tipos de ataques también se pueden dar internamente, son más fáciles de evitar teniendo un antivirus actualizado diariamente. Incluso este tipo de ataques pueden llegar desde el exterior muy fácilmente por medio de e-mails, mensajería instantánea, etc.

2.2.2.2.3.2 Puertas traseras

Son aplicaciones cliente/servidor en el que un usuario puede tener control remotamente de otro computador y realizar diversas funciones como bloquear el teclado, etc.

2.2.2.2.3.3 Ataques de Sniffing

Consiste en interceptar el tráfico de una red, analizarlo y obtener información tal como usuarios, passwords, etc.

Este tipo de ataque generalmente sucede en redes inalámbricas no cifradas.

Para realizar este ataque se necesita un software analizador de paquetes, que hoy en día los hay gratis en Internet, una computadora con tarjeta inalámbrica y estar dentro del rango de la red inalámbrica que va a ser atacada.

2.2.3 Concepto de Seguridad Perimetral

2.2.3.1 Objetivos de Seguridad Perimetral

Los objetivos de la seguridad perimetral son:

- Proteger el perímetro de la red privada ante amenazas externas.
- Filtrar eficientemente los accesos solicitados hacia la red privada.

- Tomar acción ante cualquier amenaza antes de que acceda a la red privada.

2.2.3.2 Componentes de Seguridad Perimetral

Los componentes esenciales que pueden existir en el perímetro de una red son:

2.2.3.3 Ruteadores de Perímetro

También conocido como router perimetral [5] es típicamente un router estándar que es conectado a la LAN y proporciona una conexión serie con el mundo exterior. Se conectan a otras redes de esta manera alcanzan a través de ellos el Internet, y son a menudo el blanco de los hackers, pues buscan explotar las vulnerabilidades de seguridad. Un router de perímetro sin garantía no es sólo ineficaz para filtrar el tráfico de red no deseado, sino también puede proporcionar un blanco fácil para ataques de denegación de servicio.

Debido a que todo el tráfico de Internet de una Organización pasa por estos Router, se utiliza como un primer y último firewall, por eso se los considera críticos para la defensa.

2.2.3.4 Firewalls

Consiste en un dispositivo que analiza todo los paquetes que transitan entre la red y filtra los que no deben de ser reenviados, de acuerdo con un criterio establecido de antemano.

Existen 2 tipos de firewall, los personales que protegen a un solo equipo en el cual está instalado, o los de red que protegen a los equipos de toda una red de datos.

Para que no se convierta en cuello de botella en la red, deben de procesar los paquetes a una velocidad igual o superior al router.

Su diseño ha de ser acorde con los servicios que se necesitan tanto privados como públicos (www, ftp, telnet, etc.) así como conexiones por remotas.

Al definir un perímetro el firewall opera también como NAT (Network Address Traslation) y Proxy (servidor multipasarela).

2.2.3.4.1 Firewalls de red

Existen 3 tipos de firewalls de red:

- Los filtros de paquetes, los stateful y los deep-packet inspection.

Los filtros de paquetes sirven para controlar el acceso a determinados segmentos de red definiendo que tipo de tráfico es permitido o restringido. Los filtros de paquete analizan el tráfico en la capa 4 del modelo OSI (Transporte):

- Dirección de origen
- Dirección de destino
- Puerto de origen
- Puerto de destino
- Protocolo

Este tipo de firewalls no analizan ciertos campos de Capa 3 y 4 como el número de secuencia y banderas de control TCP. 28

Los firewall Stateful analizan toda conexión que pasa por su interfaz de red, además de analizar los campos del encabezado del paquete también analiza el estado de la conexión, que sirve para detectar otros tipos de ataques que se basan en el estado de la conexión de los paquetes.

Los firewall deep-packet inspection o de inspección profunda de paquetes analizan la información en la Capa 7 (Aplicación). Existen aplicaciones que requieren un manejo especial de los paquetes de datos cuando pasan por un firewall. Estos incluyen aplicaciones y protocolos que tienen embebidos información de direccionamiento IP en sus paquetes de datos o abren canales secundarios en puertos asignados dinámicamente (P2P). Usando inspección de aplicaciones se puede identificar los puertos asignados dinámicamente por la misma y permitir o denegar el intercambio de datos por esos puertos en una conexión específica.

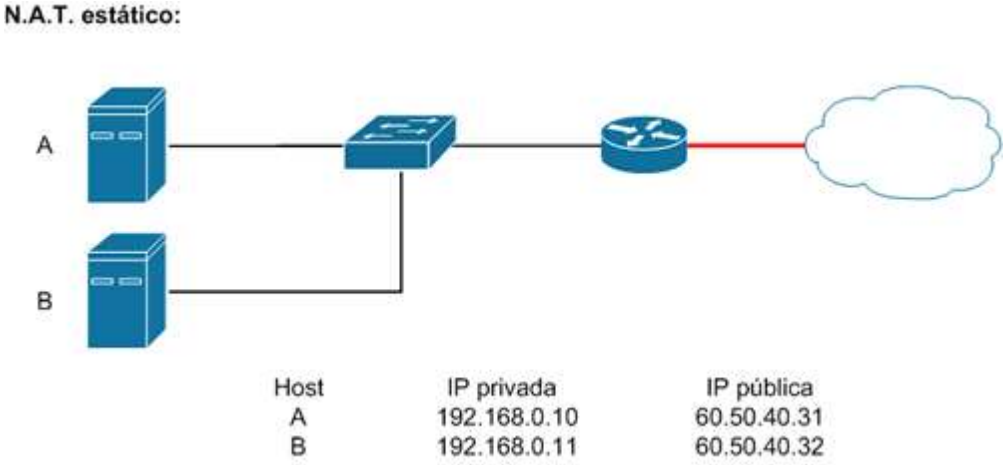
2.2.3.5 NAT (Network Address Translation)

La mayoría de firewalls existentes ofrecen el servicio de NAT[6], que consiste en enmascarar la dirección IP de los hosts con una dirección IP pública, por ejemplo, una red corporativa con 30 hosts con diferentes IP privadas dentro de la red interna, saldrán a navegar por Internet con una sola dirección IP pública.

Existen varios tipos de funcionamiento:

- Estática: Una IP privada se traduce en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. En la figura 2.3 se detalla un pequeño escenario donde es aplicado el NAT estático.

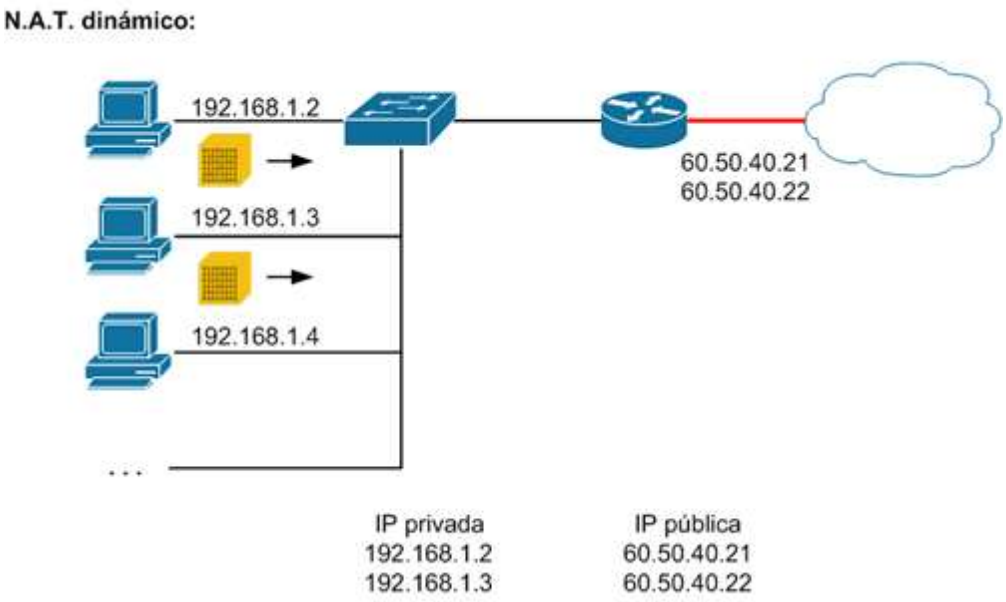
Figura 2.3: Ejemplo NAT Estático



Fuente: www.ssi-mena.blogspot.com

- Dinámica: El router tiene asignada un pool de IP públicas, de modo que cada dirección IP privada pueda usar una de las IP públicas que el router tiene asignadas. Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando. En la figura 2.4 se detalla el funcionamiento esta configuración.

Figura 2.4: Ejemplo NAT dinámico

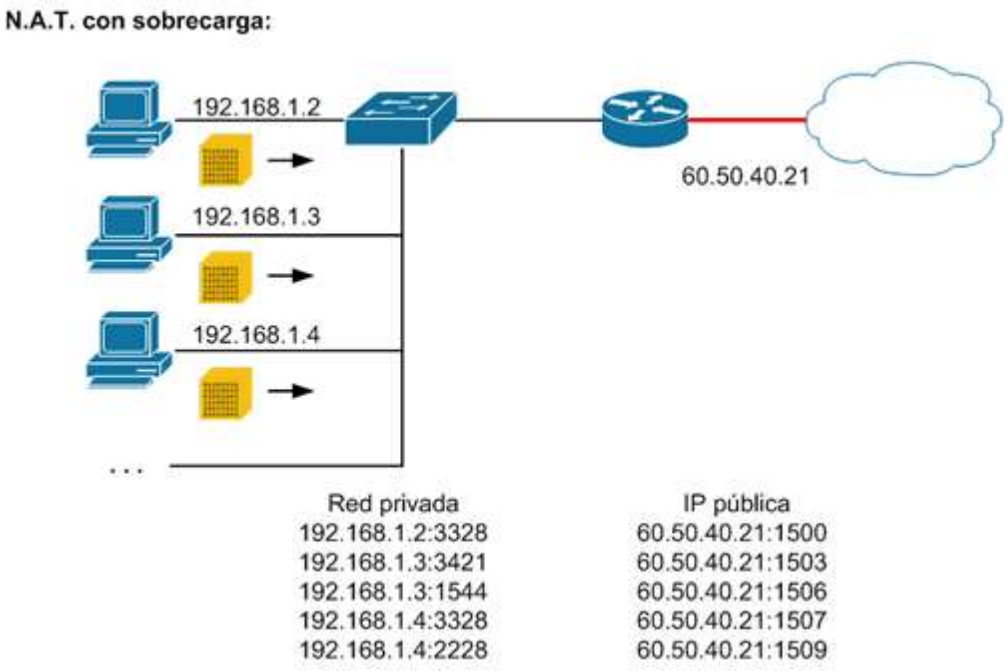


Fuente: www.ssi-mena.blogspot.com

- Sobrecarga: La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos, ya que es utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. En los protocolos TCP y UDP se disponen de un total de 65536 puertos para establecer conexiones, en la figura 2.5 se detalla un ejemplo acerca de este tipo de configuración.

  Su funcionamiento se da cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

Figura 2.5: Ejemplo NAT sobrecarga



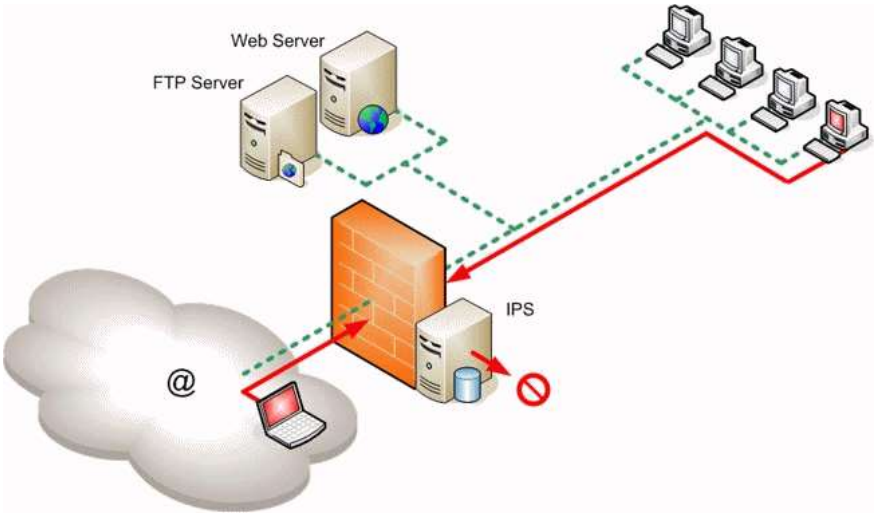
Fuente: www.ssi-mena.blogspot.com

2.2.3.6 IDS (Intrusion Detection Systems)

Un IDS [7] es un dispositivo que detecta intentos de acceso malicioso a la red privada o a hacia un host. Su utilidad es como sensores en varios puntos estratégicos de la red.

Su funcionamiento se basa en el análisis del tráfico de red, el cual al entrar en contacto con el IDS es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc… y no solo se analiza que tipo de tráfico es sino también su contenido y su comportamiento. Normalmente esta herramienta se integra con un firewall y esta combinación puede convertirse en una herramienta muy poderosa de seguridad. En la figura 2.6 se detalla una topología básica de la utilización de firewall e IPS.

Figura 2.6: Utilización de Firewall e IPS



Fuente: www.resources.infosecinstitute.com

En un sistema pasivo, el sensor detecta la posible intrusión, almacena la información y envía una señal de alerta al administrador de la red, en cambio en sistemas reactivos el IDS responde a la actividad sospechosa reprogramando el firewall para que bloquee el tráfico de donde proviene el posible ataque. Existen tres tipos básicos de IDS:

- NIDS (Network Based IDS): La mayor parte de los sistemas de detección de intrusos están basados en red. Estos IDSs detectan ataques capturando y analizando paquetes de red. Escuchando en un segmento de red, un NIDS puede monitorear el tráfico que afecta a múltiples hosts que están conectados a ese segmento, protegiendo así a estos hosts. Los IDS basados en red a menudo están formados por un conjunto de sensores localizados en varios puntos de la red. Estos sensores monitorean el tráfico de la red, realizando análisis local de este tráfico e informando ataques a la consola de gestión. Muchos de estos sensores son diseñados para correr en modo oculto, de tal forma que sea más difícil para un atacante determinar su presencia y localización.

  Ventajas:

- ❖ Los NIDSs tienen un pequeño impacto en la red, siendo normalmente dispositivos pasivos que no interfieren en las operaciones habituales de ésta.
- ❖ Se pueden configurar para que sean muy seguros ante ataques haciéndolos invisibles dentro de la red.

Desventajas:

- ❖ Pueden tener dificultades procesando todos los paquetes en una red grande o con mucho tráfico y pueden fallar en reconocer ataques lanzados durante periodos de tráfico alto.
- ❖ Los IDSs basados en red no analizan la información encriptada. Este problema se incrementa cuando la organización utiliza encriptación en el propio nivel de red (IPSec) entre hosts.
- ❖ La mayoría de los IDSs basados en red no saben si el ataque tuvo o no éxito, lo único que pueden saber es que el ataque fue lanzado. Esto significa que después de que un NIDS detecte un ataque, los administradores deben manualmente investigar cada host atacado para determinar si el intento de penetración tuvo éxito o no.
- ❖ Algunos NIDS tienen problemas al tratar con ataques basados en red que viajan en paquetes fragmentados, pues estos hacen que el IDS no los detecte o que sea inestable.

- HIDS (Host Based IDS): HIDS fue el primer tipo de IDS desarrollado e implementado. Su funcionamiento consiste en hacer uso de la información recogida de una computadora, como puede ser los ficheros de auditoría del sistema operativo. Esto permite que el IDS analice las actividades que se producen con una gran precisión, determinando exactamente qué procesos y usuarios están involucrados en un ataque particular dentro del sistema operativo. A diferencia de los NIDSs, los HIDSs pueden ver el resultado de un intento de ataque, al igual que

pueden acceder directamente y monitorizar los ficheros de datos y procesos del sistema atacado.

Ventajas:

- ❖ Los IDSs basados en host, al tener la capacidad de monitorear eventos locales a un host, pueden detectar ataques que no pueden ser vistos por un IDS basado en red.
- ❖ Pueden a menudo operar en un entorno en el cual el tráfico de red viaja encriptado, ya que la fuente de información es generada antes de que los datos sean encriptados y/o después de que el dato sea desencriptado en el host destino.

Desventajas:

- ❖ Los IDSs basados en hosts son más costosos de administrar, ya que deben ser gestionados y configurados en cada host.
- ❖ Si la estación de análisis se encuentra dentro del host monitoreado el IDS puede ser deshabilitado si un ataque logra tener éxito sobre la máquina.
- ❖ Pueden ser deshabilitados por ciertos ataques de DoS.

- DIDS (Distributed IDS): Es un IDS que opera en una arquitectura cliente-servidor, está compuesto por varios NIDS que actúan como sensores.

2.2.3.7 IPS (Intrusion Prevention Systems)

Un IPS es un sistema que establece políticas de seguridad para proteger un equipo o una red. A diferencia con un IDS que se ocupa de alertar al administrador sobre alguna actividad sospechosa, el IPS ya tiene preestablecidas políticas de seguridad que no dejarían acceder cierto tipo de tráfico o a ciertos patrones que se detecten dentro de los paquetes, en la red privada, es un tipo de protección proactiva a diferencia del IDS que es reactiva.

Tipos de Sistemas de Prevención de Intrusos (IPS)

Los IPS poseen un tipo de respuesta activa ante los ataques, es decir se aplica a cualquier función que altera o bloquea el tráfico de red como resultado de los eventos de detección de intrusión. El objetivo de la repuesta activa es automatizar la respuesta a un ataque detectado y minimizar los efectos malignos de los intentos de intrusión.

Existen cuatro estrategias distintas para la respuesta activa basada en red :

- Enlace de Datos: Deshabilita administrativamente el puerto del switch sobre el que tiene lugar el ataque.
- Red: Altera la política del firewall o router que bloquea todos los paquetes hacia o desde la dirección IP del atacante.
- Transporte: Genera mensajes resets TCP a los atacantes que usan el método del protocolo TCP o de Port Unreachable del protocolo ICMP.
- Aplicación: Altera la parte de los datos de los paquetes individuales desde el atacante. Este método requiere recalcular el checksum de la capa de transporte.

Tipos de acción de IPS

- IPS con acción de Filtrado de Paquetes.
- IPS con acción Bloqueante.
- IPS con acción de Decepción.

2.2.3.8 VPN (Virtual Private Networks)

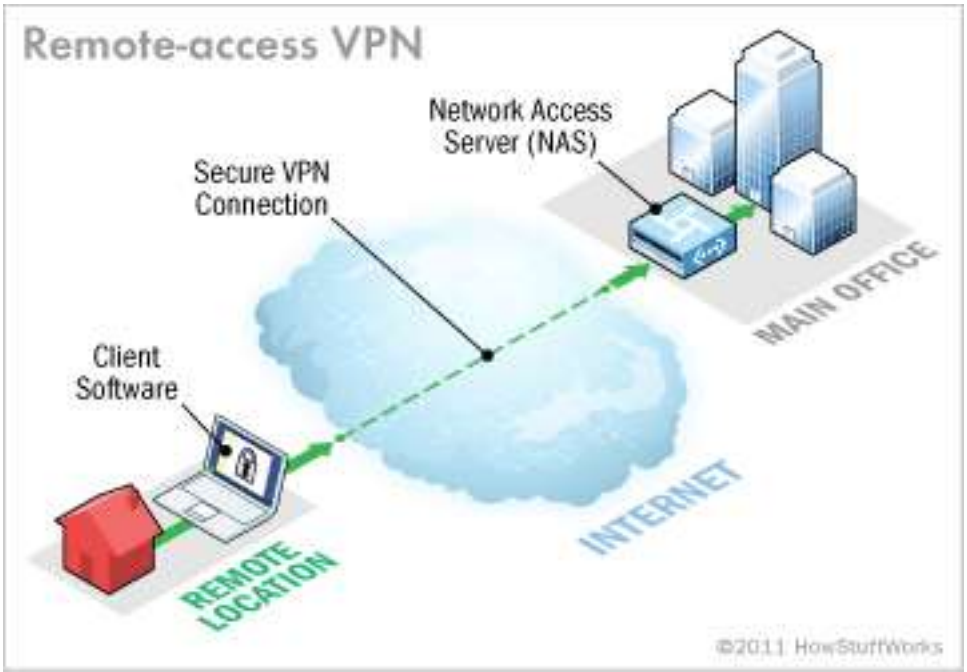
La VPN [8]es una extensión de una red local y privada que utiliza como medio de enlace una red pública como por ejemplo, Internet. También es posible utilizar otras infraestructuras WAN tales como Frame Relay, ATM, etc. Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre hosts como si fuera punto a punto. Entre una de las bondades de la VPN es que un usuario que se encuentra remotamente de la organización puede conectar individualmente a una LAN utilizando esta conexión y de esta manera utilizar aplicaciones, enviar datos,

etc. de manera segura. Las VPN utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar VPN y Redes Privadas, ya que esta última utiliza líneas telefónicas dedicadas para formar la red. Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de Internet en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta países y continentes. Por ejemplo empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación, en tanto que de otra manera habría que utilizar líneas dedicadas las cuales son muy costosas o hacer tendidos de cables que serían más costosos aun.

Ventajas de una VPN

- Seguridad: Provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.
- Costos: Ahorro de elevados costos en líneas dedicadas o enlaces físicos.
- Mejor administración: A cada usuario que se conecta se le es asignado una dirección IP asignado por el administrador, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere. En la figura 2.7 se muestra un ejemplo entre una locación remota y una oficina.

Figura 2.7: Conexión VPN



Fuente: http://computer.howstuffworks.com

2.2.3.8.1 CLASIFICACION DE VPN

Las VPNs pueden ser implementadas en HARDWARE o a través de SOFTWARE, aunque lo más importante es el protocolo que se utiliza para la implementación.

Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo Routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios.

Existen diferentes tecnologías para armar VPNs:

- DLSW: Data Link Switching(SNA over IP)
- IPX for Novell Netware over IP
- GRE: Generic Routing Encapsulation
- ATMP: Ascend Tunnel Management Protocol
- IPSEC: Internet Protocol Security Tunnel Mode

- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer To Tunneling Protocol

Diagramas

Hay varias posibilidades de conexiones VPN, las posibilidades son:

- De cliente a servidor (Client to Server): Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN.
- De cliente a red interna (Client to LAN): Un usuario remoto que utilizara servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna.
- De red interna a red interna (LAN to LAN): Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento.

Entre los más usados y con mejor rendimiento se tiene a la VPN Ipsec. A continuación se detalla su funcionamiento:

- IPSEC (Internet Protocol Secure):

  Es un protocolo de seguridad creado para establecer comunicaciones que proporcionen confidencialidad e integridad de los paquetes que se transmiten a través de Internet. IPSEC puede utilizar dos métodos para brindar seguridad, ESP (Encapsulating Security Payload) o AH (Authentication Header). La diferencia entre ambos es que ESP cifra los paquetes con algoritmos de cifrado definidos y los autentica, en tanto que AH solo los autentica. AH firma digitalmente los paquetes asegurándose la identidad del emisor y del receptor.

  IPsec tiene dos tipos de funcionamiento, el primero es el modo transporte en el cual la encriptación se produce de extremo a extremo, por lo que todas las máquinas de la red deben soportar IPsec, y el otro es el modo túnel, en el cual la encriptación se produce solo entre los

routers de cada red. Esta última opción sería la más ordenada de organizar una red VPN basada en IPsec.

2.2.3.9 SSL VPN’s

SSL (Security Sockets Layer) desarrollado por Netscape en 1994, el cual en esta primera versión no fue una versión comercial y rápidamente se migro a la versión 2.0, sin embargo ,no fue hasta su tercera versión, conocida como SSL V3.0 que alcanzo su madurez, superando los problemas de seguridad y las limitaciones de sus predecesores .

SSL proporciona los siguientes servicios:

- Cifrado de datos: La información transferida, garantiza la confiabilidad puesto que si cae en manos de un atacante, sería indescifrable.
- Autenticación de servidores: El usuario puede asegurarse de la identidad del servidor con el que establece la conexión y con el que posiblemente envíe información de carácter confidencial.
- Integridad de mensajes: Los mensajes no logran ser modificados por ningún tipo motivo mientras los paquetes viajan por internet.
- Autenticación del cliente (opcional): Esto permite al Servidor conocer la identidad del usuario, con el fin de acreditar si es que posee las credenciales necesarias para ingresar a ciertas áreas protegidas.

La VPN SSL establece una sesión codificada entre un navegador y una aplicación. Las principales características que han hecho de que sea aceptado y reconocido como una aplicación casi estándar para el comercio electrónico y las comunicaciones seguras sobre Internet es la facilidad de implantación por parte de los administradores de red y lo transparente que resulta esta aplicación para el usuario.

Las empresas pueden simplificar la creación de enlaces Internet seguros utilizando los nuevos productos que explotan el protocolo SSL ya presente en los navegadores, sin necesidad de instalar hardware VPN IPSec.

- Un usuario remoto teclea la URL de un servidor proxy/SSL situado tras el firewall corporativo.
- El usuario, una vez autenticado, recibe una lista de recursos disponibles.
- El servidor SSL/proxy facilita la comunicación entre los servidores de aplicaciones y el usuario remoto.

Características de SSL

SSL proporciona autenticación y privacidad de la información. Generalmente solo el servidor es autenticado, mientras que el cliente no se autentica, la autenticación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes. SSL permite aplicaciones cliente-servidor para evitar falsificación de identidad y mantener la integridad del mensaje.

SSL aplica una serie de fases básicas:

- Negociar entre ambos extremos el algoritmo que se utilizará en la comunicación.
- Intercambio de claves públicas y autenticación basada en cifrados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

SSL es diferente a otros protocolos en comunicaciones seguras, ya que en el modelo OSI se ubica entre capa de transporte y aplicación al igual que HTTP, FTP, SMTP, telnet, etc.

A continuación se presenta una breve descripción de las cuatro partes que componen al protocolo:

- El protocolo de registro (Record Protocol) Se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos que son objeto de la comunicación.

- Handshake que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico, es por ello que es parte importante.
- El protocolo de Alerta es el encargado de señalizar problemas y errores concernientes a la sesión SSL establecida.
- Por último, el Change Cipher Spec Protocol está formado por un único mensaje consistente en un único byte de valor 1 y se utiliza para notificar un cambio en la estrategia de cifrado.

Funcionamiento de SSL

SSL trabaja de la siguiente forma:

En primer lugar intercambia una clave de longitud de 128 bits mediante un algoritmo de cifrado el cual es asimétrico. Mediante esa clave se establece un canal seguro utilizando para ello un algoritmo simétrico previamente negociado. Tras ello toma los mensajes a ser transmitidos, los fragmenta en bloques, los comprime, aplica un algoritmo hash para obtener un resumen (MAC) que es concatenado a cada uno de los bloques comprimidos para asegurar la integridad de los mismos, luego realiza el cifrado y envía los resultados. El estado de todas estas operaciones son controladas mediante una máquina de control de estados. Una sesión SSL puede comprender múltiples conexiones.

SSL resulta muy flexible en los modelos TCP y OSI, ya que puede servir para dar seguridad a otros servicios además de HTTP para Web, solo con hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte TCP. SSL proporciona sus servicios de seguridad sirviéndose de dos tecnologías de cifrado: criptografía de clave pública (asimétrica) y criptografía de clave secreta (simétrica).

Para el intercambio de los datos entre el servidor y el cliente, utiliza algoritmos de cifrado simétrico, que pueden elegirse típicamente entre DES, triple-DES, RC2, RC4 o IDEA. Para la autenticación y para el cifrando de la clave de sesión utilizada por los algoritmos anteriores, usa un algoritmo de cifrado de

clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor una vez establecido el canal seguro.

Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea revelada por un atacante en una transacción dada, no sirva para descifrar los mensajes de futuras transacciones. Por su parte, MD5 o SHA se pueden usar como algoritmos de resumen digital (Hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Existen soluciones VPN SSL que combinan múltiples métodos de acceso en un solo dispositivo, proporcionando máxima seguridad y amplias posibilidades de acceso. El más simple es el acceso base sin clientes, que emplea funciones SSL existentes en los navegadores web, clientes de correo electrónico y dispositivos móviles estándar. Una segunda opción es la tecnología basada en agentes, que permite acceder mediante un navegador a las aplicaciones cliente/servidor. Una tercera opción también está basada en agentes y proporciona niveles de acceso ilimitados tanto al personal informático como a los usuarios especiales.

Estas opciones permiten crear grupos de usuarios que satisfagan las necesidades de cada uno según su perfil (administración, gerencia, etc.) y a los que luego se asociaran los métodos de acceso y los controles de seguridad correspondientes. El dispositivo detecta dinámicamente el tipo de conectividad dependiendo de la ubicación del usuario, del tipo de red y del dispositivo terminal utilizado, así como de los recursos a los que el usuario necesita acceder.

2.2.3.10 DMZ

Es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red. La intención de DMZ [9] es asegurar que los servidores de acceso público no puedan comunicarse con

otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido.

Los servidores en la DMZ se denominan "anfitriones bastión" ya que actúan como un puesto de avanzada en la red de la compañía.

Por lo general, las políticas de seguridad para la DMZ son las siguientes:

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ está autorizado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

Debe observarse que es posible instalar la DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

2.2.4 Concepto de Estrategia de Defensa

Una buena arquitectura de defensa trata la seguridad de la red por capas, a esto se le conoce como “Defensa en profundidad”, y ayuda a proteger los recursos de red por etapas. La defensa en profundidad comprende el perímetro, la red interna y el factor humano. Cada uno de éstos contiene varios componentes que por sí solos no son suficientes para asegurar una red, es por eso que cada uno debe ser complementario a los demás para formar una estructura de defensa óptima.

2.2.5 Concepto de Políticas de Seguridad Informática

Mantener un sistema seguro consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La confidencialidad, requiere que la información sea accesible únicamente por aquellos que estén autorizados. La integridad, que la información se mantenga inalterada ante accidentes o

intentos maliciosos. La disponibilidad significa que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos y ofrezca los recursos que requieran los usuarios autorizados cuando éstos los necesiten.

Por ende las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.

CAPITULO III: DISEÑO DE LA ARQUITECTURA DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL

3.1 Presentación del escenario de trabajo

3.1.1 La empresa

La empresa para la cual se realizó este diseño e implementación fue para Los Portales, empresa líder de la actividad inmobiliaria del Perú conformada por la alianza estratégica entre LP Holding (Grupo Raffo) e ICA de México. Más de 50 años de experiencia en el mercado nacional con cuatro unidades de negocio.

El número aproximado de trabajadores es de 500 usuarios, se estima un crecimiento del 15% anual, a su vez la empresa cuenta con distintas sucursales en las provincias del Perú.

Los Portales tuvo la necesidad de renovar, tecnológicamente hablando, esta renovación se da debido al agigantado crecimiento de la empresa lo cual se repercutió en crecimiento de clientes y a su vez de empleados.

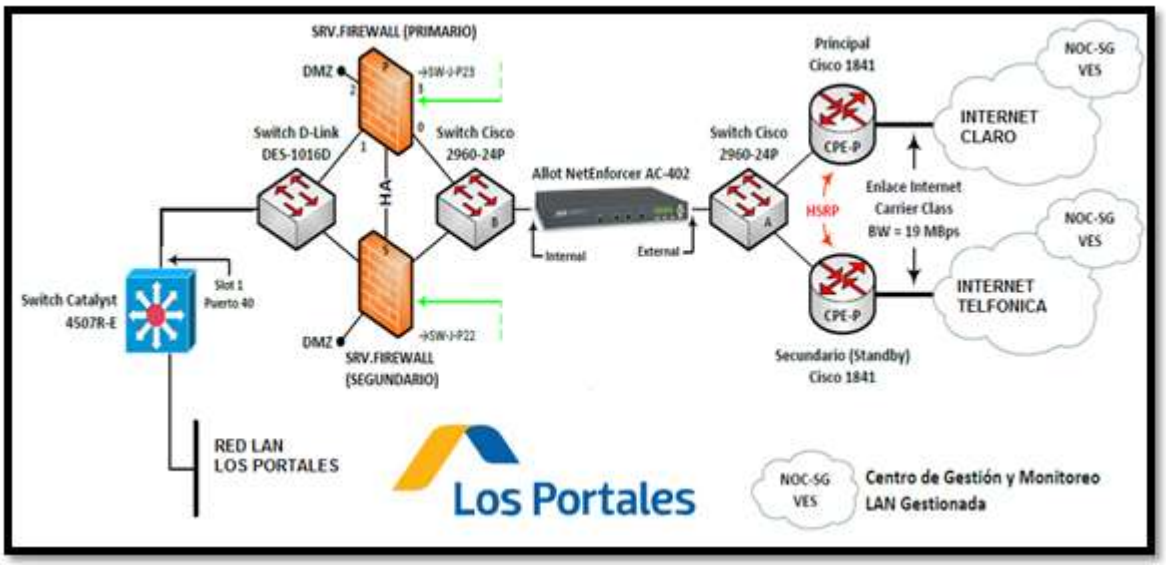
Es así que LOS PORTALES se vio en la obligación de mejorar la performance de su red, para ello debió adquirir equipos que le permitan de manera más detalla brindar un análisis y protección de su red.

Antecedentes proporcionados por el cliente:

- Cantidad de usuarios (PCs) en total: Estimado entre 500 usuarios. Estiman un crecimiento de 15% anual por año por tres años.
- Sesiones concurrentes: Picos de 14,349 sesiones concurrentes.

Se muestra en la Figura 3.1 la topología inicial del cliente LOS PORTALES.

Figura 3.1: Diagrama de red inicial



Fuente: Elaboración propia.

La red está conformada principalmente por los siguientes elementos:

- Router de Internet

  Cuenta con dos routers Cisco 1841 entregados por dos proveedores distintos de internet uno que es el principal con la empresa América Móvil y el segundo que es de contingencia con la empresa Telefónica del Perú, ambos enlaces tienen 19 Mbps dedicados, los cuales permiten la interconexión de la red la empresa con su red WAN y de tal manera tienen acceso a Internet.

- Firewall de Internet (o de perímetro)

  Cuenta con dos Firewalls Cisco Asa 5510 en alta disponibilidad con una antigüedad mayor de tres años, de los cuales se tienen las siguientes observaciones:

  - Por la antigüedad y el desmedido crecimiento de la red interna, se validación que la salud del equipo se encuentra en deterioro a nivel de recursos (CPU y memoria).

- ❖ Si bien es un Firewall con módulo UTM, los sensores IPS son muy básicos y la inspección y detección de intrusos que realiza es mínima.
- ❖ El filtro de contenidos es a nivel de categorías y no permiten restricciones ni habilitaciones puntuales.

De acuerdo al análisis realizado y la información entregada por la empresa el firewall cumple con las siguientes funciones:

- ❖ Publicación del servidor de correo para envió y recepción de correos desde internet.
- ❖ Publicación de la página web y correo web corporativo.
- ❖ Publicación mediante escritorio remoto del servidor de aplicaciones para el acceso de usuarios externos.
- ❖ Permitir la navegación de usuarios de la red interna.

- Switches

  Cuenta con 4 switches los cuales permiten la interconexión de todos los equipos de la red interna, con los equipos perimetrales, tres de los switches son capa 2 no administrables y uno de ellos es capa 3 con el cual realizan todas las vlans dentro de su red interna.

- Optimizador de ancho de banda

  Cuenta con optimizador de ancho de banda que proporciona un análisis en tiempo real, de los distintos protocolos y aplicaciones que el cliente usa en su red local.

- Servidores

  Cuenta con distintos servidores:

  - ❖ Servidor de correo Exchange 2010.
  - ❖ Servidor de directorio activo.
  - ❖ Servidor DNS.
  - ❖ Servidor de base de datos.

- Red Interna

  El cliente cuenta entre 450 y 500 usuarios, entre PC’s de escritorio y laptops.

3.2 Requerimientos de la solución

La implementación de una solución de seguridad perimetral es solo una parte de los requerimientos de la empresa en cuanto a renovación tecnológica.

A continuación se presentan todos los requerimientos de la solución manifestados por el cliente:

- Una solución que les permita proteger la red de ataques provenientes desde internet.
- Aprovechar de manera efectiva el servicio de internet, permitiendo tener visibilidad y control en todo momento del tráfico saliente y entrante.
- Control granular de acceso a Internet de direcciones URL y protocolos.
- Seguridad y granularidad en el acceso a los usuarios que se conectan de manera remota desde internet, pudiendo llevar un registro de sus accesos.
- Mínimo impacto sobre los demás elementos de red y usuarios. Es decir, que la implementación de la nueva solución de seguridad no afecte de manera negativa en la manera en que los usuarios desempeñan sus funciones.
- Presentar alta disponibilidad en el servicio, diseñando una topología que permita tener la redundancia en los equipos garantizando el servicio de Internet.

3.2.1 Requerimientos de administración y gestión

De acuerdo a las exigencias presentadas por el cliente, los requerimientos para la implementación de la solución de seguridad son:

- Gestión de la solución:
  - ❖ Regla principal

- Para la gestión de los distintos componentes de la solución de seguridad, se deben definir grupos, roles y responsabilidades para la administración lógica de los distintos componentes de la solución, de manera que sea posible identificar cada cambio realizado: sea creación o modificación de nuevas reglas en la política de seguridad.

❖ Reglas generales para el control de acceso

- Todo acceso requerido desde internet debe realizarse a través de un medio seguro y encriptado.
- Bloquear todo tráfico entrante/saliente no declarado como permitido.
- Implementar una DMZ que filtre y analice cualquier tráfico, para prohibir el acceso directo desde y hacia Internet, desde la red de usuarios.
- Utilizar NAT para enmascarar todo el tráfico saliente hacia Internet.
- No permitir la conexión de direcciones de red internas desde Internet hacia la DMZ.

❖ Reglas de asignación por usuario

- Identificar a todos los usuarios con un único usuario antes de brindarle acceso a los sistemas desde internet.
- Implementar autenticación para todos los usuarios a través de una base de datos de un servidor LDAP o Active Directory.
- Implementar autenticación local, en el mismo firewall, para el acceso remoto de los empleados, administradores y terceros.
- Habilitar el acceso compartido remoto con el proveedor de seguridad para obtener un apoyo técnico y monitoreo del equipo.
- Requerir una longitud mínima de las contraseñas a un mínimo de 9 caracteres.
- Forzar que las contraseñas de los usuarios cuenten con caracteres numéricos y alfanuméricos.

        - Prohibir el re-uso de contraseñas con una antigüedad menor a cinco cambios.
        - Bloquear una cuenta de usuario luego de seis intentos fallidos de acceso.
    - ❖ Política de evaluación constantemente la seguridad de los sistemas y procesos
        - Mantener actualizado con la última versión de firmware de cada uno de los dispositivos dedicados a la seguridad perimetral.
        - Realizar pruebas de penetración al menos una vez al año y cada vez que se realice una modificación en la red.
        - Utilizar sistemas de detección de intrusos para monitorear todo el tráfico de la red y alertar sobre eventos sospechosos.
        - Mantener los detectores de intrusos actualizados.
        - Realizar escaneos de vulnerabilidades externos e internos constantemente y cada vez que se implemente un nuevo sistema, componente de red, o se realice algún cambio en la topología de la red o a nivel del firewall.

3.2.2 Requerimientos técnicos

Los requerimientos técnicos de la solución son los siguientes:

- Capacidad de alta disponibilidad en modo activo-pasivo en ambos firewalls.
- Capacidad de configuración de enlace de respaldo en el firewall perimetral.
- Aplicación de filtro de paquetes dinámico en los firewalls.
- Bloqueo de ataques de negación de servicio.
- Capacidad de bloqueo de ataques o intentos de intrusión.

Adicionalmente existen requerimientos específicos para cada elemento de seguridad, los cuales serán utilizados para el criterio de selección de los equipos a utilizarse para construir la solución.

- Firewall Perimetral
  - ❖ Servicio DHCP para la interfaz LAN.
  - ❖ Capacidad de realizar balanceo de enlaces.
  - ❖ Capacidad de dominar distintos protocolos de enrutamiento (BGP, OSPF).
  - ❖ Capacidad de poder integrarse con el Directorio Activo o LDAP.
  - ❖ Capacidad para configurar túneles VPN.
  - ❖ Soporte de IPv6.
  - ❖ Soporte de traslación de direcciones de red (NAT, NAPT, PAT).
  - ❖ Soporte de VoIP.
  - ❖ Soporte de protocolo SPDY.
  - ❖ Control de flujo y ancho de banda.
  - ❖ Capacidad de prevención de intrusos, filtro de contenido y antivirus embebido.
  - ❖ Capacidad de manejar más de un enlace hacia internet.
- Control de Acceso Remoto (VPN SSL)
  - ❖ Acceso basado en políticas.
  - ❖ Capacidad de otorgar los accesos por dirección destino y puerto o aplicación, por usuario o grupo de usuarios, y por horarios (granularidad).
  - ❖ Control de acceso de acuerdo a regulaciones de seguridad.
  - ❖ Comunicación encriptado entre el cliente y el dispositivo VPN.
  - ❖ Soporte para equipos Mac de Apple, Windows, IOS y Android.
- Control de acceso a Internet
  - ❖ Capacidad de control a nivel de horarios.
  - ❖ Control de acceso por HTTP y HTTPS.
  - ❖ Control a nivel de inspección SSL.
  - ❖ Capacidad de aplicar políticas por usuarios y grupos de usuarios.
  - ❖ Filtro de protocolos de Internet.
  - ❖ Capacidad para filtrar direcciones en internet por su dirección y/o su dirección IP.

- ❖ Capacidad de permitir o denegar a nivel de aplicativos (Skype, Gmail chat).
- ❖ Capacidad de permitir o denegar páginas en internet por categorías.
- ❖ Capacidad para permitir o denegar direcciones en internet a través de un perfil de control de aplicación.

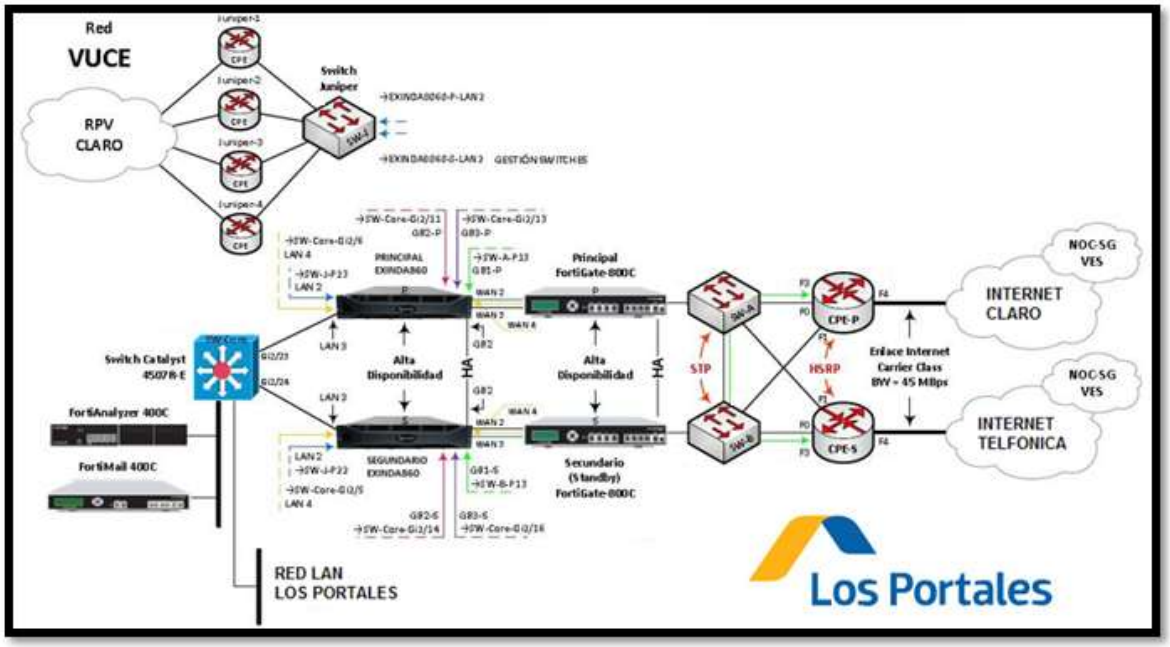
- Control de correos electrónicos
  - ❖ Inspección del correo en busca de ataques dirigidos contra el servidor de correo.
  - ❖ Capacidad de identificar el correo spam y enviarlos a cuarentena.
  - ❖ Detectar virus contenido en los archivos adjuntos de los correos externos enviados hacia los usuarios.
  - ❖ Manejar una lista Negra que deniegue un dominio especifico.
- Monitoreo almacenamiento de logs y reportes personalizados
  - ❖ Monitoreo 24x7 del tráfico y de los servicios generados en los equipos de seguridad.
  - ❖ Capacidad de almacenamiento de logs como mínimo 3 meses.
  - ❖ Capacidad de visualización de los eventos suscitados en la red en tiempo real
  - ❖ Reportes personalizados y generados automáticamente, estos reportes deben ser enviados a la bandeja de entrada del administrador de red en formato pdf.

3.3 Diseño de la nueva arquitectura de seguridad perimetral

3.3.1 Nueva arquitectura

De acuerdo a los requerimientos presentados por Los Portales, la arquitectura de red propuesta es la mostrada en la Figura 3.2.

Figura 3.2: Diagrama de red propuesta.



Fuente: Elaboración propia.

Si bien el diagrama contempla la arquitectura propuesta para toda la red de datos de LOS PORTALES, para efectos de la presente tesis, se describe únicamente la arquitectura propuesta para la seguridad perimetral, por ende la arquitectura de seguridad perimetral contempla:

- La implementación de un firewall perimetral que cumpla las funciones de control de acceso desde y hacia internet; a su vez debe cumplir con los requerimientos técnicos expuestos en el punto 3.2.2. Nuestro firewall contará con tres zonas de seguridad:
  - ❖ Zona Internet. Esta es la zona, en donde está conectado la interfaz del firewall con el dispositivo switch, el cual se encuentra ubicado detrás del router primario (CPE-P) y encargado de conmutar con el router segundario (CPE-S) del proveedor de Internet, con la finalidad de mantener el servicio de Internet ante cualquier eventualidad.
  - ❖ Zona DMZ. En esta zona se ubicará la granja de servidores de LOS PORTALES, desde este interfaz se realizará las publicaciones de los servicios hacia Internet.
  - ❖ Zona Interna. En esta zona se encontrará todo los usuarios de LOS PORTALES que deban salir hacia Internet o acceder a los servicios

internos, dependiendo de los permisos o privilegios con los que cuente cada usuario o grupos de usuarios.

- El firewall también cumplirá las funciones de motor IPS, motor antivirus y motor DoS para proteger los servidores, será un escudo ante las amenazas que provengan desde el exterior. Adicional a la seguridad perimetral el firewall trabajará como un concentrador VPN-SSL. El cual tendrá la función de proveer el acceso a usuarios remotos de manera granular y garantizando la seguridad en la conexión.
- La implementación de un equipo Antispam se comportará como un sistema de relay SMTP, llevando a cabo las labores de inspección del correo en busca de ataques dirigidos en contra del servidor de correo, así como la inspección de correos spam. Su ubicación estará detrás del switch core de capa 3.
- La implementación de un equipo Analizador que realice el monitoreo sobre los eventos registrados a nivel de Firewall, ataques, virus, VPN, utilización web, análisis forense, etc. Adicional que realice la funcionalidad de escaneo de vulnerabilidades en los servidores de LOS PORTALES, esto nos permitirá identificar los fallos del sistema operativo y de los servicios. Su ubicación estará detrás del switch core de capa 3.

Es importante recordar que en éste punto se presenta únicamente cómo estarán interconectados los componentes propuestos. La configuración y política que se les aplicará será vista más adelante.

3.4 Componentes de la nueva arquitectura de seguridad perimetral

El detalle de los componentes que conforman el nuevo diseño se presenta a continuación.

3.4.1 Firewall Perimetral

El firewall o cortafuegos perimetral está diseñada para bloquear el acceso no autorizado, desde fuera de la red y permitiendo al mismo tiempo comunicaciones autorizadas a través de un lista de acceso y políticas.

Entre las funciones principales del firewall tenemos:

- Concentrador VPN

  Cumplirá la función de crear un canal de comunicación seguro que le permita a un usuario ubicado en Internet acceder a los recursos de la red interna según el perfil de acceso asociado a su cuenta de usuario. El canal seguro estará conformado por un túnel VPN cifrado con un certificado SSLv2 de 128 bits entre el concentrador VPN y la computadora o dispositivo móvil del usuario.

  Para que el usuario pueda conectarse vía VPN, es necesario que ingrese al portal web publicado en HTTPS por el concentrador VPN SSL, ingresar su cuenta de usuario y contraseña. Una vez que estos datos son validados, se crea automáticamente el canal seguro entre el equipo y la computadora del usuario.[10]

- Detección de intrusos (IDS)

  Cumplirá la función de Detección de Intrusión, se constituye de un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red.

  El motor IDS provee seguridad hasta la capa de aplicación, sin mermar por ello el rendimiento de la red. La capacidad de IDS del firewall se basa en el módulo de routing, el módulo de firewall y la capa de aplicación. De esta forma el sistema de detección de intrusiones no se limita únicamente a la detección de ataques de nivel de red ni tampoco al análisis individual de cada paquete. El firewall reensambla el contenido de los paquetes en línea y lo procesa para identificar ataques hasta el nivel de aplicación. [11]

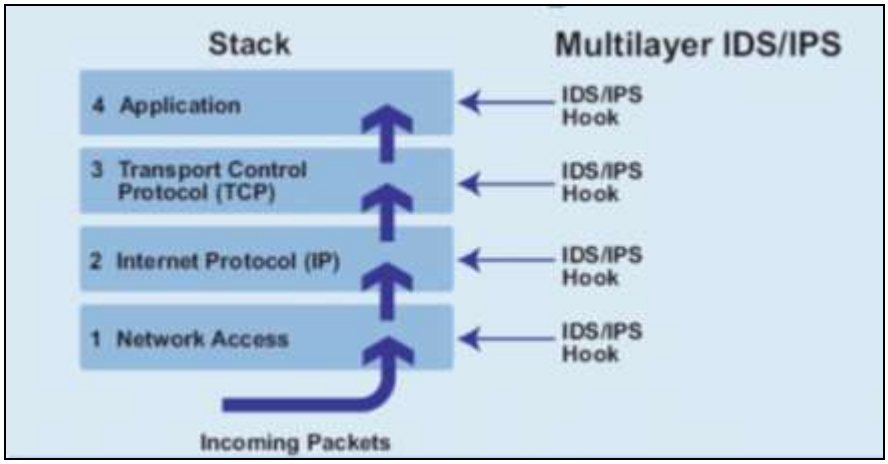
- Prevención de intrusión (IPS)

  La funcionalidad IPS del cortafuego detecta y previene los siguientes tipos de ataques:

  - ❖ Ataques de Denegación de Servicio (DoS), intentan denegar el acceso a servicios u ordenadores mediante la sobrecarga del enlace de red, de la CPU u ocupación de discos duros. El atacante no intenta conseguir información, sino interferir los accesos a los recursos de red, ejemplo inundación de paquetes, incluyendo Smurf flood, TCP SYN flood, UDP flood, y ICMP flood.
  - ❖ Ataques de Reconocimiento, son aquellos ataques a través de los cuales el atacante intenta conseguir información sobre un determinado sistema con objeto de preparar un posterior ataque basado en vulnerabilidades específicas, ejemplo port scans, buffer overflows, y OS identification.
  - ❖ Exploits, intentos de aprovecharse de vulnerabilidades o bugs conocidos de aplicaciones o sistemas operativos con el objeto de ganar acceso no autorizado a equipos o redes completas ejemplos CGI Scripts, incluyendo Phf, EWS, info2www, TextCounter, SMTP (SendMail) attack, DNS attacks, IP spoofing, Web Server attacks, Web Browser attacks; URL, HTTP, HTML, JavaScript, Frames, Java, y ActiveX.
  - ❖ Ataques de Evasión de Sondas IDS, consisten en técnicas para evadir sistemas de detección de intrusiones. El IPS de la plataforma del firewall detectará las siguientes técnicas de evasión de NIDS: Signature spoofing, Signature encoding, IP fragmentation, y TCP/UDP disassembly.

  En la figura mostrada se valida el flujo para los sensores IDS/IPS.

Figura 3.3: Multicapa IDS/IPS. [11]



Fuente: www.ipseclab.eit.lth.se

Si el sistema detecta la existencia de un archivo infectado en una transmisión, el archivo es eliminado o guardado en cuarentena, y es sustituido por un mensaje de alerta configurable por el administrador. Además, el firewall guarda un registro del ataque detectado, y puede configurarse el envío de un correo de alerta o un trap SNMP.

Al existir una integración con la funcionalidad VPN en la plataforma, es posible analizar la existencia de virus también este tipo de tráfico.

El servicio de protección antivirus provisto por el firewall es totalmente transparente para los usuarios finales. [12]

- Web Filtering

  La distribución y visualización de contenido no autorizado supone un riesgo importante para cualquier organización. Para las empresas, la monitorización del uso que sus empleados hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados o no autorizados se ha convertido en algo necesario, justificado por los costes financieros y las implicaciones legales que conlleva la pasividad en este aspecto.

El servicio web filtering puede ser configurado para escanear toda la cadena del contenido del protocolo http y https permitiéndonos filtrar direcciones URL potencialmente no asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos.

La funcionalidad de filtrado web puede definirse mediante listas creadas por el propio usuario, o bien mediante la utilización de una base de datos la cual a diario debe ser actualizada por el vendor.

- Filtrado de Tráfico Web (URL Web Filtering)

  El filtrado de URL puede implementarse utilizando bases de datos locales con listas black/white list definidas por el usuario que contienen URLs cuyo acceso está permitido o denegado. El acceso a URLs específicas puede ser bloqueado añadiéndolas a la lista de bloqueo de URLs.

  El firewall bloquea cualquier página web que coincida con la URLs especificada y muestra un mensaje de sustitución de la misma al usuario.

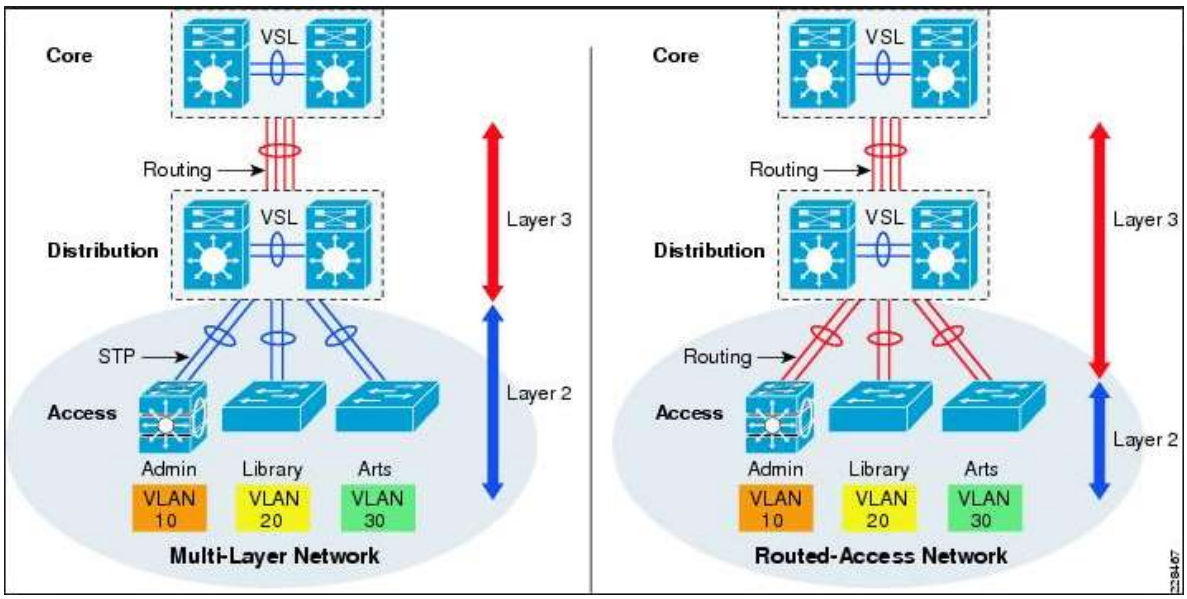
  La lista puede incluir direcciones IP, URLs completas o URLs definidas utilizando caracteres comodines o expresiones regulares. Asimismo, la lista puede ser creada manualmente o importada desde listas de URLs elaboradas por terceros.

  Asimismo, con objeto de prevenir el bloqueo de páginas web legítimas no intencionado, las URLs pueden ser añadidas a una lista de excepción que sobrescribe la URL bloqueada y listas de bloqueo de contenido. El bloqueo de URL puede ser configurado para bloquear todo o sólo algunas de las páginas de un sitio web. Utilizando esta característica es posible denegar el acceso a páginas embebidas dentro de una dirección web sin denegar el acceso completo al sitio en cuestión.

- Layer 2/3 routing

  El firewall también puede trabajar con enrutamiento dinámico, soportando RIP (v1 y v2), OSPF y BGP, así como con enrutamiento multicast (PIM sparse/dense mode), además de trabajar con enrutamiento estático y ofrecer la posibilidad de realizar policy routing, tal como se muestra en la siguiente figura 3.4.

Figura 3.4: Límites de múltiples capas y Diseño de Redes con acceso enrutado.



Fuente: www.cisco.com

- Alta Disponibilidad

  La capacidad de trabajar en cluster de alta disponibilidad (HA) dota a los firewalls de redundancia ante fallos. Además el cluster puede configurarse en modo activo-activo haciendo balanceo de carga del tráfico o en modo activo/pasivo en la que un único equipo procesa el tráfico de la red y es monitorizado por los demás para sustituirle en caso de caída.

  Un clúster activo-pasivo consiste en un equipo firewall primario que procesa todo el tráfico y uno o más equipos subordinados que están conectados a la red y al equipo primario, pero no procesan tráfico alguno.

El modo activo-activo permite balancear la carga de tráfico entre las diferentes unidades que componen el clúster. Cada firewall procesa activamente las conexiones existentes y monitoriza el estado de los otros nodos del clúster. El nodo primario procesa el tráfico y redistribuye el tráfico entre los diferentes equipos que forman parte del clúster.

3.4.2 Equipo Antispam

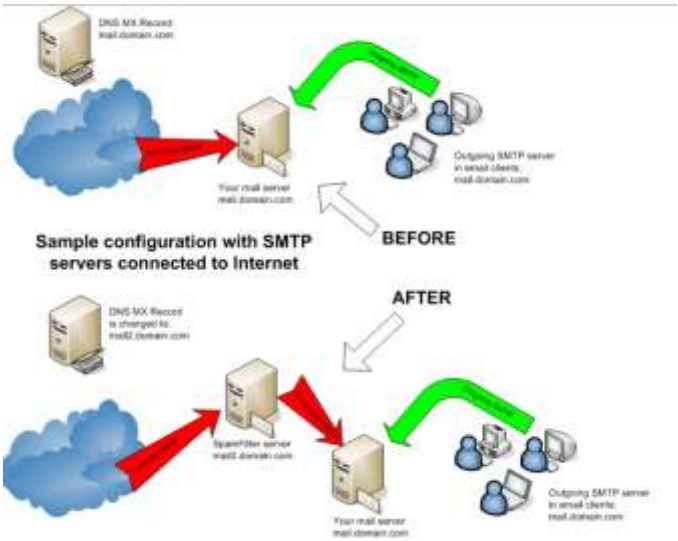
Cumplirá la función de retener todo correo considerado como no deseado o “correo basura” mediante diferentes técnicas que incluyen: método heurístico de detección de spam, políticas de control de contenido, consultas de reputación de direcciones IP y listas negras, entre otros.[13]

Los únicos canales de comunicación necesarios para el funcionamiento del antispam son: comunicación mediante el protocolo SMTP con el servidor de correo de manera bidireccional, al igual que hacia Internet; y acceso a Internet vía DNS para realizar sus consultas con los servidores de listas negras y de reputación, y HTTPS para actualizar su motor antispam. Operando en modo Gateway.

El antispam se comporta como un sistema de relay SMTP, llevando a cabo las labores de inspección del correo en busca de ataques dirigidos contra nuestros servidores o relays de correo, así como la inspección antivirus y Antispam, y las labores de enrutamiento de correo necesarias cubiertas por un sistema con un muy elevado rendimiento. Este modo de funcionamiento requiere de ciertos cambios en el sistema de correo para realizar las funciones de inspección de correo. Dichos cambios, principalmente, cubren modificaciones en los registros MX de los DNS así como cambios en el enrutamiento SMTP en el caso que se requiera hacer inspección en los correos salientes.

En la figura 3.5 se puede ver una topología que cuenta con un servidor de correos con salida hacia internet sin mayor seguridad y una topología simple que cumple con el estándar mínimo de seguridad.

Figura 3.5: Servidor de correo sin/con AntiSpam. [13]



Fuente: www.ccm.net

3.4.3 Monitoreo, repositorio de logs y reportes

El monitoreo de la estabilidad y la salud de los equipos de seguridad perimetral es un factor importante debido a que del mismo se podrá validar si es que hay un problema de ataque a la red del cliente, un intento de deshabilitación de los equipos, una caída de flujo eléctrico o si los recursos de los equipos se encuentran elevados.

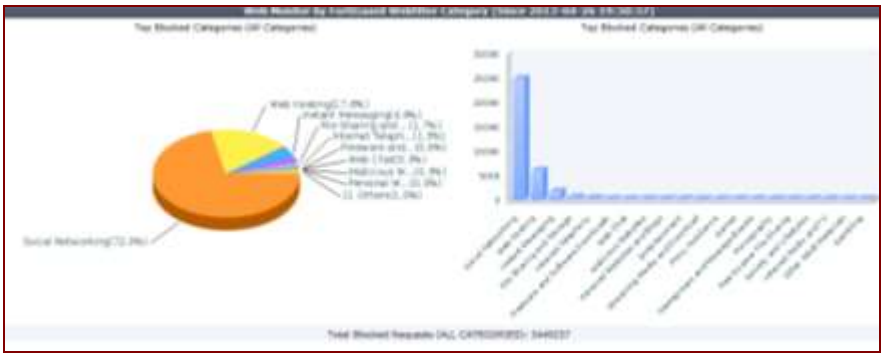
Un repositorio de logs es una plataforma dedicada al registro centralizado de logs, la gestión y tratamiento de los mismos. El mismo debe poseer la capacidad de generar más de 350 informes diferentes que nos aportan información detallada sobre los eventos registrados a nivel de firewall, ataques, virus, VPN, utilización web, análisis forense, etc. Ayuda al monitoreo de la red almacenando los logs en tiempo real, provenientes del firewall, pudiendo detectar un ataque o un mal uso de los recursos de ancho de banda de uno o varios usuarios que no cuentan con una adecuada política de seguridad.

Entre los posibles informes cabe destacar:

- Informes de ataques: ataques registrados por cada equipo firewall, señalando el momento en el que son registrados, e identificados a las fuentes más comunes de ataque.
- Informes de virus: top virus detectados, virus detectados por protocolo.
- Informe de Eventos: eventos propios del dispositivo, eventos de administración del sistema, eventos de accesos, etc.
- Informe de utilización del correo electrónico: usuarios más activos en envío y recepción, ficheros adjuntos bloqueados identificados como sospechosos.
- Informe de utilización del tráfico web: usuarios web top, sitios bloqueados, usuarios de mayor frecuencia de intento de acceso a sitios bloqueados, etc.
- Informe de utilización de ancho de banda: informes de uso del ancho de banda por usuario, día, hora y protocolo.
- Informes por protocolo: Protocolos más utilizados, usuarios ftp /telnet top.
- El repositorio de logs incluye un registro histórico y en tiempo real del tráfico de cada uno de los equipos gestionados, así como una herramienta de búsqueda en los logs.
- El repositorio de logs presenta una gama amplia de informes con soluciones para todo tipo de proyectos.

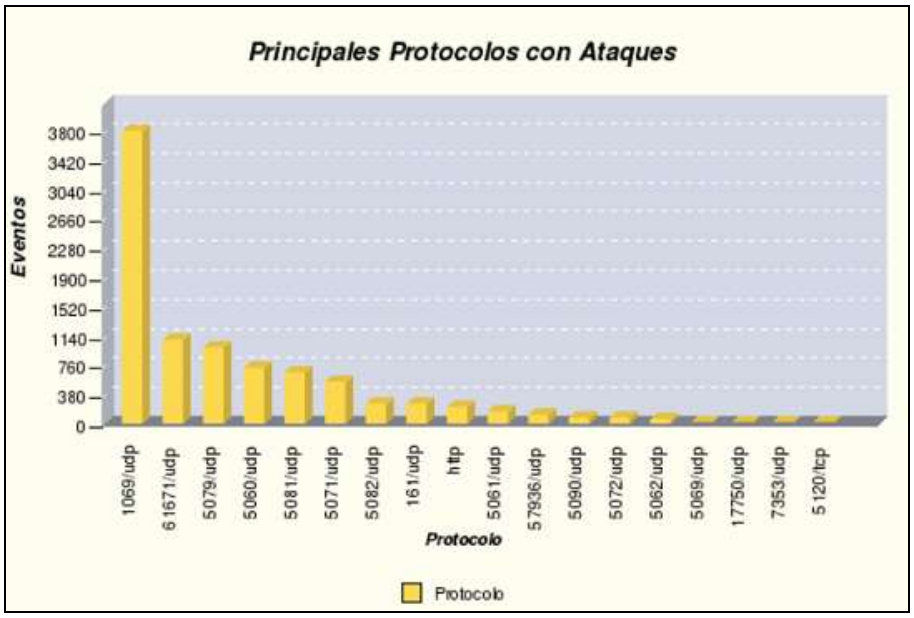
En las figuras 3.6, 3.7 y 3.8 se validan ciertos ejemplos sobre el informe grafico de los reportes.

Figura 3.6: Monitoreo en tiempo real.



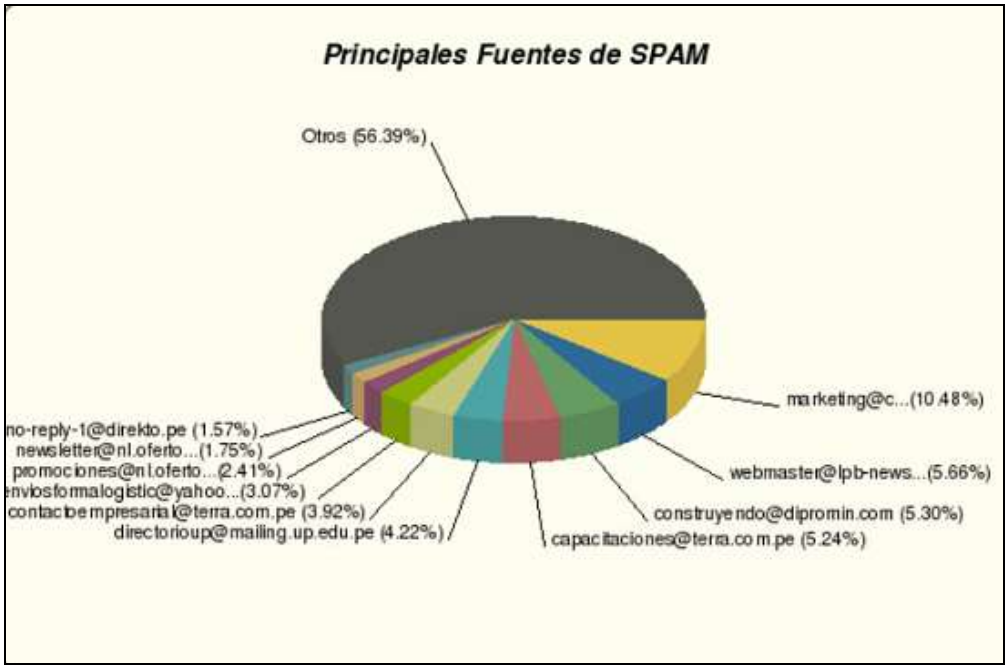
Fuente: Elaboración propia

Figura 3.7: Reporte de ataques por protocolos



Fuente: Elaboración propia

Figura 3.8: Reporte de las principales fuentes de spam



Fuente: Elaboración propia

CAPÍTULO IV: SELECCIÓN DE LOS COMPONENTES DE LA SOLUCIÓN DE LA SEGURIDAD PERIMETRAL.

Existen dos criterios que fueron tomados en cuenta para la elección de Fortinet como la solución final:

4.1 Evaluación tecnológica

Contempla cuán bien cumple el fabricante con los requerimientos de la empresa.

4.1.1 Selección del fabricante

Se realizó un análisis con diversas marcas conocidas en el mercado a nivel de seguridad informática tales como Checkpoint, Palo Alto, Juniper, Cisco, Sophos, etc. Si bien todas las marcas pueden cumplir casi con la totalidad de los requerimientos del cliente, sin embargo, como primer paso es importante conocer el posicionamiento en el mercado internacional y local de cada uno de ellos. Tener conocimiento de qué marcas son líderes en sus respectivos rubros y más aún, su comportamiento en los últimos tiempos. Es decir, si se mantuvieron como líderes, o si su ubicación privilegiada es tan solo momentánea, es un dato muy útil para elegir la mejor solución.

Existen empresas que se dedican a analizar las diferentes tecnologías en el aspecto técnico como en el comercial. Una de ellas, y la más reconocida a nivel mundial es Gartner.[14].

Gartner es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford,Connecticut, Estados Unidos, que tiene por finalidad comparar estas empresas en función de su historia, participación y crecimiento en el mercado, productos y servicios que ofrece, y su capacidad de mantenerse a la vanguardia tecnológica, proveyendo nuevas tecnologías y productos. El detalle de los criterios y metodología utilizados por Gartner para evaluar a las empresas se encuentra en su página web.

4.1.2. El cuadrante mágico de Gartner

Gartner utiliza diferentes criterios para evaluar las diferentes tecnologías y fabricantes. Esta información está disponible en la URL de Gartner, sin embargo explicaremos las cuatro categorías en las cuales se pueden ubicar los diferentes fabricantes.

- Líderes (Leaders)

  Los líderes son aquellos que se ubican en el mercado de empresas medianas y grandes, teniendo en cuenta que todos sus productos están desarrollados para empresas grandes. Adicionalmente han mostrado un gran y progresivo progreso en sus tecnologías a través del tiempo, haciendo que la valla tecnológica sea más alta para todos los competidores y tienen la capacidad, incluso cambiar el curso de la industria.

- Competidores (Challengers)

  El cuadrante de competidores contiene vendedores que tienen una buena ubicación en el mercado pero no son líderes en términos tecnológicos. Cuentan con una fuerza de ventas agresiva y son muy buenos para cerrar contratos, sin embargo sus productos cuentan con un limitado número de funciones avanzadas.

- Visionarios (Visionaries)

  Son aquellos que tienen buenos diseños y funcionalidades para el mercado, muchos de ellos pueden considerarse como productos de “siguiente generación”, pero no cuentan con una buena base comercial, estratégica o económica para competir con los líderes y competidores; o influenciar en el curso de la industria.

- Jugadores de base (Niche Players)

Usualmente son fabricantes que se adecuan rápidamente a los cambios en el mercado pero no pueden definir su curso. La mayoría son pequeños vendedores con soluciones para empresas pequeñas.

En los estudios publicados por Gartner a mediados del 2013 y 2014, Fortinet [15] se ubica en el cuadrante de líderes de Gestión Unificadas de Amenazas los dos últimos años.

De tal manera se muestra el cuadrante mágico de Gartner durante los años 2013 y 2014 en las siguientes figuras 4.1, 4.2.

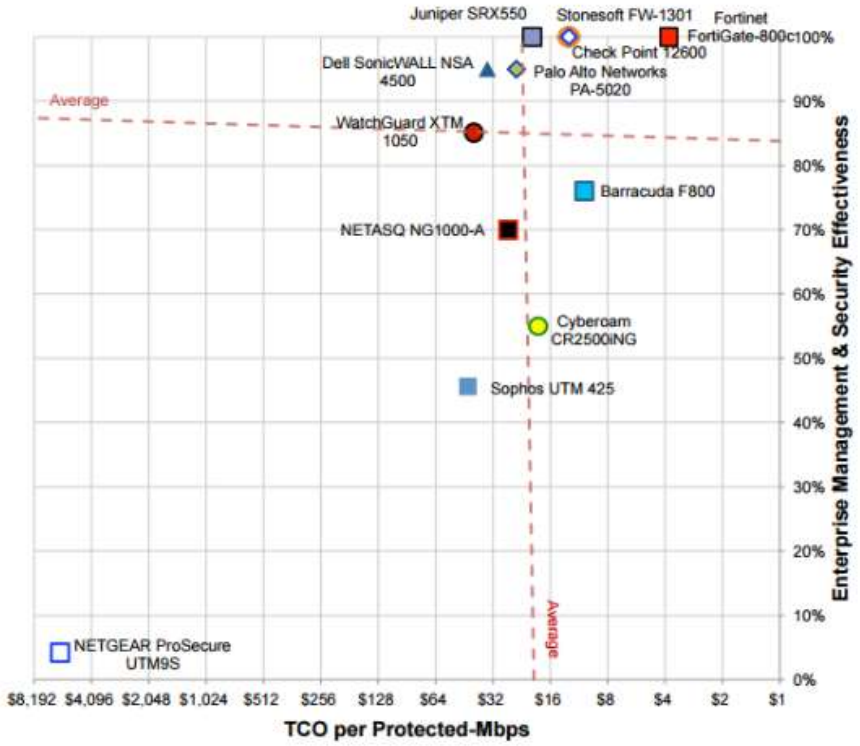
Figura 4.1: Cuadrante mágico de Gartner 2013.

Fuente: www.fortinet.com

Figura 4.2: Cuadrante mágico de Gartner 2014.

Fuente: www.fortinet.com

Figura 4.3: Cuadrante mágico de Gartner 2014 – Firewalls



Fuente: www.fortinet.com

Entre las opciones más recomendadas según la Figura 4.3 se evaluaría los equipos firewall según sus funcionalidades del equipo.

Tabla 4.1: Listado de equipos firewall

Producto	Administración y Protección	Valor	Generalidades
Barracuda F800	Neutro	Recomendado	Neutro
Check Point 12600	Recomendado	Recomendado	Recomendado
Cyberoam CR2500ING	Bajo	Neutro	Neutro
Dell SonicWALL NSA 4500	Recomendado	Neutro	Neutro
Fortinet FortiGate 800C	Recomendado	Recomendado	Recomendado
Juniper SRX550	Recomendado	Recomendado	Recomendado
Palo Alto Networks PA-5020	Recomendado	Neutro	Neutro

Fuente: Elaboración propia

Entre los 03 equipos más recomendados revisariamos con que funcionalidades cuentan dichos dispositivos.

Tabla 4.2: Funcionalidades de Firewall

	Fortinet	Juniper SRX	Check Point
Firewall	●	●	●
VPN	●	●	●
Application Control	●	●	●
IPS	●	●	●
Web Filtering	●	●	●
Anti-botnet	●	●	●
Anti-Spam	●	●	●
Virtual Domain	●	●	●
Wireless LANController	●	●	●
WAN Optimization	●	●	●
Vulnerability Assessment	●	●	●
Endpoint Control	●	●	●

Fuente: Elaboración propia

De los resultados de la Tabla 4.2 podríamos realizar un análisis comparativo entre los equipos Juniper SRX 550 y FortiGate 800C, tal como se indica en la Tabla 4.3.

Tabla 4.3: Carateristicas Técnicas

	Juniper SRX550	FortiGate 800C
Firewal Performance	5.5 Gbps	20 Gbps
IPS performance	800 Mbps	6 Gbps
AES256+SHA-1 /3DES+SHA-1 VPN performance	1.0 Gbps	1.3 Gbps
Maximum concurrent session	375,000	7 000000
New sessions / second (sustained, TCP,3-way)	27,000	190000
Maximum security policies	7,256	100,000
High Availability	Active/Active Active/Pasive	Active/Active Active/Pasive , Clustering
10/100/1000 Ethernet	10 ports	12 ports

Fuente: Elaboración propia

Del comparativo en la Tabla 4.3 debido al alto performance que tiene el equipo FortiGate 800C sobre el equipo Juniper, se erigiría la primera opción.

Para la elección del equipo AntiSpam se hizo un listado con las necesidades específicas del cliente. Se detalla en la Tabla 4.4.

Tabla 4.4: Características AntiSpam

	Fortinet	Barracuda	IronPort	Secure Computing	BorderWare
ICSA Labs Anti-Spam Certified					
All technology developed in-house					
No per-user licensing fees					
Bi-directional inspection					
Transparent/Server Mode					
On-box archiving					
Local sender reputation					
Dynamic heuristic rule updates					
Greylisting					
High availibility configurations					
Basic-mode GUI					
User-defineable dictionaries					
Part of a complete security solution					

Fuente: Elaboración propia

Siendo estas necesidades cubiertas por los equipos Fortinet y IronPort

Se tendría que elegir un modelo representativo por cada una de estas 02 marcas, respetando las características solicitadas por el cliente.

Tabla 4.5 Características Técnicas

Performance	IronPort C370	FortiMail 400C
Storage	1.2 TB	2 TB
RAID Mirroing	RAID 10	Software: 0,1
Memory	4 GB	4 GB
CPU	1x4	1x4
Email Domains	500	500
Recipient based policies -incoming or outcoming	800/2000	600/3000
Server Mode Mailboxes	10,000	1,000
Antispam,Antivirus, Authentication and Content Profile	50/100	50/200

Fuente: Elaboración propia

De la Tabla 4.5 el equipo FortiMail 400C es el que cuenta con más prestaciones, es un equipo mucho más robusto en cuanto a las especificaciones técnicas.

Para la elección del equipo Recolector de Logs, se procedió la selección bajo las decisiones de los equipos anteriores, bajo el criterio de que es la opción más adecuada contar con toda la solución enfocada en una sola marca, ya que tendremos mejores resultados ante la interacción entre estos equipos, debido a su compatibilidad.

Figura 4.4 Modelos de FortiAnalyzer

FortiAnalyzer	100C	400C	1000C	2000B	4000B
Hardware Specification					
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes
10/100/1000 Ethernet	2	4	4	6	2
10/100 Ethernet	1	0	0	0	0
1GbE SFP	0	0	0	0	2
Number of Hard Drives	1	1	1 (Three Drives Optional)	2 (Four Drives Optional)	6 (Eighteen Drives Optional)
Total Hard Drive Capacity	1 TB	2 TB	2 TB (8 TB Optional)	4 TB (12 TB Optional)	6 TB (24 TB Optional)
RAID Storage Management	No	No	No (Yes with Optional Drives 0, 1, 10)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 6, 10, 50, 60)
Redundant Hot Swap Power Supplies	No	No	No	Yes	Yes
System Performance					
Standalone Mode Performance (Logs / Sec)	Up to 200	Up to 625	Up to 1,000	Up to 3,000	Up to 6,000
Data Receive Rate	800 Kbps	2.5 Mbps	4 Mbps	12 Mbps	24 Mbps
Number of Licensed Network Devices	100	200	2,000	2,000	2,000
Number of FortiClient Agents	100	2,000	No Restriction	No Restriction	No Restriction
Number of ADOMs Supported	1	10	50	100	250
FortiGate Models Supported	All Models	All Models	All Models	All Models	All Models
Dimensions					

Fuente: www.fortinet.com

Los Logs que serían enviados por el equipo FortiGate 800C serían recolectados y procesados por el equipo FortiAnalyzer 400C, el cual generaría los reportes generados por el cliente. La elección de este modelo en específico está dada a que cubre en su totalidad las necesidades del cliente. Ver Figura 4.4

4.1.3. Fortinet como solución final

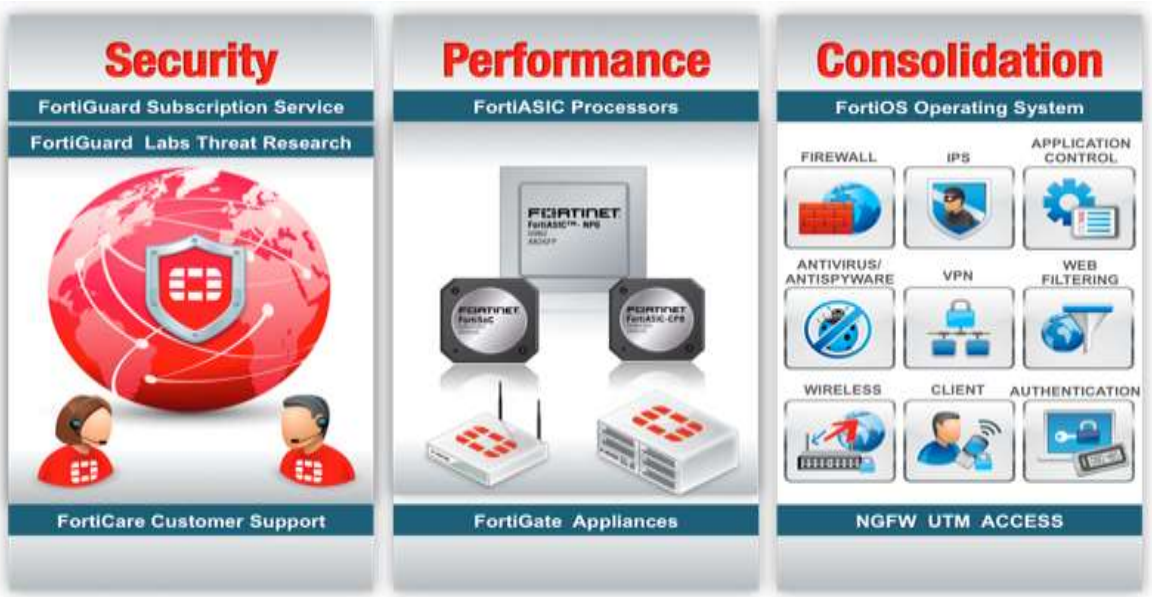
La clave del posicionamiento como líder y la fortaleza de Fortinet en el mercado UTM, radica en FortiGate que ofrece una poderosa combinación de rendimiento ASIC-acelerado lo que ofrece una respuesta multi-amenazas integrada y en constante actualización.

Los equipos de seguridad Fortinet constituyen una nueva generación de equipos de seguridad de muy alto rendimiento que garantizan la protección completa de nuestros sistemas en tiempo real. La serie FortiGate, que ofrece altísimos niveles de escalabilidad, rendimiento, seguridad y flexibilidad de despliegue, es la única plataforma de Gestión Unificada de Amenazas (UTMUnified Threat Management) que cuenta con seis certificaciones ICSA y que además cumple el estándar ATCA –Advanced Telecom Computing Architecture–, integrando una completa gama de funciones y servicios de seguridad para proteger las redes de las sofisticadas amenazas combinadas.

Entre las funcionalidades integradas de estas plataformas de Gestión Unificada de Amenzas –UTM– se incluyen cortafuegos de inspección de estado, VPN IPSec y SSL, detección y prevención de intrusiones, filtrado de contenido web, antispam, antivirus, controles de mensajería instantánea y controles P2P (peer-to-peer). Estos servicios de seguridad funcionan conjuntamente para prevenir que los ataques mixtos afecten a la red.

De tal manera da alta seguridad con una base de datos que se actualiza constantemente, un laboratorio dedicado a la búsqueda y resolución de nuevas amenazas, alto rendimiento con procesadores propietarios que brindan un mejor desempeño físico al equipo y consolidación como firewall UTM, tal como muestra en la figura 4.5.

Figura 4.5: Ventajas competitivas.



Fuente: www.ic.co.uk

A su vez vale recalcar la gran cantidad de certificados que avalan la trayectoria y brindan una marcada ventaja con los demás vendors. Tal como se muestra en la figura 4.6.

Figura 4.6: Comparativo de certificados.

Fuente: www.ic.co.uk

4.1.3.1 Servicios Fortinet

Fortinet ofrece de forma conjunta con su equipamiento servicios profesionales que garantizan el soporte, la actualización y el correcto mantenimiento de los niveles de servicio demandados. Gracias a los equipos técnicos distribuidos a lo largo de todo el mundo, Fortinet es capaz de ofrecer soporte internacional con cobertura 24x7x365, actualizando en tiempo real las bases de datos de firmas de antivirus e IDS/IPS y los motores de estas aplicaciones, así como actualizando de forma continuada las bases de datos en las que se apoyan los servicios Fortiguard Web Filtering y Fortiguard AntiSpam. El Servicio FortiProtect Distribution Network (FDN) se encarga de la distribución de estas actualizaciones a lo largo de todo el mundo, existiendo el compromiso con aquellos clientes que contratan el servicio FortiProtect Premier Services de disponer de la firma correspondiente a cualquier nuevo ataque en menos de 3 horas.

4.1.3.2 Características técnicas de los equipos

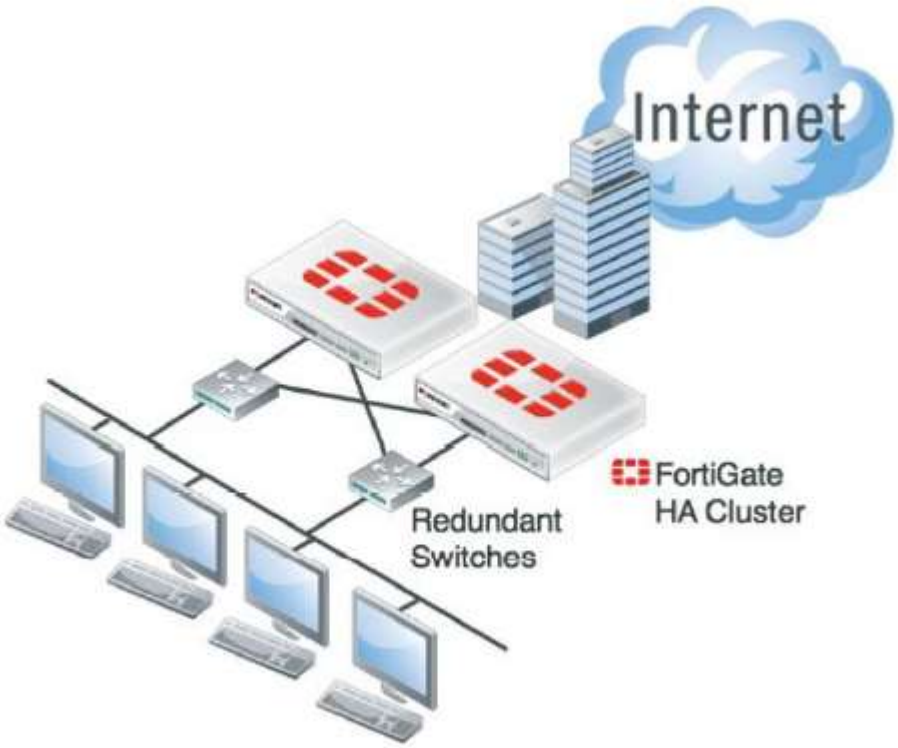
4.1.3.2.1 La Arquitectura FortiGate

La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de “Circuitos Integrados de Aplicación Específica”, conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones. La tecnología incluye el Procesador FortiASICTM y el Sistema Operativo FortiOSTM los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos.

4.1.3.2.2 Alta disponibilidad

Conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí. Activo-Activo (en modo router y transparente): La configuración de "alta disponibilidad" [16] en activo-activo es muy similar a la de activo-pasivo, aunque en este caso los dos nodos comparten los servicios de una manera activa, normalmente balanceados, consiguiendo una disponibilidad mayor ya que los servicios se entregan antes. Pasivo-Activo: Se trata de disponer de un nodo funcionando, contando con todos los servicios que componen el sistema de información al que denominaremos Activo, y el otro nodo que se denominará Pasivo en el que se encuentran duplicados todos estos servicios, pero detenidos a espera de que se produzca un fallo. Se aprecia en la figura 4.7 un arreglo redundante de firewalls Fortigate.

Figura 4.7: Modelo de redundancia



Fuente: www.docs-legacy.fortinet.com

4.1.3.2.3 Virtualización - VDOMs

Los equipos FortiGate permiten la utilización de Dominios Virtuales [16], de modo que sobre una única plataforma física podemos configurar hasta 500 Equipos virtuales, completamente independientes entre sí y con todas las funcionalidades que posee cada plataforma física. Todos los equipos FortiGate disponen en su configuración básica de la capacidad de definición de hasta 10 dominios virtuales, siendo posible ampliar el número de éstos en los equipos de gama alta (a partir de la gama FG3000), llegando hasta 500 Dominios Virtuales. Cada uno de estos dominios virtuales representan de forma lógica una máquina independiente del resto, asignándoles interfaces lógicos (VLAN's) o físicos con la posibilidad de trabajar en modo router o transparente, aplicar diferentes perfiles y políticas sobre cada máquina, etc.

4.1.3.2.4 Networking

La línea de soluciones de seguridad multiamenaza FortiGate Series ofrece a las empresas un sencillo despliegue, al permitir su instalación sin problemas en redes de última generación.

- Modos de Operación:
  - ❖ Modo NAT
  - ❖ Modo transparente: Se coloca delante del servidor existente y presenta una integración imperceptible en el entorno de red donde se ubica. Permite colocar el dispositivo en la red sin realizar ningún cambio de dirección IP. Cuando se opera en modo transparente todas las interfaces de la unidad hardware se encuentran en la misma subred IP y el dispositivo actúa como puente.
- Soporte PPPoE (Protocolo Punto a Punto sobre Ethernet)
- Soporte DDNS
- DHCP for Branch Office
- Proxy DNS
- Protocolos de Routing: Static, RIP v1 and v2, OSPF
- Soporte SNMP
- Posibilidad de personalización de los mensajes mostrados a los usuarios relativos a cada una de las funcionalidades
- ICSA Certification
- Stateful Inspection (Inspección profunda de paquetes)
- Virtual IP
- 802.1q VLAN support
- Políticas de autenticación basadas en grupos de usuarios
- Autenticación externa: Radius, LDAP
- Proceso acelerado por ASIC

4.1.3.2.5 Balanceo

Suministra una completa solución de acceso remoto que consolida la aceleración WAN, VPN y multi-homing para garantizar una conectividad rápida y fiable de las operaciones remotas y acceso global seguro a las aplicaciones distribuidas que se encuentran en el centro de datos. Soporta balanceo estático de ISPs y políticas basadas en rutas (policy routing) con la posibilidad de enrutar los paquetes por cualquier otro dato que no sea la dirección destino del paquete.

4.1.3.2.5.1 Balanceo de carga

Los dispositivos FortiGate permiten la configuración de IP's virtuales (VIP's) de manera que estas ofrecen balanceo de carga de servidores [16], teniendo la capacidad de que las peticiones realizadas a la IP virtual puedan ser atendidas por un grupo de servidores habilitados para ese efecto. La distribución del balanceo de carga puede ser configurada a nivel de puertos TCP o UDP, con la posibilidad de tener varios servicios desplegados en la misma IP y atendidos por grupos de servidores distintos. Cada uno de los servidores que componen grupo de balanceo, puede ser monitorizado a nivel ICMP, TCP o http de manera que ente el fallo de un servidor, el servicio continúa activo en el resto de equipos, dotando a la plataforma de alta disponibilidad. Se muestra en la figura 4.8 un modelo de balanceo de carga.

Figura 4.8: Balanceo de cargas

Fuente: www.docs-legacy.fortinet.com

4.1.3.2.6 Calidad de servicio (Traffic shaping)

El Traffic shaping o catalogación de tráfico controla el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento, baja latencia, y/o un ancho de banda determinado, pudiendo priorizar políticas de firewall por: ¬ Ancho de banda garantizado ¬ Ancho de banda máximo ¬ Priorización dinámica entre políticas

4.1.3.2.7 VPN

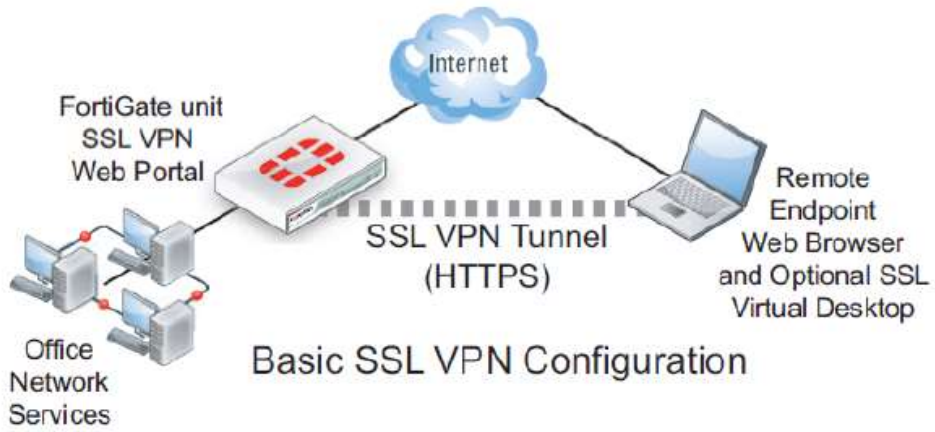
Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales[16] basadas en protocolos IPSec y SSL, además de PPTP. De esta forma, oficinas pequeñas, medias, corporaciones e ISPs pueden establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet. Al estar integrada la funcionalidad VPN en la propia plataforma FortiGate, el tráfico VPN puede ser analizado por el módulo de Firewall así como por las funcionalidades adicionales antivirus, IPS, web filtering, antispam, etc. Algunas características son:

- Soporte para VPN Site-to-Site, en modo router y transparente.
- Soporte para VPN cliente en modo router y transparente
- Soporte DDNS.
- Soporte DES, 3DES,AES256, L2TP,PPTP
- Load Sharing e clustering
- Gestión de Certificados Digitales
- Autenticación externa (Radius, LDAP)
- Nat /Pat
- Xauth sobre Radius
- Internet Key Exchange (IKE)
    - ❖ Diffie-Hellman (DH) Groups 1, 2, 5
    - ❖ RSA Certificates
- Protocolos de routing RIP, RIP2, OSPF
- IPSEc Nat transversal

- Dead peer detection
- DHCP sobre IPSec
- Soporte para VPN Hub and Spoke
- Proceso acelerado por ASIC

En la figura 4.9 se muestra una configuración básica de VPN SSL.

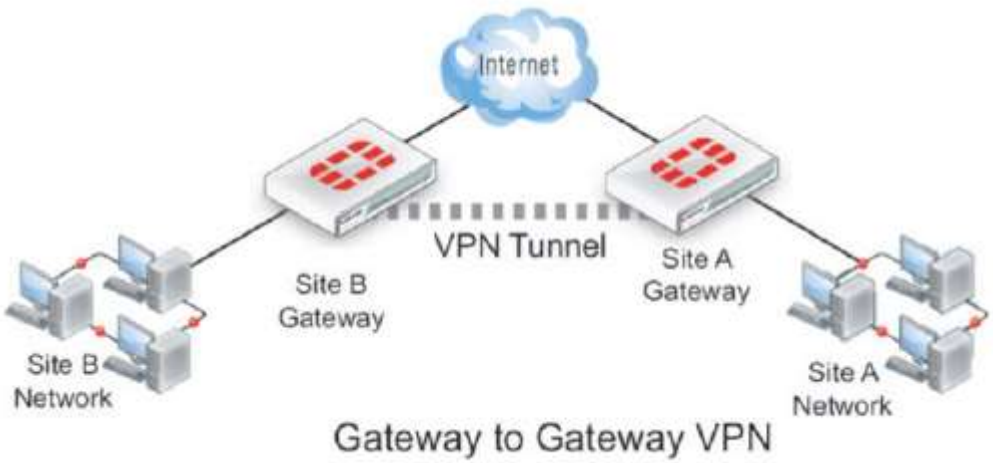
Figura 4.9: Configuración basica VPN SSL.



Fuente: www.docs-legacy.fortinet.com

En la figura 4.10 se muestra una configuración basica de VPN IPSEC.

Figura 4.10: Configuración básica VPN IPSEC



Fuente: www.docs-legacy.fortinet.com

4.1.3.2.8 Antivirus

La protección Antivirus [16] se encarga de detectar, desinfectar y/o eliminar de códigos maliciosos a la empresa, con actualizaciones en tiempo real para proteger contra nuevos ataques. Certificado por ICSA Network Antivirus es capaz de analizar los siguientes protocolos: HTTP, FTP, SMTP, POP3, IMAP y posibilidad de buscar virus en cualquier otro puerto distinto al de por defecto para estos protocolos y basada en firmas.

Características:

- Soporte de escaneo del tráfico de los túneles IPSec terminados en el dispositivo.
- Posibilidad de update de firmas en modo Push y Pull
- Heuristic detection
- Grayware detection
- Spyware detection
- Block by file size and Type
- Posibilidad de cuarentena automática
- Posibilidad de redirección de los ficheros infectados para análisis
- Soporte de ficheros comprimidos ZIP, LHA, LZH , ARJ, CAB, TAR, GZ, RAR, incluso anidados
- Proceso acelerado por ASIC
- Funcionalidad proporcionada por el mismo fabricante del equipo CPE

4.1.3.2.9 IDS/IPS

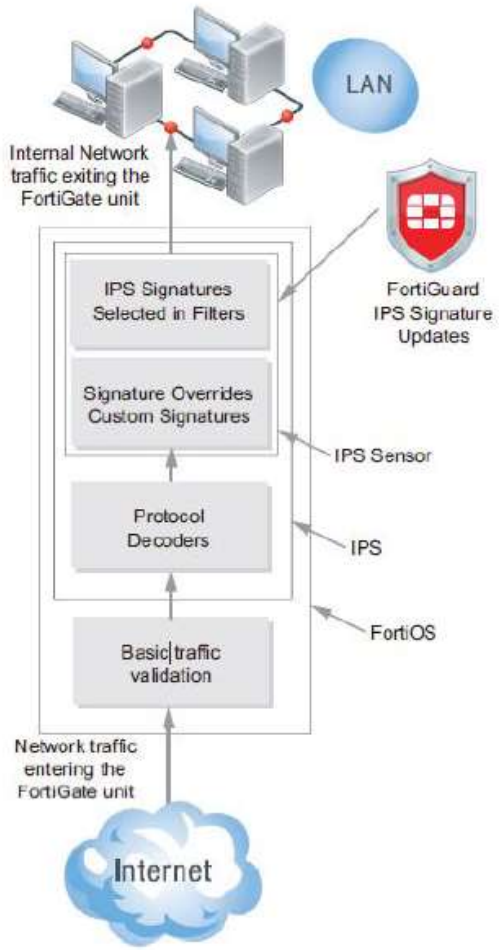
Detección y Prevención de Intrusión [16] es un sistema que se encarga de la detección y prevención automática, y en tiempo real, de más de 4.000 tipos de ataques. Esto permite a la Seguridad FortiGate parar los ataques que evaden los sistemas de antivirus convencionales a base de anfitrión, y proporciona la respuesta inmediata a amenazas de extensión rápidas. Usando la Red de Distribución global FortiGuard, FortiGate para los ataques más perjudiciales en el perímetro de red independientemente de si la red es cableada, inalámbrica, etc. Además la tecnología única de Fortinet también apoya la heurística a base

de comportamiento que añade capacidades de reconocimiento valuosas más allá simplemente de la correspondencia del contenido contra firmas conocidas Fortinet 7 Proceso acelerado por ASIC y certificado por ICSA cumple las siguientes características:

- Soporte de escaneo del tráfico de los túneles IPSec terminados en el dispositivo.
- Posibilidad de update de firmas en modo Push y Pull
- Posibilidad de creación de firmas
- Detección de anomalías de protocolo
- Basado en estadísticas
    - ❖ Flooding – Si el número de secciones están atacando un único destino y supera el umbral, el destino está experimentando flooding.
    - ❖ Scan – Si el número de sesiones de un único origen en un segundo sobrepasa el umbral, el origen está siendo escaneado.
    - ❖ Source – Si el número de sesiones concurrentes son de un mismo origen y supera el umbral, se alcanza el máximo de sesiones de origen.
    - ❖ Destination session limit - Si el número de sesiones concurrentes son de un mismo destino y supera el umbral, se alcanza el máximo de sesiones de destino.
- Anomalías de protocolos: Revisión de paquetes y sesiones para la conformidad de los estándares de internet.

En la figura 4.11 se muestra como los motores IPS se integran al servicio Fortiguard.

Figura 4.11: Integración motores IPS con base de datos Fortiguard.



Fuente: www.docs-legacy.fortinet.com

4.1.3.2.10 AntiSpam

La funcionalidad AntiSpam ofrecida por los equipos FortiGate [16] consiste en la aplicación de diferentes filtros sobre el tráfico de intercambio de correo electrónico (protocolos SMTP, POP3 e IMAP). Aquellos filtros que requieren la conexión con servidores externos (FortiGuard Antispam o los servicios de Listas Negras en tiempo real) se ejecutan de forma simultánea con los otros filtros, optimizando el tiempo de respuesta del análisis de los mensajes. Tan pronto como alguno de los filtros aplicados identifica el mensaje como spam se procede a realizar la acción definida para cada filtro que podrá ser:

- Marcar el mensaje como Spam (Tagged): El mensaje quedará identificado como Spam, y en el perfil de protección podremos decidir si se deja pasar, identificándolo como Spam y pudiendo incluir en la cabecera del mismo o en el encabezamiento MIME un mensaje identificativo, o bien si preferimos descartar el mensaje (solo sobre SMTP).
- Descartar (Discard): En este caso el mensaje es desechado, en el caso de SMTP es posible sustituirlo con un mensaje predefinido que advierta al usuario del envío de Spam.

Los filtros antispam aplicados por la plataforma FortiGate a los mensajes de correo se basan en el control por origen del mensaje y el control por el contenido del mismo.

- Control de origen
  - ❖ Dirección E-mail
  - ❖ Por dirección IP de servidor de correo
  - ❖ Listas estáticas (mantenida localmente el Fortigate)
  - ❖ Listas dinámicas (listas negras por DNS en tiempo real disponibles en internet)
  - ❖ HELO DNS lookup (SMTP)
- Control de contenido
  - ❖ Cabeceras MIME
  - ❖ Lista de palabras prohibidas
- Servicio administrado antispam (FortiGuard AntiSpam)
  - ❖ Base de datos Open Relay
  - ❖ Base de datos URI

4.1.3.2.11 URL Filtering

El Servicio de Filtrado Web de Fortinet [16] entrega actualizaciones para regular actividades web. Con 75 categorías de contenidos web, más de 30 millones de sitios web nominales y más de dos mil millones de páginas web, el Servicio de Filtración de FortiGuard [18] es uno de los servicios integrados más

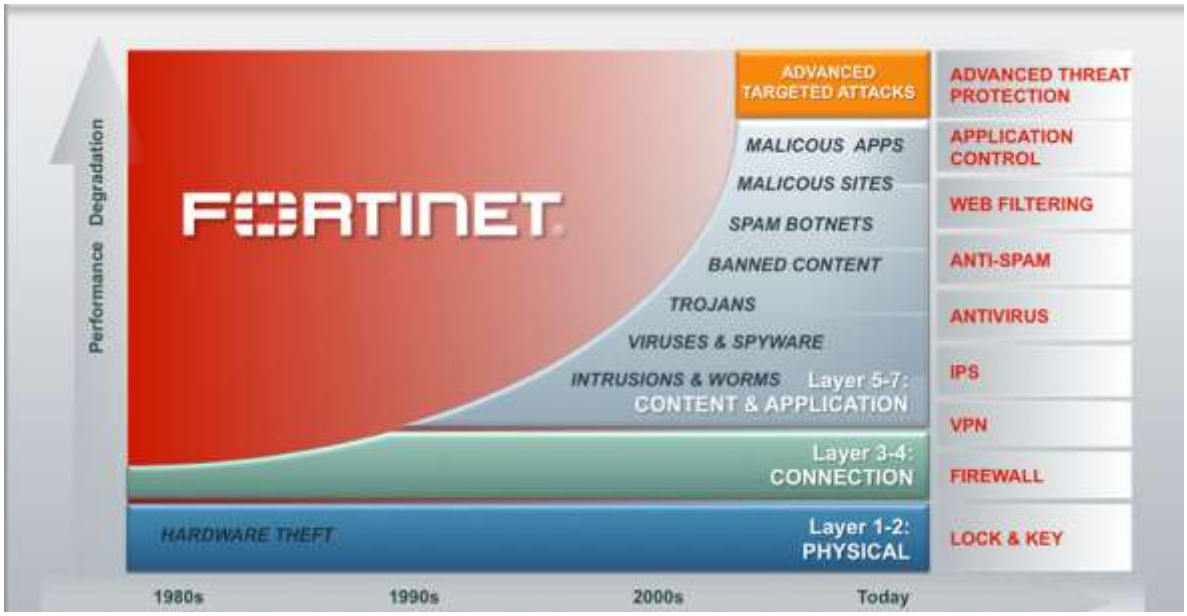
exacto de la industria. La solución Fortiguard Web Filter consiste en dos partes, los Servidores Fortiguard y el sistema de seguridad multiamenaza FortiGate. Los servidores FortiGuard contienen una base de datos de posiciones que consiste en unos mil millones de direcciones de páginas web. El servicio de Filtración FortiGuard [17] puede ser activado sobre todos los sistemas de seguridad FortiGate para regular y bloquear el acceso a los sitios web dañinos, inadecuados y peligrosos que pueden contener ataques de Phishing y/o malware como spyware. Las posibilidades de filtrado son múltiples:

- Filtrado de URL
    - ❖ Por direcciones IP
    - ❖ URLs completas
    - ❖ URLs definidas usando wildcards o regular expressions.
    - ❖ Posibilidad de importar listas de terceros

- URL Exempt list
- Filtrado de contenido - Listas negras/blancas locales
- Filtrado de Scripts Java applets, cookies, y activeX
- Servicio administrado de filtro URL (FortiGuard)
    - ❖ Más de 25 millones de dominios categorizados
    - ❖ 56 categorías

En la siguiente figura 4.12 se muestra de manera gráfica atreves del tiempo la evolución de firewall Fortigate.

Figura 4.12: Desempeño de Fortinet desde 1980 a la actualidad.



Fuente: www.fortinet.com

4.1.3.3 Sistema de Gestión

Una vez instalada la unidad hardware se puede configurar y gestionar. Además se posibilita la administración basada en roles para múltiples administradores con funciones dedicadas. Las formas de gestión son:

- Gestor basado en Web

  Es posible configurar, gestionar y monitorizar el estado de la unidad hardware utilizando http, https (mejor opción) a través de un computador que opere en red. Los cambios de configuración son efectivos de forma inmediata.

- Interfaz de línea de comandos ó CLI

  Se puede conectar al puerto serie de un pc de gestión al conector DB9 de consola serie. Se puede utilizar una conexión Telnet o mejor SSH para conectarse al CLI desde cualquier red a la que esté conectado el equipo, incluido internet. La CLI soporta la misma configuración y funcionalidades de monitorización que el gestor basado en web, además

se puede utilizar la CLI para opciones de configuración avanzadas que no son disponibles desde el gestor basado en web.

- Actualizaciones automáticas

  Servicios de Suscripción de Seguridad FortiGuard, permite la protección de red Fortinet 9 actualizada 24x7 frente a todo tipo de amenaza. Actualmente, más de 135.000 sistemas UTM FortiGate cubren en tiempo real en todo el mundo las amenazas de seguridad basadas en contenido de las actuales redes corporativas que han rebasado las capacidades de las tradicionales defensas basadas en cortafuegos.

4.1.3.4 Sistema de logging y reporting

- Funcionalidades de gestión de logs y generación de informes. Proporciona un registro de eventos del funcionamiento antivirus, antispam, etc., así mismo posibilita la generación de informes a medida en diversas modalidades, como la personalizada y la planificada.
- Centralización de logs: Posibilidad de almacenar eventos en memoria, discos duros ó envío de información a un sistema de Syslog externo o Fortianalyzer.
- El archivado de contenidos permite guardar información relevante: SMTP, POP3, FTP, HTTP, IM
- Espacio reservado para cuarentena de antivirus.
- Alertas por email para eventos críticos.

4.1.3.5 Nuevas funciones FortiOs (Sistema Operativo)

4.1.3.5.1 Fortinet wan acceleration

La opción de WAN Acceleration está pensada para mejorar e incrementar rendimiento y seguridad en comunicaciones a través de redes de área extensa, como puede ser el caso de Internet o MacroLans.

4.1.3.5.2 Web caching

Básicamente se aceleran transacciones con aplicaciones WEB reduciendo la carga de dichos servidores web y el ancho de banda utilizado, así como la percepción de latencia por el usuario final.

4.1.3.5.3 Aceleración SSL

Gracias a los circuitos ASIC CP6 de última generación se acelera el cifrado y descifrado de trafico SSL.

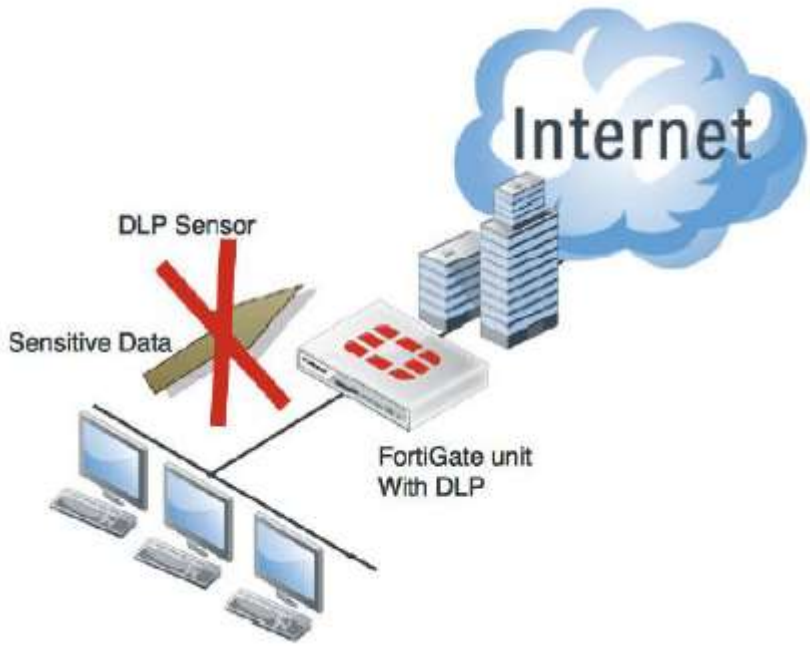
4.1.3.5.4 Inspección de contenido y análisis en comunicaciones ssl

Básicamente se lleva a cabo una arquitectura del tipo ‘man-in-the-middle’ y de esta forma se permite inspeccionar contenidos (por ejemplo detectar un virus) en comunicaciones tunelizadas sobre SSL como HTTPS, SMTPS, POP3S o IMAPS.

4.1.3.5.5 Data leak protection

Protección de fuga de datos en diferentes protocolos de transferencia de datos utilizados usualmente (smtp,ftp,http, etc) con reglas o grupos de reglas predefinidas (por ejemplo una de ellas inspecciona en busca de números de tarjetas de crédito) o totalmente personalizables. Se muestra de manera gráfica en la figura 4.13.

Figura 4.13: Operatividad del DLP

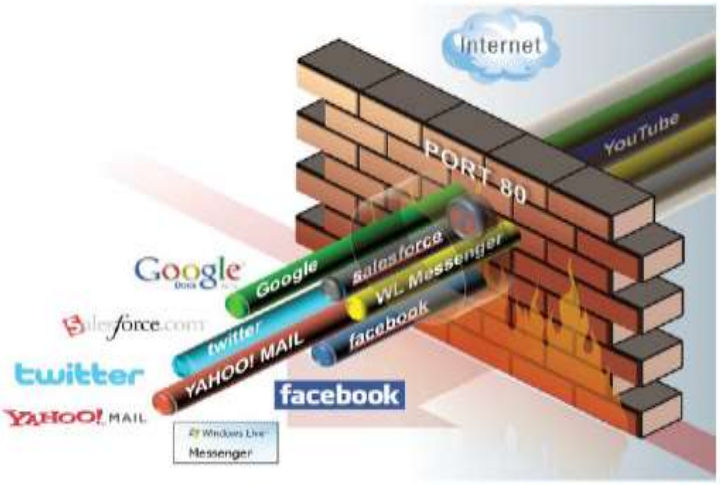


Fuente: www.docs-legacy.fortinet.com

4.1.3.5.6 Control de aplicaciones

Control de tráfico basándose en las aplicaciones que lo generan y con independencia del puerto utilizado. Antes ya se contaba con controles para algunos protocolos (sobre todo P2P e IM) ahora se han incluido controles para más protocolos/aplicaciones con independencia del puerto por lo que se ha realizado un apartado especial para este control de aplicaciones. Se demuestra de manera gráfica en la figura 4.14 como se da el bloqueo de aplicaciones.

Figura 4.14: Funcionamiento de bloqueo de aplicaciones.



Fuente: www.redeszone.net

4.1.3.5.7 End point compliance

Integración de la capa firewall perimetral con el puesto de trabajo. Mediante Forticlient es posible asegurar los puestos de trabajo (AV,IPS,AP,WF) dentro y fuera del entorno laboral. En el entorno laboral se pueden aplicar las políticas de seguridad de Firewall perimetral basándose en el grado de seguridad que el puesto de trabajo concreto necesita gracias a Forticlient. Se pueden aplicar unas u otras políticas de seguridad y dar al Firewall información del puesto de trabajo tal como Hostname, IP, volumen de tráfico generado en KB, versión del SSOO, Dominio, tipo de CPU, memoria etc.

4.1.4 Evaluación técnica

Luego de haber presentado un primer criterio de selección del fabricante para la solución perimetral, se procede a mostrar las características técnicas para el firewall Fortigate, el Antispam FortiMail y el equipo de monitoreo, repositorio de logs y reportes FortiAnalyzer cumpliendo con los requisitos técnicos presentados en el punto 3.2.2.

- Especificación técnica del firewall FortiGate.

Se presenta las especificaciones técnicas del firewall FortiGate 800C cumpliendo con el requerimiento dado inicialmente por LOS PORTALES. Como se valida en figura 4.15. (Ver anexo 01)

Figura 4.15: Especificaciones técnicas FortiGate.

	FORTIGATE 800C
Hardware Specifications	
Accelerated 10 GE SFP+ Interfaces	2
Accelerated 10/100/1000 Interfaces (RJ-45)	12
Accelerated GE SFP or 10/100/1000 Shared Interfaces	8
Accelerated 10/100/1000 Bypass Interfaces	2 pairs
10/100/1000 Management Interface	2
Maximum Network Interfaces	26
Internal Storage	60 GB
Included Transceivers	2x SFP (SX 1GE)
USB Ports (Client/Server)	1 / 1
System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 20 Gbps
Firewall Latency (64 byte UDP packets)	6 µs
Firewall Throughput (Packets Per Second)	30 Mpps
Concurrent Sessions (TCP)	7 Million
New Sessions/Second (TCP)	190,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte packets)	8 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	1.3 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	10,000
IPS Throughput	6 Gbps
Antivirus Throughput	1.7 Gbps
CAPWAP Clear-text Throughput (HTTP)	4.80 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiAPs (Total / Tunnel Mode)	1,024 / 512
Maximum Number of FortiTokens	1,000
Maximum Number of Registered FortiClients	2,000
High Availability Configurations	Active/Active, Active/Passive, Clustering
Unlimited User Licenses	Yes

	FORTIGATE 800C
Dimensions	
Height x Width x Length (inches)	1.75 x 17 x 16.42
Height x Width x Length (mm)	44 x 432 x 417
Weight	19.4 lbs (0.0 kg)
Form Factor	Rack mount (attachable ears)
Environment	
Power Required	100–240V AC, 60–50 Hz
DC Power (FG-800C-DC Required)	-48V VDC (Normal)
Redundant Power Supply (Hot-swappable)	Optional
Power Consumption (Average / Maximum)	158 W / 189 W
Heat Dissipation	645 BTU/h
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	
Safety	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Compliance	
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN

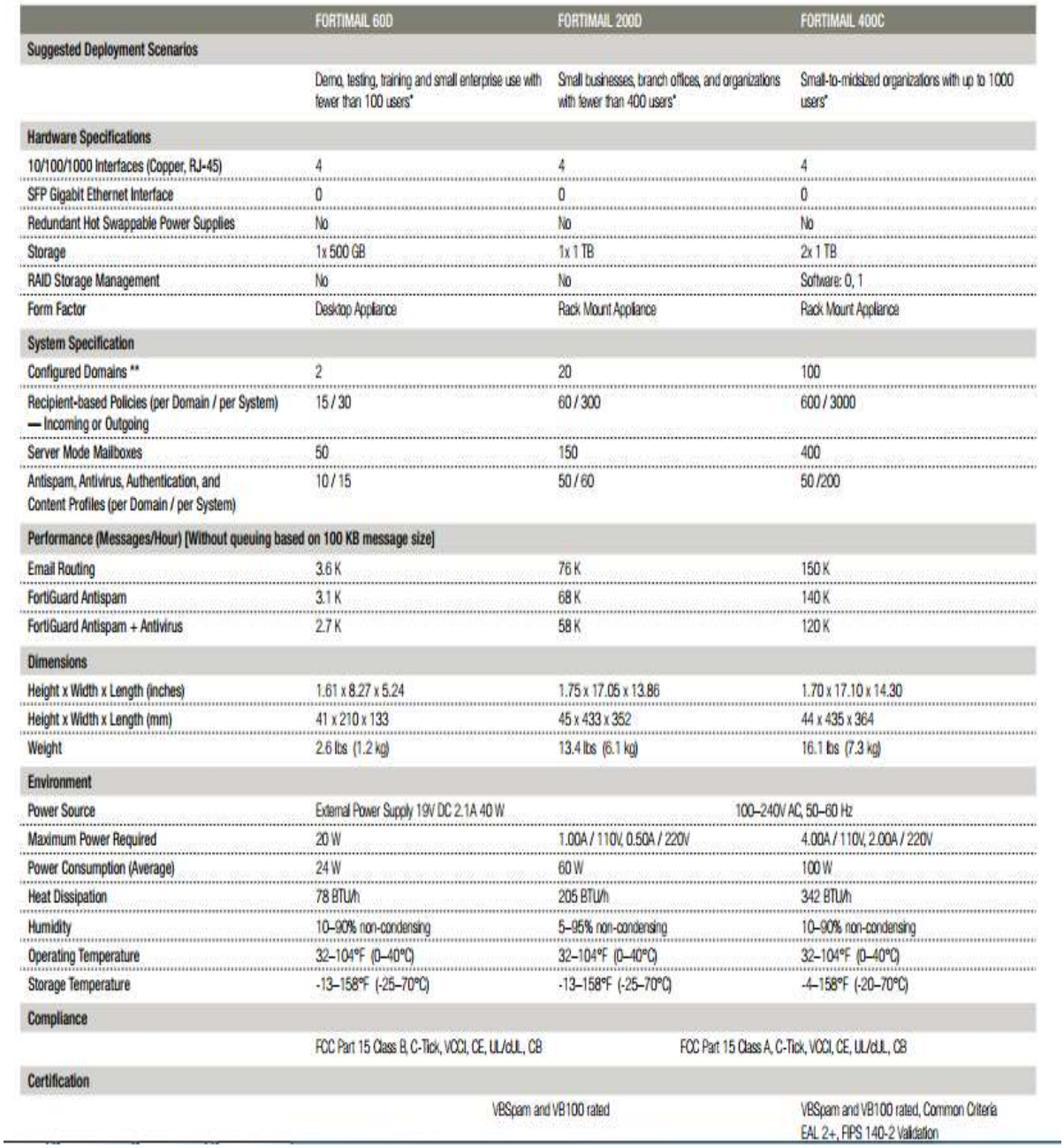
All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. Antivirus Throughput is measured in proxy mode.

Fuente: www.fortinet.com

- Especificación técnica del Antispam FortiMail

Se presenta las especificaciones técnicas del equipo Antispam FortiMail 400C cumpliendo con el requerimiento dado inicialmente por Los Portales. Como se valida en figura 4.16. (Ver anexo 02)

Figura 4.16: Especificaciones técnicas FortiMail.



	FORTIMAIL 60D	FORTIMAIL 200D	FORTIMAIL 400C
Suggested Deployment Scenarios			
	Demo, testing, training and small enterprise use with fewer than 100 users*	Small businesses, branch offices, and organizations with fewer than 400 users*	Small-to-midsized organizations with up to 1000 users*
Hardware Specifications			
10/100/1000 Interfaces (Copper, RJ-45)	4	4	4
SFP Gigabit Ethernet Interface	0	0	0
Redundant Hot Swappable Power Supplies	No	No	No
Storage	1x 500 GB	1x 1 TB	2x 1 TB
RAID Storage Management	No	No	Software: 0, 1
Form Factor	Desktop Appliance	Rack Mount Appliance	Rack Mount Appliance
System Specification			
Configured Domains **	2	20	100
Recipient-based Policies (per Domain / per System) — Incoming or Outgoing	15 / 30	60 / 300	600 / 3000
Server Mode Mailboxes	50	150	400
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	10 / 15	50 / 60	50 /200
Performance (Messages/Hour) [Without queuing based on 100 KB message size]			
Email Routing	3.6 K	76 K	150 K
FortiGuard Antispam	3.1 K	68 K	140 K
FortiGuard Antispam + Antivirus	2.7 K	58 K	120 K
Dimensions			
Height x Width x Length (inches)	1.61 x 8.27 x 5.24	1.75 x 17.05 x 13.86	1.70 x 17.10 x 14.30
Height x Width x Length (mm)	41 x 210 x 133	45 x 433 x 352	44 x 435 x 364
Weight	2.6 lbs (1.2 kg)	13.4 lbs (6.1 kg)	16.1 lbs (7.3 kg)
Environment			
Power Source	External Power Supply 19V DC 2.1A 40 W		100–240V AC, 50–60 Hz
Maximum Power Required	20 W	1.00A / 110V, 0.50A / 220V	4.00A / 110V, 2.00A / 220V
Power Consumption (Average)	24 W	60 W	100 W
Heat Dissipation	78 BTU/h	205 BTU/h	342 BTU/h
Humidity	10–90% non-condensing	5–95% non-condensing	10–90% non-condensing
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-4–158°F (-20–70°C)
Compliance			
	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB		FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certification			
		VBSpam and VB100 rated	VBSpam and VB100 rated, Common Criteria EAL 2+, FIPS 140-2 Validation

Fuente: www.fortinet-fortimail.com

- Especificación técnica del equipo de monitoreo FortiAnalyzer

  Se presenta las especificaciones técnicas del equipo FortiAnalyzer 400C cumpliendo con el requerimiento dado inicialmente por Los Portales. Como se valida en figura 4.17. (Ver anexo 03).

Figura 4.17: Especificaciones técnicas FortiAnalyzer.

FortiAnalyzer	200D	400C	1000C	2000B	4000B
Capacity and Performance					
GB/Day of Logs	5	15	25	75	150
Sessions/Day	18 M	55 M	85 M	260 M	520 M
Maximum Log Rate (Standalone Mode)	350	625	1,000	3,000	6,000
Average Retention at 5 GB Logs/Day	3 months	6 months	2 years	3 years	6 years
Devices/ADOMs/VDOMs Supported (Max)	150	200	2,000	2,000	2,000
Hardware Specification					
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes
Total Interfaces	4x GbE	4x GbE	4x GbE	6x GbE	2x GbE, 2x GbE SFP
Number of Hard Drives	1	1	1 (4 Drives Max)	2 (6 Drives Max)	6 (24 Drives Max)
Removable Hard Drives	No	No	Yes	Yes	Yes
Storage Capacity	1x 1 TB	1x 2 TB	1x 2 TB (8 TB Max)	2x 2 TB (12 TB Max)	6x 1 TB (24 TB Max)
RAID Storage Management	No	No	No (Yes with Optional Drives 0, 1, 10)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 6, 10, 50, 60)
Redundant Hot Swap Power Supplies	No	No	No	Yes	Yes
Dimensions					
Height x Width x Length	1.8 x 17.1 x 13.9 in (45 x 433 x 352 mm)	1.7 x 17.1 x 14.7 in (44 x 435 x 364 mm)	1.7 x 17.1 x 24.7 in (43 x 434 x 627 mm)	3.4 x 17.4 x 26.8 in (86 x 443 x 681 mm)	6.9 x 19.1 x 27.2 in (175 x 485 x 690 mm)
Weight	13.4 lbs (6.1 kg)	14.7 lbs (6.7 kg)	35.0 lbs (15.9 kg)	63 lbs (28.6 kg)	94.5 lbs (43 kg)
Form Factor	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 2 RU	Rack mount, 3 RU
Environment					
AC Power Supply	100 – 240 VAC, 50 – 60 Hz, 6 Amp Max	100 – 240 VAC, 50 – 60 Hz, 4 Amp Max	100 – 240 VAC, 50 – 60 Hz, 7.5 Amp Max	100 – 240 VAC, 50 – 60 Hz, 9 Amp Max	100 – 240 VAC, 50 – 60 Hz, 11.5 Amps Max
Power Consumption (AVG)	60W	100W	189W	200W	420W for 6 HDD
Heat Dissipation	205 BTU/h	411 BTU/h	643.6 BTU/h	519 BTU/h	1433.7 BTU/h (6 drives) 2034.6 BTU/h (12 drives)
Operating Temperature	32–104 °F (0–40 °C)	50–90 °F (10–35 °C)	32–95 °F (0–35 °C)	50–95 °F (10–35 °C)	32–104 °F (0–40 °C)
Storage Temperature	-13–158 °F (-25–70 °C)		-40–149 °F (-40–65 °C)		-13–158 °F (-25–70 °C)
Humidity	5 to 95% non-condensing	10 to 90% non-condensing	5 to 95% non-condensing		
Compliance					
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, UL/cUL, CB, NOM, GOST	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, UL/cUL, CB

Fuente: www.fortinet.com

4.2 Evaluación económica

4.2.1 Inversión de Capital (CAPEX)

Se refiere al gasto de capital que se requiere hacer para la ejecución del proyecto. Los CAPEX son utilizados por una compañía para adquirir o mejorar los activos fijos. En resumen, la inversión en la construcción de todo el sistema de seguridad perimetral para que esté listo para su funcionamiento.

Se incluye la compra de los bienes tales como los dos firewalls, el antispam, el reporteado de logs, a su vez se incluye la licencia y los servicios de garantía (RMA).

La solución de la instalación de seguridad perimetral interna incluye dos dispositivos de Seguridad Perimetral Fortinet modelo FortiGate-800C con los Servicios Firewall, Antivirus Perimetral, Antispam Perimetral, IDS-IPS, Filtro Web, Control de Aplicaciones, Inspección de Tráfico SSL, Data Leak Prevention, Politicas basadas en Identidad más un equipo FortiMail-400C dedicado para Antivirus, Antispam y Antimalware de correo electrónico más un equipo de Gestión de LOGs y Reportería FortiAnalyzer-400C.

Se presenta el detalle de sus costos tabla 4.6.

Tabla 4.6 : Capex

Concepto	Cantidad	Costo Unitario ($)	Costo Unitario (S/.)	Costo Total (S/.)
Equipos				
Firewall Fortigate 800C	2	10000	33300	66600
Fortimail 400C	1	6995	23293.35	23293.35
Fortianalyzer 300D	1	8995	29953.35	29953.35
Licencias				
Licenciamiento de los servicios firewall Fortigate antivirus, filtro web, IDS/IPS, VPN IPSEC/SSL, control de aplicaciones, data leak prevation, traffic Shaping por 36 meses (Forticare and FortiGuard UTM Bundle)	1	17059	56806.47	56806.47
Licenciamiento premium Fortimail bundle forticare por 36 meses (24x7 FortiCare plus FortiGuard Bundle Contract)	1	8353	27815.49	27815.49
Licenciamiento premium Fortianalyzer bundle forticare por 36 meses(24x7 FortiCare Contract)	1	5903	19656.99	19656.99
Instalación				
Servicio de instalacion incluye la configuración y puesta en marcha de dos equipos Fortigate 800C, un Fortimail 400C, un Fortianalyzer 400C	1	2680	8924.4	8924.4
TOTAL				233050.05

Fuente: Elaboración propia

4.2.2 Inversión en Operación y Mantenimiento (OPEX)

Son definidos como los gastos de operación y mantenimiento de la red, que se tendrán que realizar para tener el sistema en buen estado. Se plantea que para el proyecto el cliente contrate un servicio de soporte primer nivel que brinde apoyo en configuraciones y mantenimientos preventivos y correctivos, una vez concluido el periodo de licenciamiento (36 meses), el cliente deberá renovar licencias para todos sus equipos.

Se presenta el detalle de sus costos tabla 4.7

Tabla 4.7 : Opex

	Costo (S/.)			
Concepto	**Año 1**	**Año 2**	**Año 3**	
Soporte				
Soporte Fortigate primer nivel 7x24x365, soporte correctivo y preventivo.	5.4612	5.4612	5.4612	
Soporte Fortimail primer nivel 7x24x365, soporte correctivo y preventivo.	**2264.4**	**2264.4**	**2264.4**	
Soporte Fortianalyzer primer nivel 7x24x365, soporte correctivo y preventivo.	1198.8	1198.8	1198.8	
Licencias				
Licenciamiento de los servicios firewall Fortigate antivirus, filtro web, IDS/IPS, VPN IPSEC/SSL, control de aplicaciones, data leak prevation, traffic Shaping por 36 meses (Forticare and FortiGuard UTM Bundle)	18935.49	18935.49	18935.49	
Licenciamiento premium Fortimail bundle forticare por 36 meses (24x7 FortiCare plus FortiGuard Bundle Contract)	9271.83	9271.83	9271.83	
Licenciamiento premium Fortianalyzer bundle forticare por 36 meses(24x7 FortiCare Contract)	652.33	652.33	652.33	
TOTAL	32328.3112	32328.3112	32328.3112	96984.9336

Fuente: Elaboración propia

4.2.3 Costo Total de la Propiedad (TCO)

Es una herramienta destinada a analizar y hacer más eficiente la adquisición de tecnología. El principio básico del TCO es que los costos de propiedad de cualquier bien tienen componentes más allá de los estipulados en el precio de compra del mismo y costos en los cuales se debe incurrir para garantizar el funcionamiento correcto del bien durante la vida útil del mismo.

Para nuestro proyecto se estipula un tiempo de vida útil de tres años, por ende especificamos el siguiente cuadro (tabla xxxx) referente al TCO donde consideramos la compra de los activos, la puesta en producción, las licencias a nivel de UTM, servicios de fábrica y soporte de mantenimiento preventivo y correctivo.

Tabla 4.8: TCO

	Costo (S/.)			
Concepto	**Año 1**	**Año 2**	**Año 3**	
Equipos				
Firewall Fortigate 800C	66600			
Fortimail 400C	23293.35			
Fortianalyzer 300D	29953.35			
Instalación				
Servicio de instalación incluye la configuración y puesta en marcha de dos equipos Fortigate 800C, un Fortimail 400C, un Fortianalyzer 400C	8924.4			
Soporte				
Soporte Fortigate primer nivel 7x24x365, soporte correctivo y preventivo.	5.4612	5.4612	5.4612	
Soporte Fortimail primer nivel 7x24x365, soporte correctivo y preventivo.	**2264.4**	**2264.4**	**2264.4**	
Soporte Fortianalyzer primer nivel 7x24x365, soporte correctivo y preventivo.	1198.8	1198.8	1198.8	
Licencias				
Licenciamiento de los servicios firewall Fortigate antivirus, filtro web, IDS/IPS, VPN IPSEC/SSL, control de aplicaciones, data leak prevation, traffic Shaping por 36 meses (Forticare and FortiGuard UTM Bundle)	18935.49	18935.49	18935.49	
Licenciamiento premium Fortimail bundle forticare por 36 meses (24x7 FortiCare plus FortiGuard Bundle Contract)	9271.83	9271.83	9271.83	
Licenciamiento premium Fortianalyzer bundle forticare por 36 meses(24x7 FortiCare Contract)	652.33	652.33	652.33	
TOTAL	161099.41	32328.31	32328.31	225756.03

Fuente: Elaboración propia

4.3 Presentación de la solución propuesta

La elección de la solución de seguridad perimetral Fortinet se decidió basándose en:

Su posicionamiento en el mercado actual de tecnología de la información, el cual fue provisto por Gartner en el punto 4.1.2.Cuadrante mágico de Gartner.

Las características técnicas y funcionalidades, la cual fue provisto a través de los cuadros de las especificaciones técnicas contenidos en el punto 4.1.3. Evaluación técnica.

4.3.1 Propuesta técnica

La solución propuesta es la siguiente:

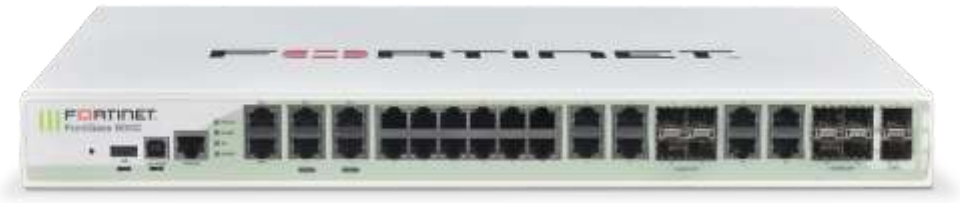
- Firewall Perimetral. Se escogió el equipo FortiGate, debido a que el equipo cuenta con una solución de firewall, adicionalmente cuenta con un concentrador VPN, equipo IPS, equipo Antivirus y equipo proxy para la navegación, todo en un solo dispositivo, además de un ahorro en dinero por que las licencias es equipo y no por número usuarios.
- Equipo Antispam. Se escogió el equipo de FortiMail, debido el equipo cuenta con una base de datos, Fortiguard, actualizada a nivel mundial y que protegerá de cualquier correo malicioso enviado hacia la red de LOS PORTALES.
- Equipo de Monitoreo. Se escogió el equipo de FortiAnalyzer, debido a la compatibilidad de recepción de Log que cuenta con el FortiGate y FortiMail por ser de la misma marca. Adicional al monitoreo en tiempo real y envío de reportes personalizados también cuenta con el módulo de escaneo de vulnerabilidades donde inspecciona los punto débiles que pueda presentar los servidores de la red.

CAPÍTULO V: IMPLEMENTACIÓN LA SOLUCIÓN DE LA SEGURIDAD PERIMETRAL

En este capítulo, se brindará a detalle la implementación mas idonea para cada uno de los equipos de seguridad, los cuales según los cuadros comparativos son ideales para la infraestructura de seguridad que el cliente Los Portales solicita.

Por ende la plataforma Fortigate es la que se acomoda de mejor manera a los requerimientos del cliente y se muestran a continuación en las figuras 5.1, 5.2 y 5.3.

Figura 5.1: FortiGate 800C (ver anexo 01)



Fuente: http://www.avfirewalls.com

Figura 5.2: FortiAnalyzer 400C (ver anexo 02)

Fuente: http://www.avfirewalls.com

Figura 5.3: FortiMail 400C (ver anexo 03)

Fuente: http://www.avfirewalls.com

5.1. Cronograma de trabajo

Para la implementación de nuestro proyecto se estipula el siguiente cronograma de trabajo (Tabla 5.1), siguiendo los hitos detallados en este capítulo.

Tabla 5.1: Cronograma de trabajo

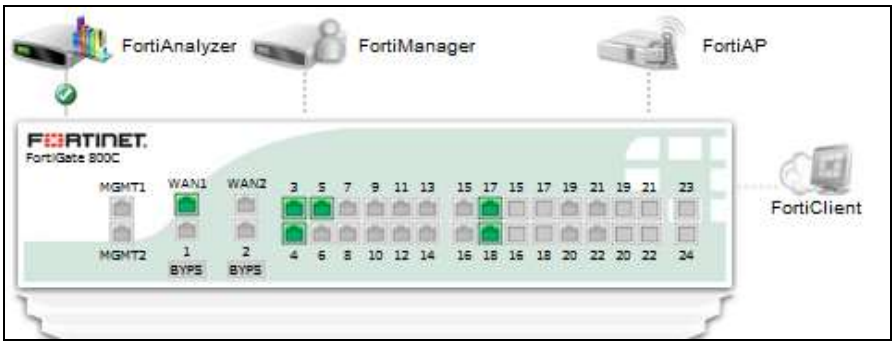
		Dia1	Dia2	Dia3	Dia4	Dia5	Dia6
1	Instalación del equipo Firewall	x	x				
2	Configuración de los servicios de seguridad en el Firewall			x			
3	Configuración del módulo de Políticas del firewall				x		
4	Instalación del FortiMail					x	
5	Configuración del FortiMail					x	
6	Pruebas de correo						x
7	Instalación del FortiAnalyzer						x

Fuente: Elaboración propia

5.2. Instalación del equipo Firewall

Este equipo se instalaría en el del Data Center de la empresa, se presentan los puertos físicos activos los cuales en la figura 5.4 se aprecian los puertos de color verde, que negociaran con los demás equipos.

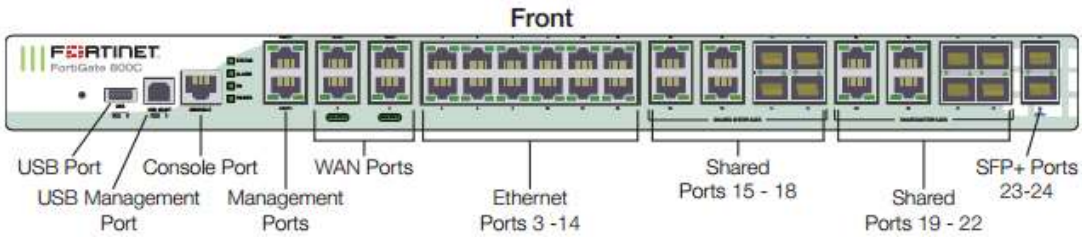
Figura 5.4: Detalle de conexiones del Firewall (ver anexo 01)



Fuente: www.fortinet.com

En la figura 5.5 se muestra la vista frontal del FortiGate 800C, las distribuciones de los puertos e interfaces.

Figura 5.5: Vista frontal Fortigate 800C (ver anexo 01)



Fuente: http://www.avfirewalls.com

5.2.1 Interfaces configuradas

Se detalla el listado de puertos en la figura 5.6 utilizados los cuales están asignado a cada interface en el equipo FortiGate:

Figura 5.6: Cuadro de interfaces

Puertos	Detalles
Port3	Interface conectado a la red LAN
Port4	Interface conectado a la DMZ
WAN1	Interface conectado al enlace
Port17	Interface conetcado para el HA entre los FortiGate
Port18	

Fuente: Eleboración propia

Estas interfaces se encuentran asociadas a distintos objetos y segmentos como se detalla en la figura 5.7.

Figura 5.7: Interfaces del FortiGate

Name	IP/Netmask	Access	Administrative Status	Link Status	Type	Ref.
mgmt1	192.168.1.99 / 255.255.255.0	PING,SSH			Physical	1
mgmt2	0.0.0.0 / 0.0.0.0				Physical	0
wan1 (INET)	200.62.224.194 / 255.255.255.224	HTTPS,PING,SSH,SNMP			Physical	100
port1	0.0.0.0 / 0.0.0.0				Physical	0
wan2	0.0.0.0 / 0.0.0.0				Physical	0
port2	0.0.0.0 / 0.0.0.0				Physical	1
port3 (LAN)	172.16.0.1 / 255.255.255.0	HTTPS,PING,SSH,SNMP			Physical	147
port4 (DMZ)	192.168.10.1 / 255.255.255.0	PING			Physical	62
port5 (VUCE-REF)	0.0.0.0 / 0.0.0.0				Physical	3
REF10	20.6.6.2 / 255.255.255.0	PING			VLAN	8
LD_VUCE	20.6.7.4 / 255.255.255.0	PING			VLAN	23
port6	0.0.0.0 / 0.0.0.0				Physical	0
port7	0.0.0.0 / 0.0.0.0				Physical	0
port8	0.0.0.0 / 0.0.0.0				Physical	0
port9	0.0.0.0 / 0.0.0.0				Physical	0
port10	0.0.0.0 / 0.0.0.0				Physical	1
port11	0.0.0.0 / 0.0.0.0				Physical	0
port12	0.0.0.0 / 0.0.0.0				Physical	0
port13	0.0.0.0 / 0.0.0.0				Physical	0
port14	0.0.0.0 / 0.0.0.0				Physical	0
port15	0.0.0.0 / 0.0.0.0				Physical	0
port16	0.0.0.0 / 0.0.0.0				Physical	0
port17 (HA1)	0.0.0.0 / 0.0.0.0				Physical	1
port18 (HA2)	0.0.0.0 / 0.0.0.0				Physical	1
port19	0.0.0.0 / 0.0.0.0				Physical	0

Fuente: Elaboración propia

5.2.2 Tabla de enrutamiento

El equipo FortiGate como todo equipo viene configurado por defecto,teniendo solo una única ruta estática la cual viene con el nombre Default Route, es por ello que se configuran diversas rutas de esta manera se obtiene una tabla de ruteo en base a las necesidades de la red de la empresa.

El FortiGate selecciona la mejor ruta según la información de la tabla de ruteo. A su vez se cuenta con una Sub-tabla que tiene por nombre “Forwarding Table”, la cual es utilizada para enviar los paquetes según dicha información. Tal como se muestra en la figura 5.8.

Figura 5.8: Interfaces del FortiGate

0.0.0.0/0.0.0.0	200.62.224.193	wan1
10.6.6.0/255.255.255.0	20.6.6.5	MEF10
10.163.63.0/255.255.255.224	20.6.7.1	LD_VUCE
20.6.8.0/255.255.255.0	20.6.7.1	LD_VUCE
20.6.9.0/255.255.255.0	20.6.7.1	LD_VUCE
20.6.10.0/255.255.255.0	20.6.7.1	LD_VUCE
172.10.11.0/255.255.255.0	20.6.7.1	LD_VUCE
172.16.60.0/255.255.255.0	172.16.0.229	port3
172.16.100.0/255.255.255.0	172.16.0.229	port3
172.16.101.0/255.255.255.0	172.16.0.229	port3
172.16.108.0/255.255.255.0	172.16.0.229	port3
172.16.109.0/255.255.255.0	172.16.0.229	port3
172.16.110.0/255.255.255.0	172.16.0.229	port3
172.16.112.0/255.255.255.0	172.16.0.229	port3
172.16.115.0/255.255.255.0	172.16.0.229	port3
172.16.116.0/255.255.255.0	172.16.0.229	port3
172.16.117.0/255.255.255.0	172.16.0.229	port3
172.16.206.0/255.255.255.0	172.16.0.229	port3
172.16.207.0/255.255.255.0	172.16.0.229	port3
192.168.2.0/255.255.255.0	172.16.0.229	port3
192.168.3.0/255.255.255.0	172.16.0.229	port3
192.168.4.0/255.255.255.0	172.16.0.229	port3
192.168.5.0/255.255.255.0	172.16.0.229	port3
192.168.6.0/255.255.255.0	172.16.0.229	port3
192.168.8.0/255.255.255.0	172.16.0.229	port3
192.168.9.0/255.255.255.0	172.16.0.229	port3
192.168.15.0/255.255.255.0	172.16.0.229	port3
192.168.16.0/255.255.255.0	172.16.0.229	port3
172.16.20.0/255.255.255.0		ssl.root

Fuente: Elaboración propia

5.2.3 Configuración SNMP

A traves del protocolo SNMP se realizará el monitoreo correspondiente al equipo FortiGate, esto ayudará a saber cual es el estado del equipo. A continuación se muestra la configuración y el nombre asociado de esta comunidad ntsecurity en la figura 5.9.

Figura 5.9: Habilitación del protocolo SNMP

Fuente: Elaboración propia

5.2.4 Configuración del High Ability (HA)

En la propuesta realizada, se detalla el uso de dos equipos configurados en High Ability es decir en alta disponibilidad.

- **Máster:** Es el equipo que está cumpliendo el rol de maestro dentro del clúster.
- **Slave:** Es el equipo que cumple la función de esclavo, es decir está en espera y entrar en acción si es que hubiera alguna eventualidad con el equipo principal.

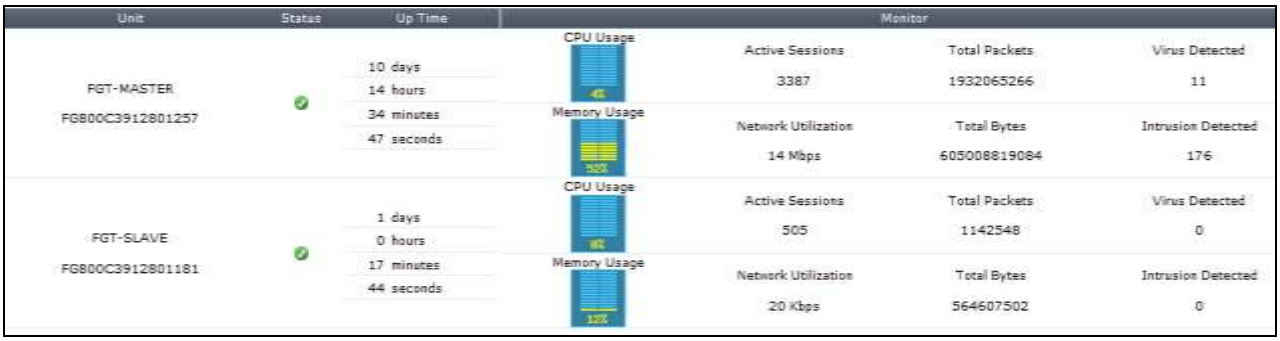
En la figura 5.10 se detalla el estado del sistema del clúster.

Figura 5.10: High Ability (HA)

Fuente: Elaboración propia

Se muestra en la figura 5.11. el estado del sistema del clúster.

Figura 5.11: Clúster habilitado

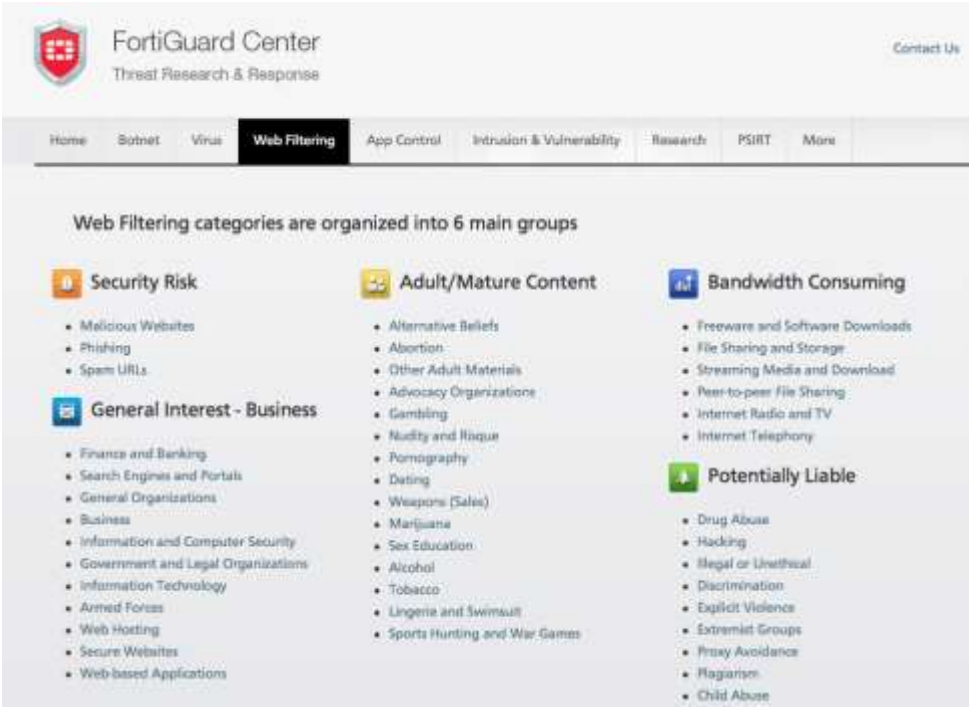


Fuente: Elaboración propia

5.2.5 Licenciamiento del Equipo

El equipo FortiGate hace consultas a la web FortiGuard [16] www.FortiGuard.com está dirección viene a ser la Base de Datos a la cual consulta el equipo para realizar los distintos filtros, accesos ó denegaciones. Es necesario que el equipo cuente con licenciamiento y los servicios del firewall activados en su totalidad. En la figura 5.12 se muestra la base de datos Fortiguard.

Figura 5.12: FortiGuard



Fuente: www.fortiguard.com

En la figura 5.13 se muestra el estado de las licencias en la consola web del equipo firewall Fortigate.

Figura 5.13: Licencia del FortiGate

Fuente: Elaboración propia

5.2.6 Información del sistema

Se muestra en la figura 5.14 la información de los equipos en la cual se describen datos importantes, los cuales se observan a continuación:

Figura 5.14: Información del sistema

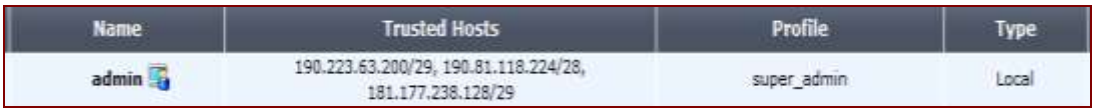
Fuente: Elaboración propia

5.2.7 Usuario administrador

El equipo FortiGate tiene distintos tipos de perfiles de usuarios con diferentes privilegios.

Para el caso de este equipo el usuario **admin** es el único que posee la administración del equipo siendo esta administrada por el proveedor de servicio de seguridad, quién cuenta con direcciones de red de confianza, las cuales son las únicas desde donde podrán acceder al equipo, como se ve en la figura 5.15.

Figura 5.15: Usuarios FortiGate



Fuente: Elaboración propia

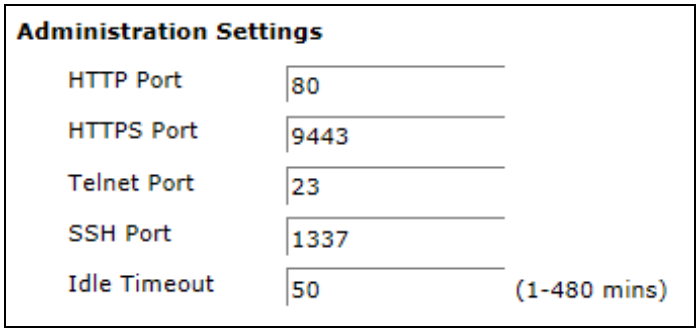
5.2.8 Puertos de acceso

Se muestran los puertos los cuales se utilizán en la conexión del equipo.Por un tema de seguridad se modificaron los siguientes puertos :

- **Acceso web vía (HTTPS)** antes puerto por default **443** ahora es el puerto **9443.**
- **Acceso vía (SSH)** antes puerto por default **22** ahora es el puerto **1337.**

En la figura 5.16 se muestra la configuración de puertos.

Figura 5.16: Puertos de administración



Fuente: Elaboración propia

5.2.9 Integración con el FortiAnalyzer

Se realizó la integración del firewall con el equipo FortiAnalyzer 400C el cual está etiquetado con el nombre “LOS_PORTALES-800C”.

La integración se realizó de forma exitosa pues se visualiza en el FortiAnalyzer el almacenamiento de todos los logs de navegación así como también los eventos que generan en el firewall.

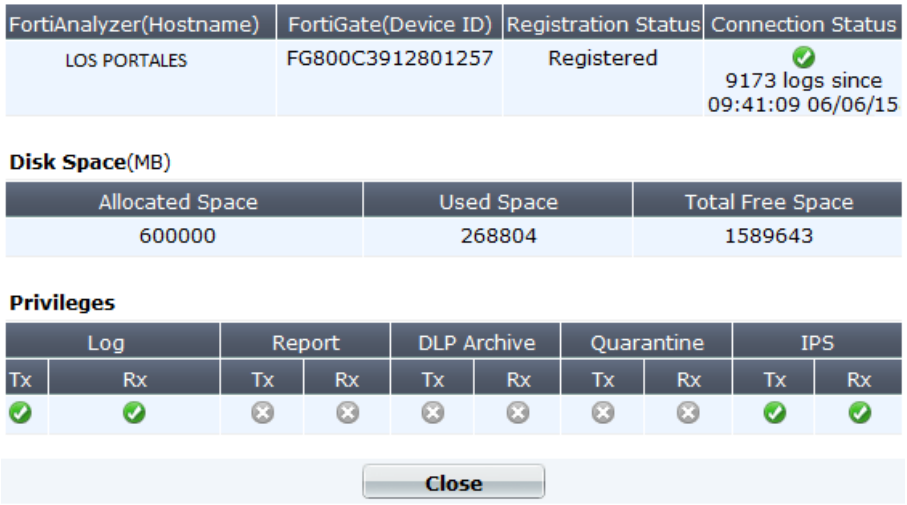
La conectividad puede validarse en el equipo, de esta forma nos aseguramos que el Firewall está enviando Logs. Se valida dicha información en la figura 5.17.

Figura 5.17: Puertos de administración

Fuente: Elaboración propia

En la figura 5.18 se valida el test de conexión entre Fortigate y FortiAnalyzer.

Figura 5.18:. Validación de envío de Log's



FortiAnalyzer(Hostname)	FortiGate(Device ID)	Registration Status	Connection Status
LOS PORTALES	FG800C3912801257	Registered	9173 logs since 09:41:09 06/06/15

Disk Space(MB)

Allocated Space	Used Space	Total Free Space
600000	268804	1589643

Privileges

Log		Report		DLP Archive		Quarantine		IPS	
Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx

Close

Fuente: Elaboración propia

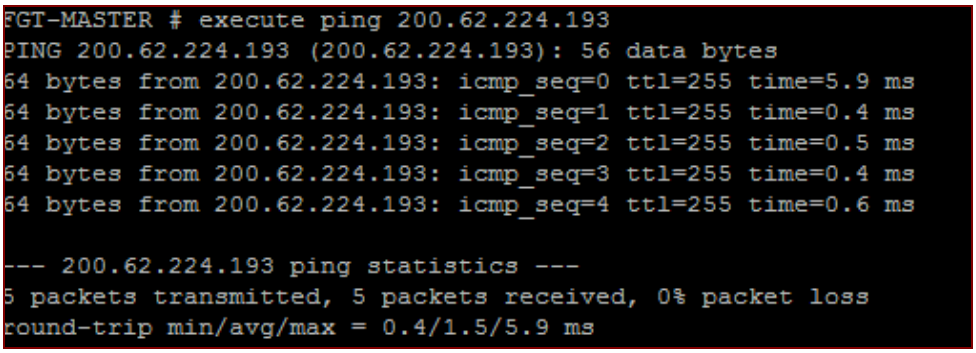
5.2.10 Pruebas de conectividad

Se realizan las pruebas de conectividad a nivel de red luego de haber instalado el equipo y haber configurado los parámetros de red en las interfaces.

Siendo el ISP Claro Perú.

- Pruebas de conectividad desde el equipo Master hacia el Router cuya dirección IP es **200.62.224.193** del enlace de Claro, como se muestra en la figura 5.19.

Figura 5.19: Test de conectividad - FGT-MASTER



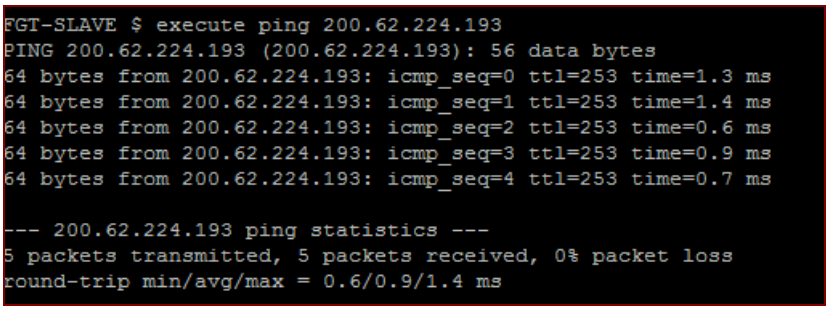
```
FGT-MASTER # execute ping 200.62.224.193
PING 200.62.224.193 (200.62.224.193): 56 data bytes
64 bytes from 200.62.224.193: icmp_seq=0 ttl=255 time=5.9 ms
64 bytes from 200.62.224.193: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 200.62.224.193: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 200.62.224.193: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 200.62.224.193: icmp_seq=4 ttl=255 time=0.6 ms

--- 200.62.224.193 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/1.5/5.9 ms
```

Fuente: Elaboración propia

- Pruebas de conectividad desde el equipo Master hacia el Router cuya dirección IP es **200.62.224.193** del enlace de Claro, como se muestra en la figura 5.20.

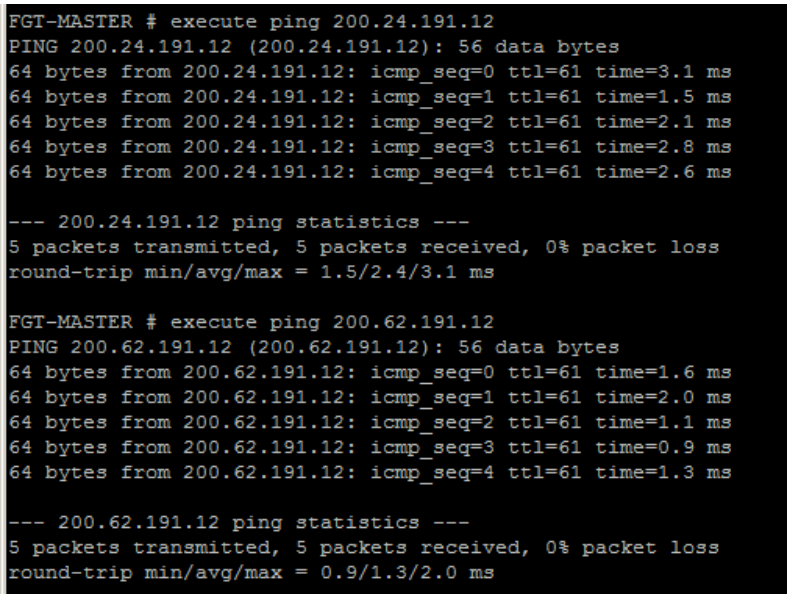
Figura 5.20: Test de conectividad - FGT-SLAVE



Fuente: Elaboración propia

- Pruebas de conectividad desde el equipo Master a servidores externos (DNS de Claro) **200.24.191.12, 200.62.191.12,** como se muestra en la figura 5.21.
-

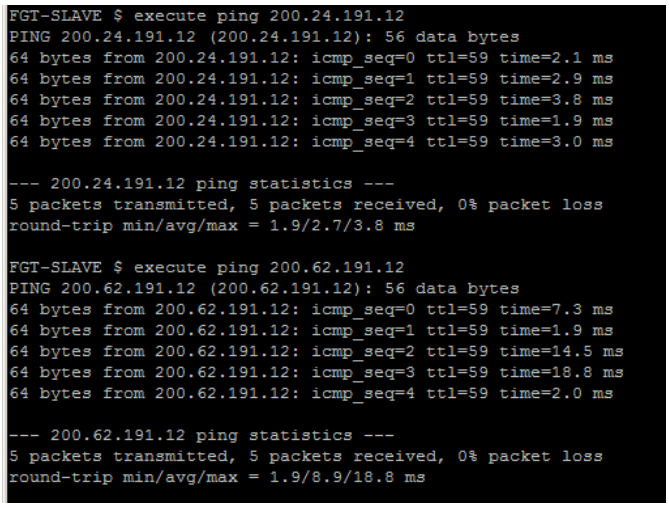
Figura 5.21: pruebas hacia los DNS - FGT- MASTER



Fuente: Elaboración propia

- Pruebas de conectividad desde el equipo Slave a servidores externos (DNS de Claro) **200.24.191.12, 200.62.191.12,** como se muestra en la figura 5.22.

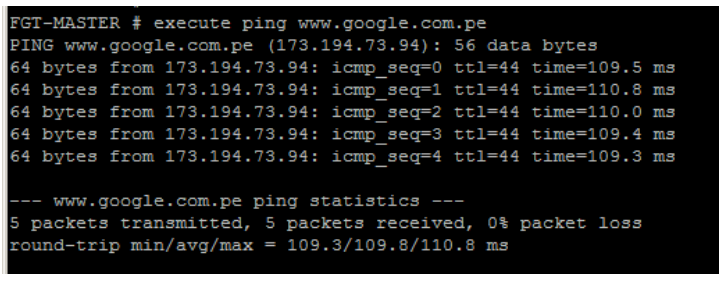
Figura 5.22: Test hacia los DNS - FGT- SLAVE



Fuente: Elaboración propia

- Pruebas de conectividad desde el equipo Master a nivel de red verificando los saltos a sitios web externos como por ejemplo http://www.google.com, como se muestra en la figura 5.23.

Figura 5.23: Test a página Web FGT-MASTER



Fuente: Elaboración propia

- Pruebas de conectividad desde el equipo Slave a nivel de red verificando los saltos a sitios web externos como por ejemplo http://www.google.com, como se muestra en la figura 5.24.

Figura 5.24: Test a página Web FGT-SLAVE

```
FGT-SLAVE $ execute ping www.google.com.pe
PING www.google.com.pe (173.194.73.94): 56 data bytes
64 bytes from 173.194.73.94: icmp_seq=0 ttl=42 time=109.3 ms
64 bytes from 173.194.73.94: icmp_seq=1 ttl=42 time=109.9 ms
64 bytes from 173.194.73.94: icmp_seq=2 ttl=42 time=110.2 ms
64 bytes from 173.194.73.94: icmp_seq=3 ttl=42 time=112.2 ms
64 bytes from 173.194.73.94: icmp_seq=4 ttl=42 time=110.8 ms

--- www.google.com.pe ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 109.3/110.4/112.2 ms
```

Fuente: Elaboración propia

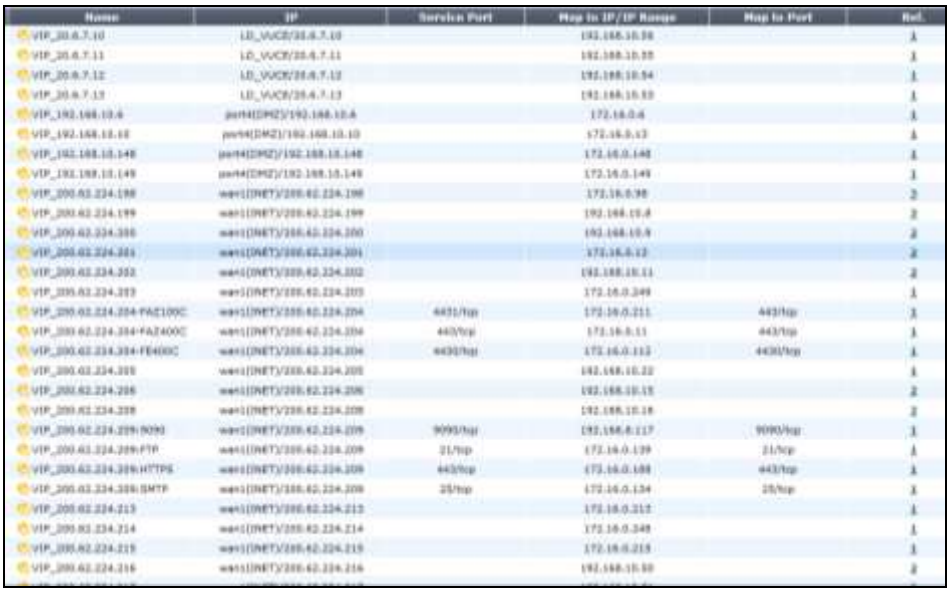
5.2.11 IP Virtual (VIP)

VIP o IP Virtual [16] nos ayudan a publicar un servicio interno hacia Internet. Para la cual se hace un NAT estático ya sea uno a uno o por servicio “Nat de ingreso”.

En el caso de Los Portales tiene NAT uno a uno así también se han definido puertos para algunos casos.

Se detalla en la figura 5.25. todas las publicaciones

Figura 5.25: Publicación de servicios



Fuente: Elaboración propia

5.3 Configuración de los servicios de seguridad en el Firewall

Se muestra la configuración en el equipo a nivel de UTM [16] especificando las características de configuración del Antivirus, Filtros Web, Control de Aplicaciones esto es según las necesidades de la infraestructura de la empresa.

5.3.1 Antivirus

En esta sección se ha creado un perfil único para todos los usuarios en la cual analizara las tramas de los protocolos **HTTP, HTTPS** y **FTP**, como se muestra en la figura 5.26.

Figura 5.26: Perfil Antivirus

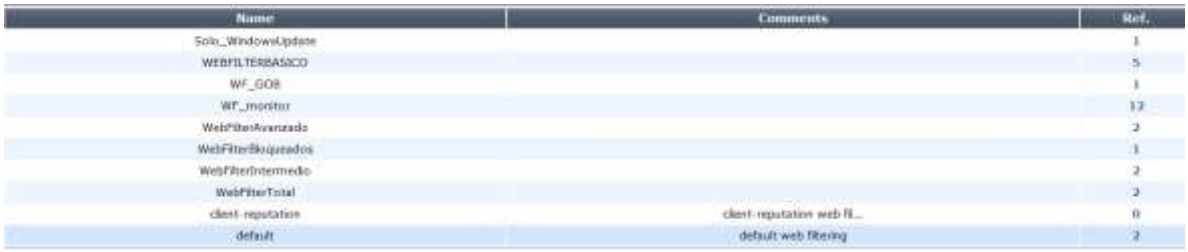
Fuente: Elaboración propia

5.3.2 Filtro Web

- **Filtro por categorías**

  Los filtros de Acceso Web son creados por categorías según los perfiles de los usuarios, se han sido divido en 9 grupos de acuerdo a las necesidades de la empresa, cada perfil de acceso web tiene sus respectivas categorías bloqueadas y habilitadas como se muestra en la figura 5.27.

Figura 5.27: Filtros web

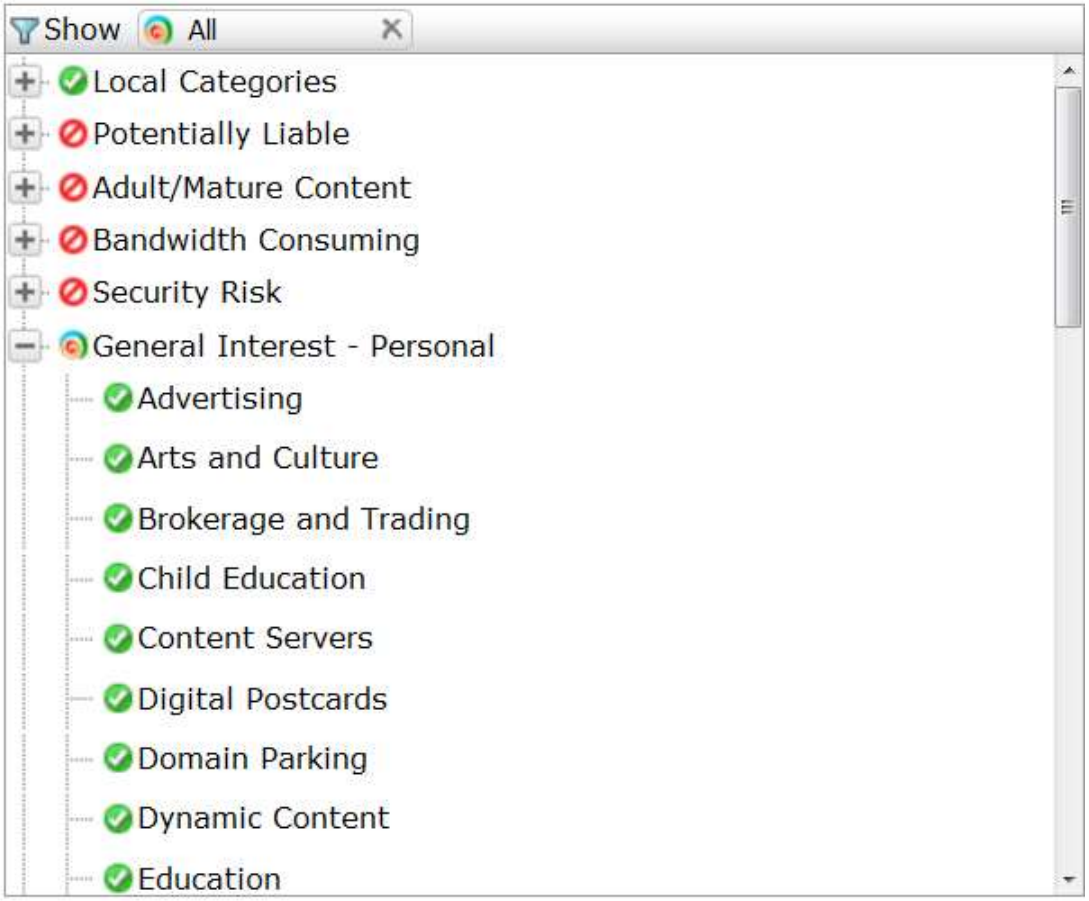


Name	Comments	Ref.
Soln_WindowsUpdate		1
WEBFILTERBASICO		5
WF_GOB		1
WF_monitor		13
WebFilterAvanzado		2
WebFilterBloqueados		1
WebFilterIntermedio		2
WebFilterTotal		2
client-reputation	client-reputation web fil...	0
default	default web filtering	2

Fuente: Elaboración propia

Figura 5.28 se referencia las categorias establecidas a la base de datos Fortiguard.

Figura 5.28: Filtros web por Categoría



Fuente: Elaboración propia

- **Filtro por URL**

  Se crean los filtros de acceso vía URL específicos , en está sección se da acceso o restricción considerando que por categoría están siendo restringidos ó cuentan con acceso, como se aprecia en la figura 5.29.

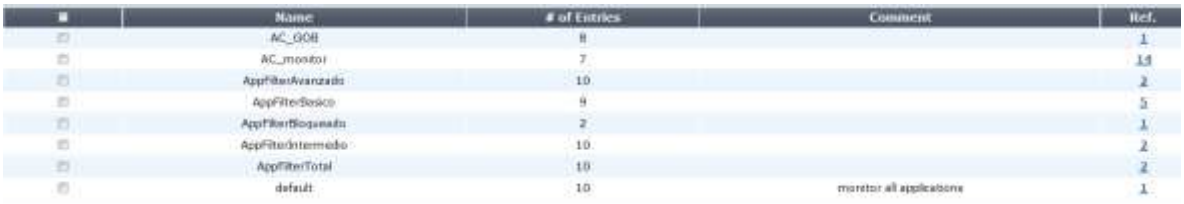
Figura 5.29: Filtros por URL

Fuente: Elaboración propia

5.3.3 Control de Aplicación

En este apartado se crean los filtros de control de aplicaciones correspondientes a los diferentes perfiles según las necesidades de la empresa, cada filtro de aplicación tiene sus respectivas aplicativos bloqueadas y habilitadas, como se muestra en la figura 5.30.

Figura 5.30: Control de aplicaciones



Fuente: Elaboración propia

A su vez se tendra los filtros por categorias dadas por la base de datos Fortiguard como se ve en el figura 5.31.

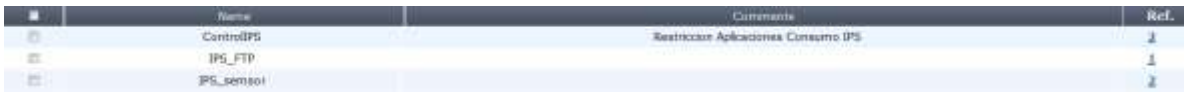
Figura 5.31: Configuración de Control de Aplicaciones

Fuente: Elaboración propia

5.3.4 Sensores IPS

En este apartado se crean los sensores IPS [16] para los servidores las cuales ayudan a detectar ataques a los servicios de la empresa, como se ve en la figura 5.32.

Figura 5.32: Sensores IPS



Fuente: Elaboración propia

5.3.5 DoS Sensor

En este apartado se configuran los sensores DoS [16] para los servidores, los cuales ayudan a detectar algún tipo de ataque o tráfico anómalo en los servicios de la empresa. Este agregado se deja en monitoreo para poder verificar si es que hay algún tipo de intento de denegación de servicio y sobre ello tomar las medidas preventivas del caso, como se aprecia en la figura 5.33.

Figura 5.33: Sensor DoS

Fuente: Elaboración propia

En la figura 5.34. se muestra las políticas en la cual se aplica el sensor DoS.

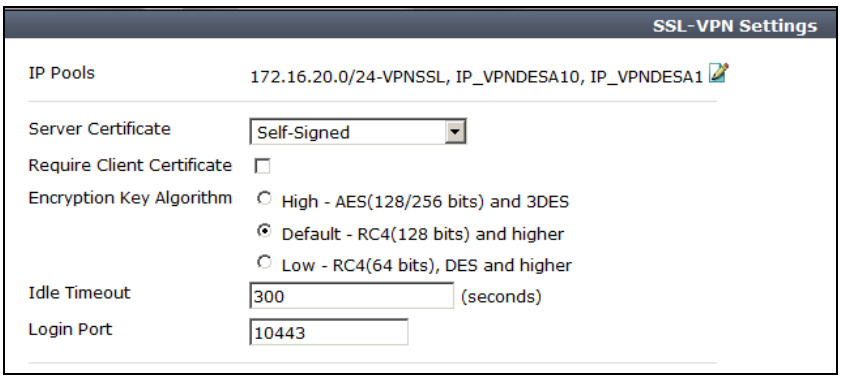
Figura 5.34: Política aplicada al Sensor DoS

Fuente: Elaboración propia

5.3.6 Configuración VPN SSL

En este apartado se creó la VPN SSL para la conexión de usuarios remotos y de este modo puedan acceder a los recursos de la empresa, como se muestra en la figura 5.35.

Figura 5.35: Configuración VPN SSL



Fuente: Elaboración propia

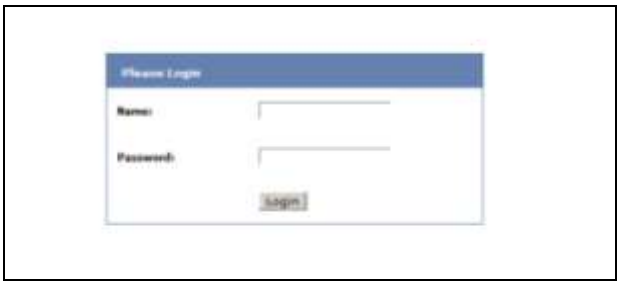
A su vez se tiene distintos grupos de VPN que hacen referencia a diferentes niveles de accesos en la misa, tal como se muestra en la figura 5.36.

Figura 5.36: Grupos VPN SSL

Fuente: Elaboración propia

En la figura 5.37 se muestra el Portal de acceso vía web.

Figura 5.37: Portal de acceso VPN SSL



Fuente: Elaboración propia

5.4 Configuración del módulo de Políticas del firewall

A continuación se detallan las políticas de seguridad que han sido configuradas en el firewall.

5.4.1 Políticas LAN a WAN.

En la figura 5.38. se muestran las políticas de seguridad configuradas en el firewall donde se pueden observar los filtros aplicados previamente configurados.

Figura 5.38: Políticas de LAN a WAN

Fuente: Elaboración propia

5.4.2 Políticas WAN a LAN

El detalle de las politicas se dan por el sentido de las interfaces de Wan a LAN, como se muestra en la figura 5.39.

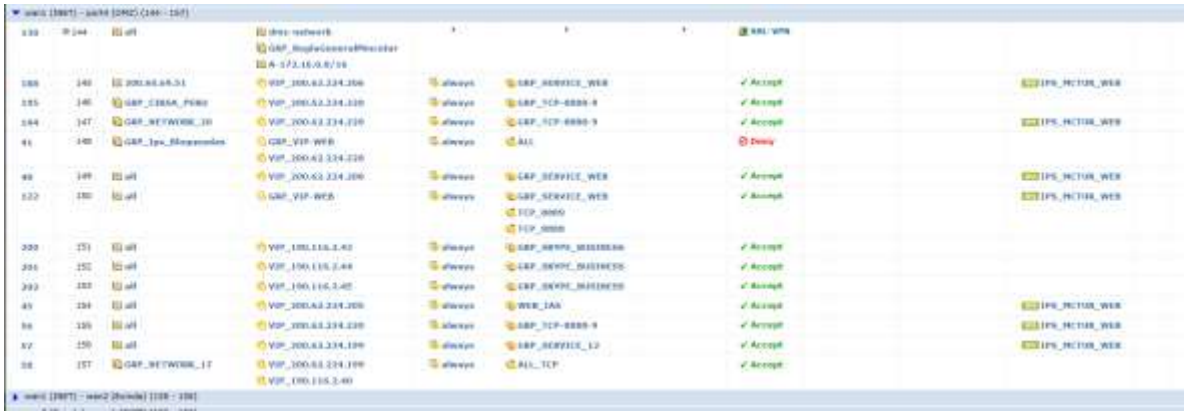
Figura 5.39: Políticas de WAN a LAN

Fuente: Elaboración propia

5.4.3 Políticas WAN a DMZ

El detalle de las politicas se dan por el sentido de las interfaces de Wan a LAN, como se muestra en la figura 5.40.

Figura 5.40: Políticas de WAN a DMZ

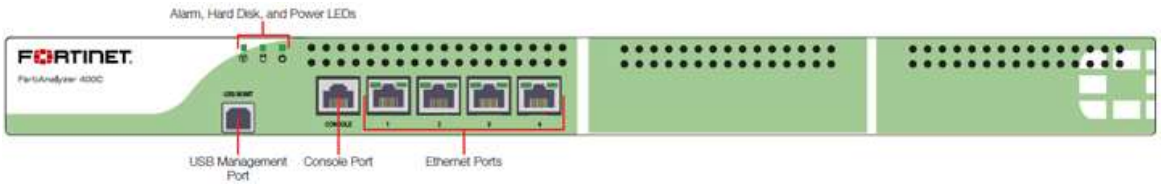


Fuente: Elaboración propia

5.5 Instalación del FortiAnalyzer

En este apartado se explicará la configuración del equipo FortiAnalyzer. Este equipo cumplirá la función de almacenar toda información que los equipos FortiGate es decir el envio de eventos o Logs, se muestra la parte frontal en la figura 5.41.

Figura 5.41: FortiAnalyzer parte Frontal (ver anexo 03)



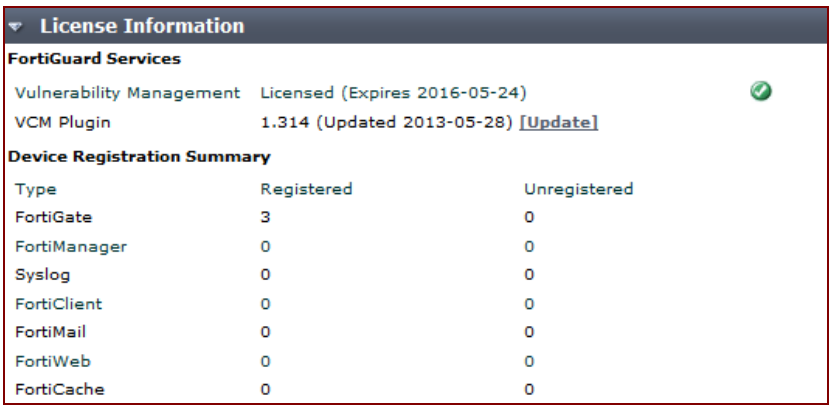
Fuente: www.avfirewalls.com

5.5.1 Licenciamiento del equipo

Las licencias se activaron satisfactoriamente en el equipo, dicha activación se realiza en el portal de Fortinet de tal manera se valida que dicho licenciamiento

este asociado con el número de serie del equipo. En la figura 5.42 se detalla el licenciamiento y servicios del FortiAnalyzer activados en su totalidad.

Figura 5.42: Licenciamiento de FortiAnalyzer



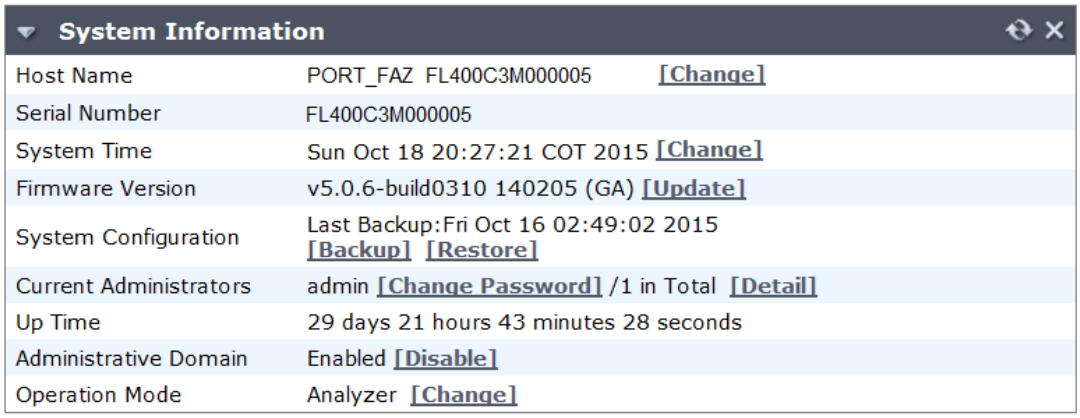
Fuente: Elaboración propia

5.5.2 Información del sistema

Se muestra la información del equipo en la cual se describe como se está configurado a nivel de sistema el FortiAnalyzer.

Se muestra datos importantes en la figura 5.43 como:

Figura 5.43: Información del sistema



Fuente: Elaboración propia

5.5.3 Interfaces configurados

Ahora se muestra en la figura 5.44 el direccionamiento IP asignado a la interface en el FortiAnalyzer.

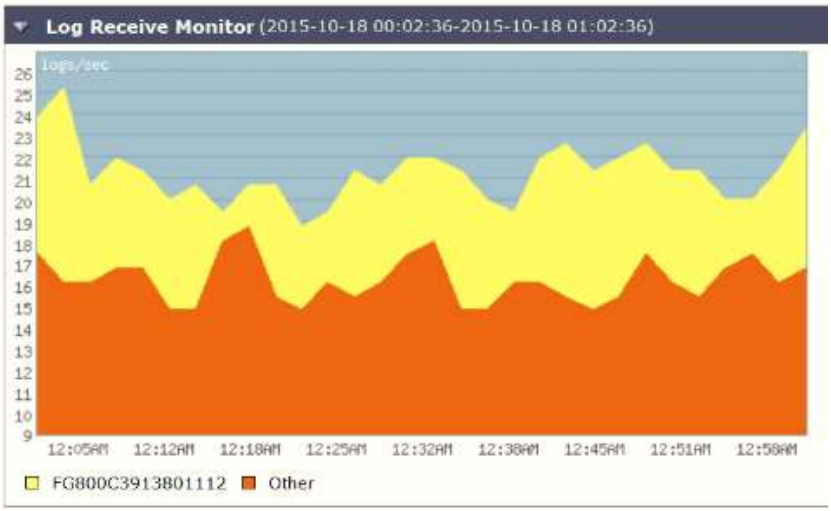
Figura 5.44: Interfaz de gestión

Fuente: Elaboración propia

5.5.4 Recepción de Log

Se procede a verificar la recepción de log del cliente y se corrobora que el canal de envió es ideal para la cantidad, se valida en la figura 5.45 la recepción de logs.

Figura 5.45: Tráfico de Log

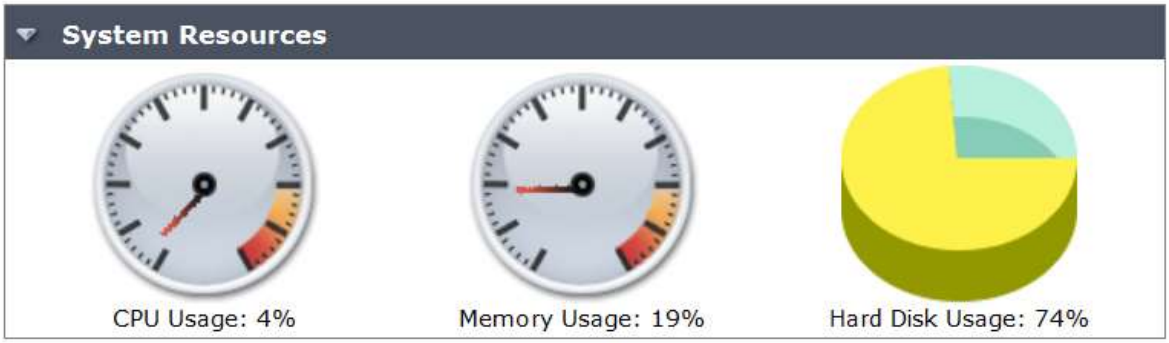


Fuente: Elaboración propia

5.5.5 Recursos

Se muestra en la figura 5.46 tal cual se ve en la consola web el espacio consumido del disco, CPU y memoria del FortiAnalyzer.

Figura 5.46: Ventana de Recursos



Fuente: Elaboración propia

5.5.6 Usuario Administrador

La administración del equipo es dada por el usuario admin el cual es el usuario del proveedor de seguridad, se tiene configurado las direcciones de red de confianza las cuales son las únicas desde donde se podrá acceder al equipo, como se valida en la figura 5.47.

Figura 5.47: Usuario Administrador

Fuente: Elaboración propia

5.5.7 Configuración SNMP

Se muestra la configuración realizada para el monitoreo del equipo atreves de sistemas SNMP. En este apartado se ha configurado el protocolo SNMP con nombre de la comunidad **ntsecurity**, como se valida en la figura 5.48.

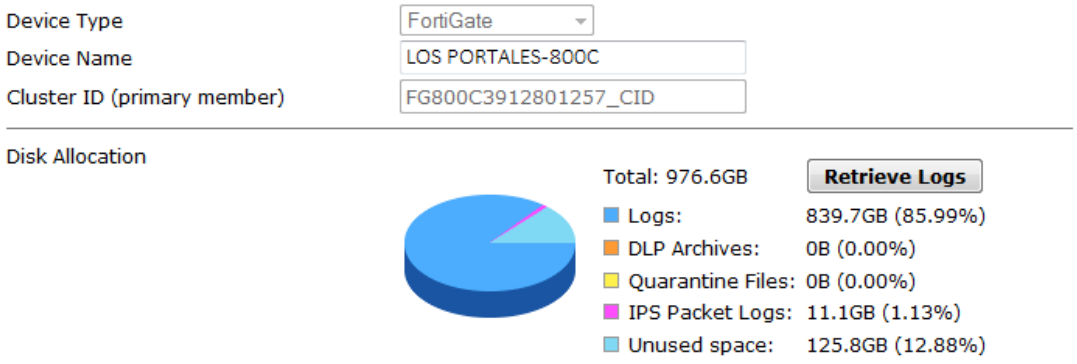
Figura 5.48: Comunidad SNMP

Fuente: Elaboración propia

5.5.8 Integración de los equipos al FortiAnalyzer

Se integró al FortiAnalyzer todos los equipos de Los Portales, las cuales son un los dos FGT800C en HA que si están enviando los Log en modo clúste, como se valida en la figura 5.49.

Figura 5.49: Cuota de disco asignado



Fuente: Elaboración propia

5.5.9 Monitor de log

Se muestra en la figura 5.50 los Log's almacenados en el FortiAnalyzer actualmente de todos los equipos registrados.

Figura 5.50: Log en tiempo real

Fuente: Elaboración propia

5.6 Instalación del FortiMail

En este apartado se explicará la configuración del equipo FortiMail. Este equipo servirá para proteger a la empresa de correos spam por medio de políticas.

5.6.1 Licenciamiento del equipo

Las licencias se activaron satisfactoriamente en los equipos, como se valida en la figura 5.51. Se detalle el licenciamiento y servicios del firewall activados en su totalidad.

Figura 5.51: Información de licencia

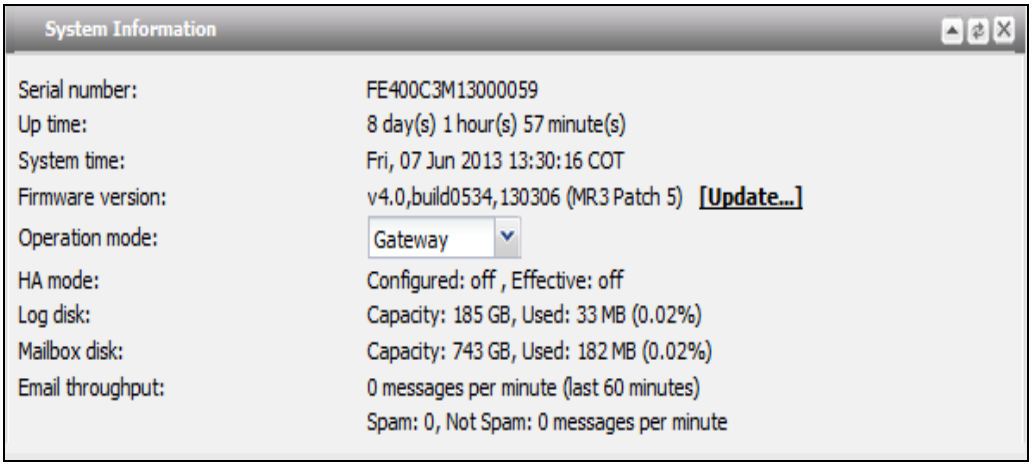
Fuente: Elaboración propia

5.6.2 Información del sistema

Se muestra la información del equipo en la cual se describe como se está configurado a nivel de sistema el FortiMail.

Se muestra datos importantes en la figura 5.52 como:

Figura 5.52: Información del sistema

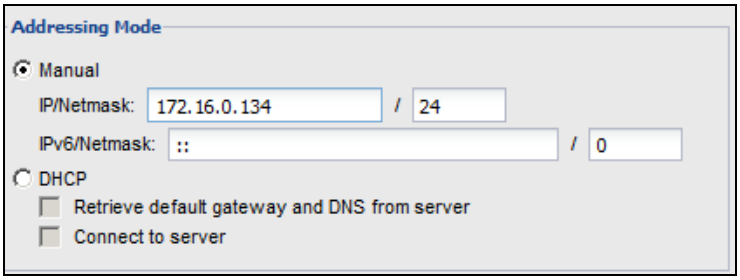


Fuente: Elaboración propia

5.6.3 Interfaces configurados

El direccionamiento IP que se asignó a la interface en el FortiMail se detalla en la figura 5.53.

Figura 5.53: Interfaz de gestión

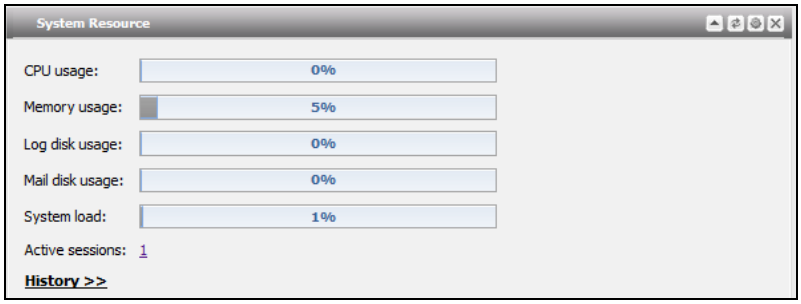


Fuente: Elaboración propia

5.6.4 Recursos

Se muestra el porcentaje de almacenamiento del Disco, así mismo el CPU y memoria del equipo.

Figura 5.54 Ventana de Recursos



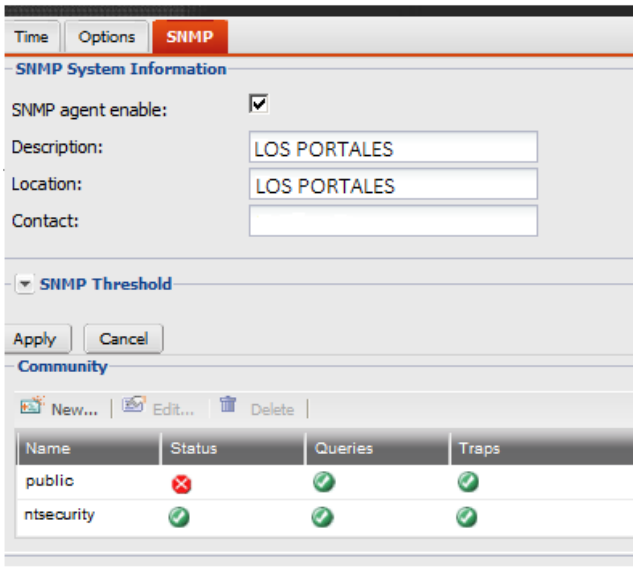
Fuente: Elaboración propia

5.6.5 Configuración SNMP

Se muestra la configuración realizada para el monitoreo del equipo atreves de sistemas SNMP. En este apartado se ha configurado el protocolo SNMP con nombre de la comunidad **ntsecurity**.

Se muestra en la figura 5.55 se muestra la configuración asociado al fortimail.

Figura 5.55 Comunidad SNMP

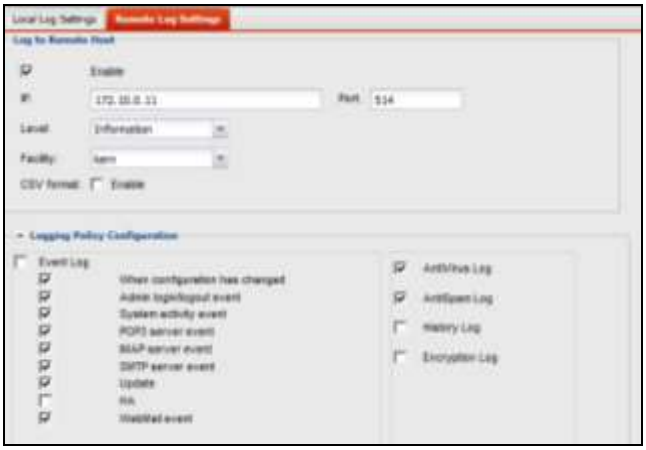


Fuente: Elaboración propia

5.6.6 Integración del equipo al FortiAnalyzer

En la Figura 5.56 se muestra la configuración que tiene el equipo FortiMail para que realice el envio de Logs al FortiAnalyzer.

Figura 5.56: Envío de log remoto al FortiAnalyzer



Fuente: Elaboración propia

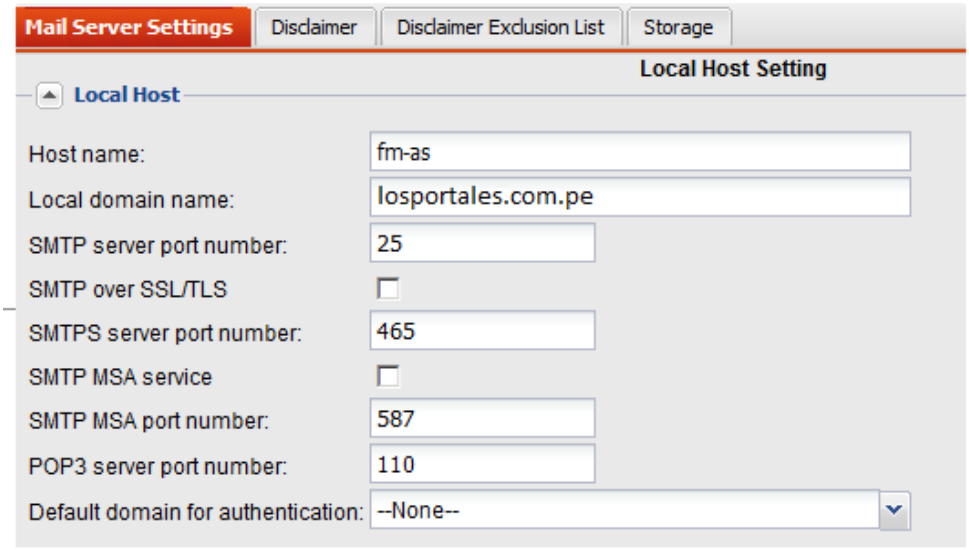
5.7 Configuración del FortiMail

Después de la instalación física del equipo y conexión de las interfaces se proceden a configurar el FortiMail.

5.7.1 Configuración del Módulo Mail Settings

En este módulo se configura el Nombre de host del FortiMail. Así como el Dominio, puerto, se detalla en la figura 5.57 lo detallado.

Figura 5.57: Configuración Mail Server



Fuente: Elaboración propia

5.7.2 Configuración del Módulo Domain

En este módulo se configura los dominios que el FortiMail protegerá, en este caso solo es uno “losportales.com.pe”, “hotelcountry.com” y “caudalosa.com.pe”, como se ve en la figura 5.58.

Figura 5.58: Dominio

Fuente: Elaboración propia

5.7.3 Configuración del Módulo Policy

Se detalla la configuración de las dos modalidades en políticas basadas en el recipiente las cuales son: **Incoming y Outcoming**

- **Incoming**

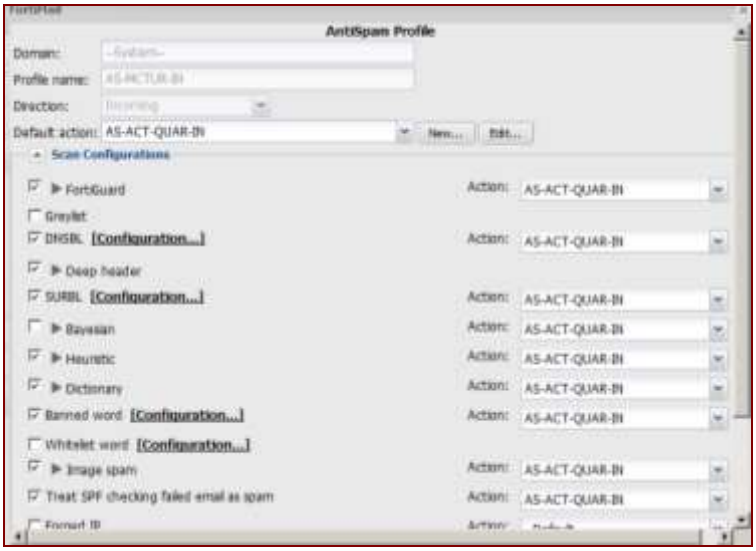
En esta opción se ha configurado las políticas de ingreso de correo, en la cual se aplica los filtros antispam y antivirus, como se ve en la figura 5.59.

Figura 5.59: Políticas de correo de ingreso

Fuente: Elaboración propia

Se configuro también el filtro antispam en la política de entrada, cuya acción es enviar a cuarentena, como se muestra en la figura 5.60.

Figura 5.60: Filtro AntiSpam



Fuente: Elaboración propia

- **Outcoming**

En esta opción se ha configurado las políticas de salida de correo como se puede mostrar en la figura 5.61.

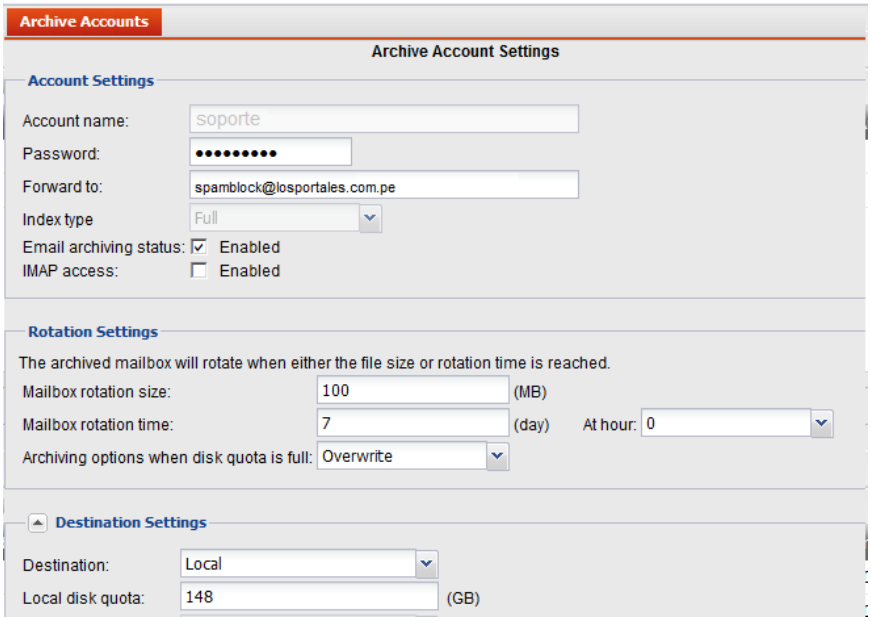
Figura 5.61: Filtro de Correo de salida

Fuente: Elaboración propia

5.7.4 Módulo archiving

En este módulo se ha configurado la funcionalidad de archivar todos los correos que salen a través del FortiMail. Con esta funcionalidad el cliente podrá guardar todos los correos que el FortiMail procese, se observa en la figura 5.62.

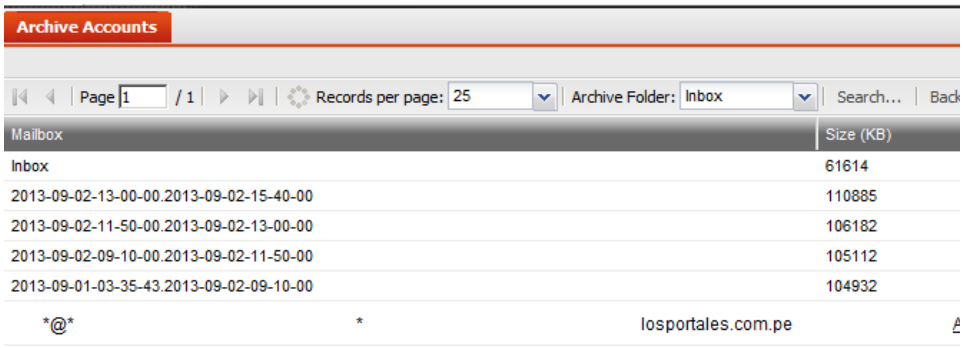
Figura 5.62: Archiving



Fuente: Elaboración propia

Se muestra en la figura 5.63 el archivamiento de correos en el disco duro del FortiMail.

Figura 5.63: Verificación del archivamiento



Fuente: Elaboración propia

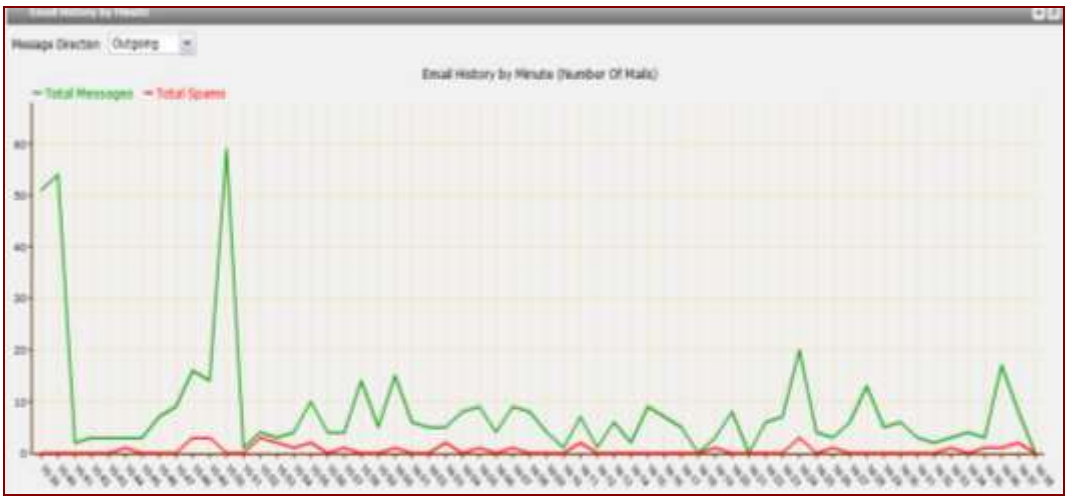
5.8 Pruebas de correo

Terminada la configuración y puesta en producción del equipo, se muestran las pruebas de la operatividad de la configuración:

5.8.1 Trafico de correo

Se puede observar que hay tráfico de correo ingresante, el cual se aprecia en el cuadro histórico, en la figura 5.64.

Figura 5.64: Trafico histórico

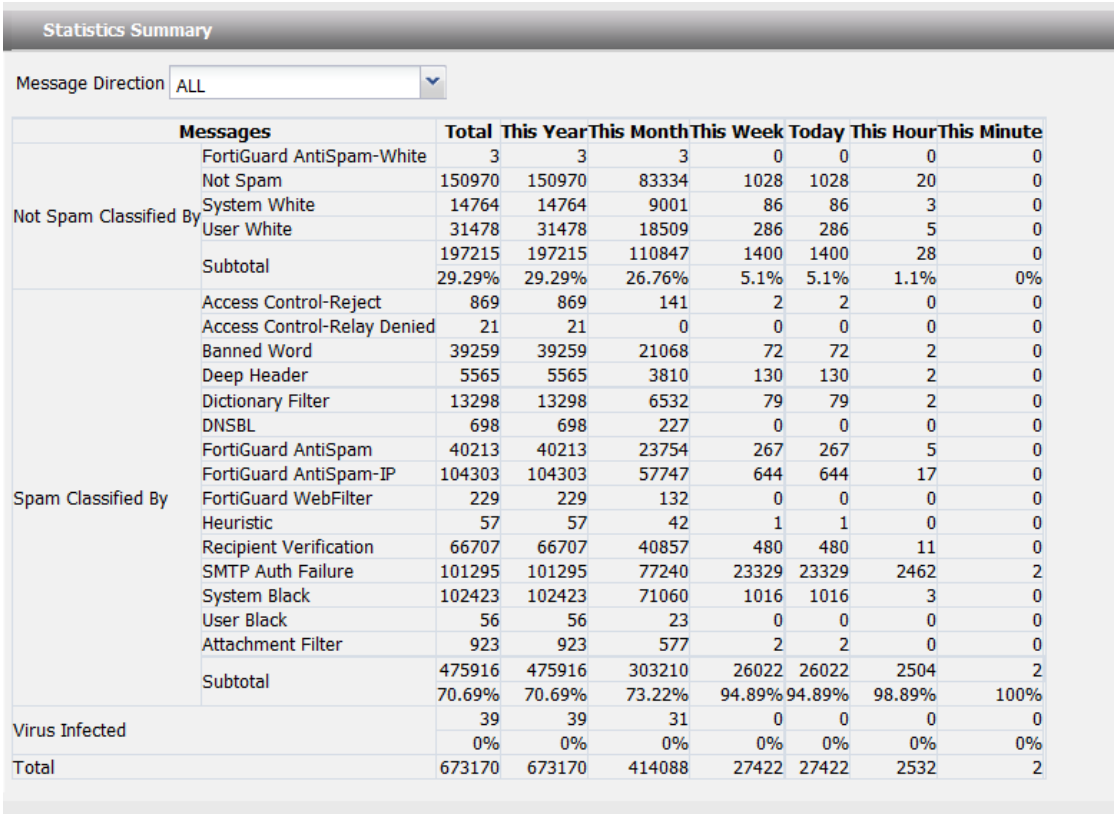


Fuente: Elaboración propia

5.8.2 Cuadro Estadístico

Se puede observar un cuadro estadístico de trafico de correo ingresante, el cual se aprecia en la figura 5.65.

Figura 5.65: Cuadro estadístico



Statistics Summary

Message Direction ALL

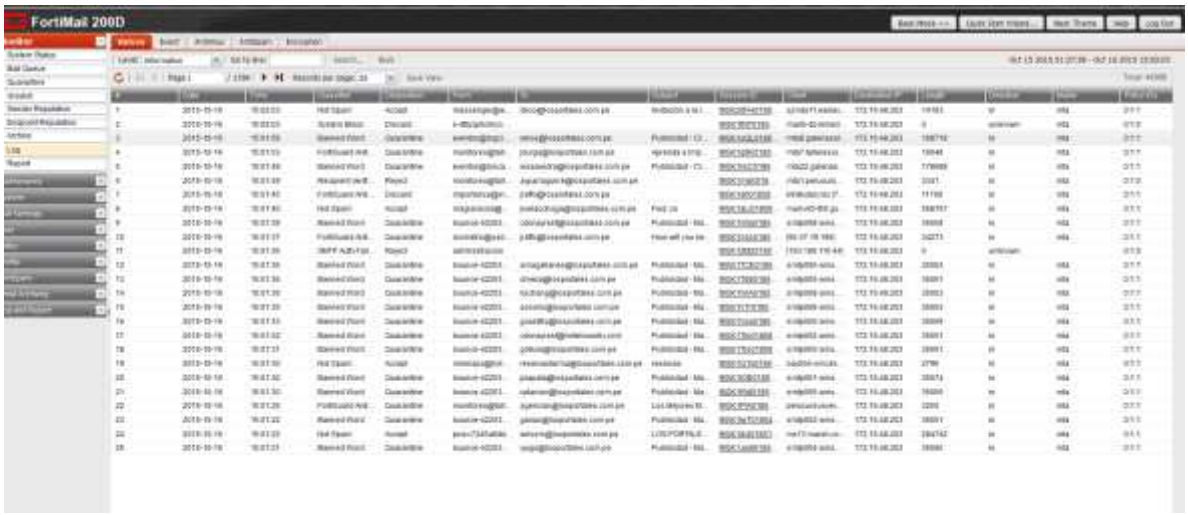
Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	FortiGuard AntiSpam-White	3	3	3	0	0	0	0
	Not Spam	150970	150970	83334	1028	1028	20	0
	System White	14764	14764	9001	86	86	3	0
	User White	31478	31478	18509	286	286	5	0
	Subtotal	197215	197215	110847	1400	1400	28	0
		29.29%	29.29%	26.76%	5.1%	5.1%	1.1%	0%
Spam Classified By	Access Control-Reject	869	869	141	2	2	0	0
	Access Control-Relay Denied	21	21	0	0	0	0	0
	Banned Word	39259	39259	21068	72	72	2	0
	Deep Header	5565	5565	3810	130	130	2	0
	Dictionary Filter	13298	13298	6532	79	79	2	0
	DNSBL	698	698	227	0	0	0	0
	FortiGuard AntiSpam	40213	40213	23754	267	267	5	0
	FortiGuard AntiSpam-IP	104303	104303	57747	644	644	17	0
	FortiGuard WebFilter	229	229	132	0	0	0	0
	Heuristic	57	57	42	1	1	0	0
	Recipient Verification	66707	66707	40857	480	480	11	0
	SMTP Auth Failure	101295	101295	77240	23329	23329	2462	2
	System Black	102423	102423	71060	1016	1016	3	0
	User Black	56	56	23	0	0	0	0
	Attachment Filter	923	923	577	2	2	0	0
	Subtotal	475916	475916	303210	26022	26022	2504	2
		70.69%	70.69%	73.22%	94.89%	94.89%	98.89%	100%
Virus Infected		39	39	31	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
Total		673170	673170	414088	27422	27422	2532	2

Fuente: Elaboración propia

5.8.3 Log de Correo

Se puede observar en la figura 5.66 los log de coreos salientes en el FortiMail.

Figura 5.66: Log generado en el FortiMail



Fuente: Elaboración propia

CONCLUSIONES

1. En el presente informe hablamos sobre la importancia de la seguridad perimetral en general y en la empresa Inmobiliaria a la cual mencionamos, hicimos referencias sobre a las formas que existen para proteger los sistemas informáticos y la información que contienen sobre accesos no autorizados, daños, modificaciones o destrucciones para proteger los equipos y la red de Los Portales, se hace la acotación omitido información que pueda crear brecha de seguridad para el cliente.
2. Todo sistema es susceptible de ser atacado, por lo que conviene prevenir esos ataques. Conocer las técnicas de ataque ayuda a defenderse más eficientemente. Por ende el fin de esta esta Tesis es dar a conocer de manera real como se ha puede generar una barrera de seguridad contra muchos de los tipos de ataques actuales.
3. La solución de la seguridad perimetral instalada en Los Portales fue realizado en un primer momento en un ambiente de laboratorio y luego implementados en la red de Los Portales, realizando las validaciones respectivas con aprobación del cliente.
4. Los equipos fueron instalados y configurados para poder dar la máxima protección a la red, pero siempre se debe estar actualizando y monitoreando buscando nuevas amenazas que puedan existir en Internet o con el pasar del tiempo los accesos de restricción de un servicio hayan variado, por eso es recomendable realizar periódicamente una depuración en las políticas antiguas como parte de un mantenimiento preventivo.

RECOMENDACIONES

1. Estamos hablando de una empresa que crece día a día, por tanto el tipo de red crece de manera escalable, será necesario entonces hacer un análisis cada cierto tiempo, es decir realizar las pruebas correspondientes con respecto a la respuesta que tienen los equipos y luego de ello poder decidir entre migrar a equipos de mayor performance o en todo caso agregar más equipos a la red que de tal forma que permita el buen desempeño.
2. La empresa por medio de reportes generados por su equipo FortiAnalyzer podrá visualizar al detalle todos los tipos de eventos y consumo de Bw, es aquí donde el administrador de red tendrá que evaluar entre la segmentación de su red y/o considerar evaluar los perfiles web y redefinir los accesos por contenidos.
3. Por buenas prácticas, se recomienda que la versión de firmware de cada uno de los equipos sea la más estable, es decir la recomendada por el fabricante, ya que de esta manera se puede garantizar el buen funcionamiento en conjunto de los dispositivos.
4. El administrador de la red debe de considerar tener una bitácora de casos, en donde se encuentren todos los cambios o configuraciones realizadas, que serán solicitadas a la empresa que les brinda servicio de administración de sus equipos o en su defecto para tener un orden apropiado en las políticas configuradas en el equipo Firewall.

REFERENCIAS BIBLIOGRAFÍA

[1] Análisis de redes y sistemas de comunicaciones Xavier Hesselbach Serra, Jordi Altés Bosch https://goo.gl/YVhro2

[2] Historia delitos informáticos, http://web.mit.edu/rhel-doc/3/rhel-sg-es-3/ch-sgs-ov.html

[3] Phishing, http://www.seguridad.internautas.org/html/451.html

[4] Seguridad en Internet Olaf Adam, https://goo.gl/QMkFJq

[5] Router Perimetral, http://www.upcommons.upc.edu/

[6] NAT en Firewall, https://www.ingate.com/files/Solving_Firewall-NAT_Traversal.pdf

[7] IDS, www.segu-info.com.ar

[8] VPN, http://www.kb.netgear.com

[9] DMZ, http://es.ccm.net/contents/pdf/589-dmz-zona-desmilitarizada

[10] Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander SchmidA, Comprehensive Guide to Virtual Private Networks, Volume I (1999).

[11] Diego González lopez, Diego, Sistema de detección de Intrusos, Versión 1.01 (2007).

[12] Michael Erbscholoe, Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code 1st Edition (2005).

[13] Guido Schryen, Anti-Spam Measures: Analysis and Design. (2010).

[14] Gartner Analyst, http://www.gartner.com/technology/analysts.jsp.

[15] Fortinet

http://www.fortinet.com

[16] The Fortigate Cookbook

http://cookbook.fortinet.com

[17] Labs Fortigate

http://www.fortiguard.com

ANEXO 01 Fortigate 800C

FORTINET

DATASHEET

FortiGate®-800C

Accelerated Security for Mid-Sized Enterprises and Large Branch Offices

FortiGate Unified Threat Management (UTM) systems from Fortinet® offer you the freedom to select the security solution that most closely matches your port density, performance, and bandwidth needs. With firewall performance of 20 Gbps and IPS throughput of 8 Gbps and 10-GbE interfaces in a 1U form-factor, FortiGate-800C is ideal for mid-sized enterprises and large enterprise branch offices. The FortiGate-800C platform gives you the ability to improve your security posture and accelerate your network performance while simplifying your network infrastructure.

The Power of Unified Threat Management

Like other members of the FortiGate product family, the FortiGate-800C combines firewall, application control, IP Sec and SSL VPN, intrusion prevention, antivirus, antimalware, antispam and Web filtering into a single device. Equipped with these broad security capabilities, the FortiGate-800C can help organizations meet regulatory compliance requirements and protect against the latest targeted attacks, network vulnerabilities and malicious applications.

The FortiGate-800C supports today's advanced networks with with two (2) 10-GbE and twelve (12) 10/100/1000 interfaces that can be easily partitioned into independent security zones and custom combinations of LAN and WAN ports. Eight (8) shared copper/fiber GbE interfaces support evolving networks that may be migrating to fiber on select network segments. You can protect your network availability with two (2) pairs of bypass-enabled ports, allowing continued network operations in the event of device failure. Dual-WAN redundant connections for maximum reliability and availability are also supported by default and a dedicated DMZ port adds an extra layer of protection for Web-facing servers. The onboard USB management port provides an easy way to setup and configure the device using the FortiExplorer configuration wizard. In addition, the FortiGate-800C features 64 GB of internal storage for WAN optimization, local SQL-based reporting, or data archiving for policy compliance.

FortiOS 4.3: Redefining Network Security

FortiOS 4.3 is the software foundation of FortiGate multi-threat security platforms. Developed solely for security, performance and reliability, it is a purpose-built operating system that leverages the power of the FortiASIC content and network processors. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, antivirus/ antispyware, antispam, web filtering, application control, data loss prevention, and end point network access control.

The FortiASIC Advantage

FortiASIC processors power FortiGate platforms. With exclusive hardware, the purpose built, high performance Network, Security, and Content processors use intelligent and proprietary digital engines to accelerate resource intensive security services.

Challenge	Solution
Visibility and control of new applications and content	FortiGate devices deliver complete, comprehensive application control, enabling you to block unwanted traffic and behavior.
Time-sensitive applications require extremely low latency during transit	FortiGate-800C appliance ensures that security is never a bottleneck. Up to 20 Gbps firewall performance and up to 8 Gbps IPSec VPN performance ensures optimal performance of latency-sensitive applications.
Internal network segmentation is difficult to deploy	FortiGate-800C appliance with 24 hardware-accelerated switched ports permit a wide-array of deployments.
Evolution of network infrastructure	The FortiGate-800C includes 2 10-GbE interfaces for maximum performance, as well as shared media interfaces to ease the transition from copper to fiber.
Eliminating blind spots caused by using multiple non-integrated security technologies	Fortinet combines core security technologies such as firewall, VPN, intrusion prevention, and application control into a single platform, providing an effective all-in-one solution.

FortiGate Consolidated Security Solutions

Fortinet's consolidated security solutions provide you with an integrated set of core security and network services in a single, easy-to-manage, high-performance appliance that gives you unmatched flexibility to deploy the right mix of technology for your unique requirements. In addition, FortiGuard® Subscription Services include dynamic updates to ensure your security environment remains current and your corporate resources are protected against the latest threats.

Technical Specifications	FortiGate-800C
HARDWARE	
Accelerated 10-GbE SFP+ Interfaces	2
Accelerated 10/100/1000 Interfaces (RJ-45)	12
Accelerated GbE SFP or 10/100/1000 Shared Interfaces	8
Accelerated 10/100/1000 Bypass Interfaces	2 pairs
10/100/1000 Management Interface	2
Maximum Network Interfaces	26
Internal Storage	64 GB
USB Ports (Client/Server)	1 / 1
SYSTEM PERFORMANCE	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 20 Gbps
Firewall Latency (64 byte UDP packets)	6 µs
Firewall Throughput (Packets Per Second)	31 Mpps
Concurrent Sessions (TCP)	7 M
New Sessions/Sec (TCP)	180,000
Firewall Policies (System / VDOM)	100,000 / 50,000
IPSec VPN Throughput (512 byte packets)	9 Gbps
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000
Client-to-Gateway IPSec VPN Tunnels	50,000
SSL-VPN Throughput	1 Gbps
Concurrent SSL-VPN Users (Recommended Max)	1,000
IPS Throughput	6 Gbps
Antivirus Throughput (Proxy Based / Flow Based)	1.7 / 2.1 Gbps
Virtual Domains (Default / Max)	10 / 10
Max Number of FortiAPs	512
Max Number of FortiTokens	1,000
Max Number of FortiClients	2,000
High Availability Configurations	Active/Active, Active/Passive, Clustering
Unlimited User Licenses	Yes

Technical Specifications	FortiGate-800C
DIMENSIONS AND POWER	
Height	1.75 in (44 mm)
Width	17 in (432 mm)
Length	16.42 in (417 mm)
Weight	18.8 lb (8.5 kg)
Rack Mountable	Yes (Attachable Ears)
AC Power	100-240 VAC, 60-50 Hz
Power Consumption (Avg)	158 W
Power Consumption (Max)	183 W
Heat Dissipation	645 BTU/h
Redundant Power Supply (Hot-swappable)	Optional
ENVIRONMENT AND CERTIFICATIONS	
Operating temperature	32 - 104 °F (0 - 40 °C)
Storage temperature	-13 - 158 °F (-25 - 70 °C)
Humidity	20 to 90% non-condensing
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN

All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files.

Orderable	SKU
Unit	
FortiGate-800C	FG-800C
Optional Accessories	SKU
FG-800C, FG-900C and FG-1000C AC Power Supply	SP-FG800C-PS

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road 20-01, The Concourse
Singapore 199555
Tel +65.6513.3734
Fax +65.6295.0015

ANEXO 02 Fortimail 400C

FORTINET

DATASHEET

FortiMail™

Comprehensive Messaging Security

Proven Security

FortiMail appliances and virtual appliances are proven, powerful messaging security platforms for any size organization – from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, FortiMail appliances employ Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats.

Intelligent Protection

FortiMail prevents your messaging systems from becoming threat delivery systems. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents other antispam gateways from blacklisting your users by blocking outbound spam and malware, including mobile traffic. FortiMail dynamic and static user-blocking gives you granular control over all of your email policies and users.

Enforce secure content delivery with FortiMail Identity-Based Encryption (IBE), S/MIME, or TLS email encryption options. Prevent accidental and intentional loss of confidential data using FortiMail predefined or customized dictionaries.

High Performance and Unmatched Flexibility

FortiMail appliances provide high-performance email routing and security by utilizing multiple high-accuracy antispam filters. When coupled with industry leading real-time antivirus and antispyware protection from FortiGuard Services, FortiMail provides you with extremely fast and accurate messaging security that won't affect end users or delay their communications. Deploy messaging security in the mode that best suits your environment and users with FortiMail's unmatched flexibility.

Comprehensive Messaging Security

- ✓ Inspect more than 2 million emails per hour
- ✓ Unmatched deployment flexibility
- ✓ Apply Identity-Based Encryption in both push and pull methods
- ✓ Use customized and predefined dictionaries to prevent data loss
- ✓ Enforce email and security policies at a granular level
- ✓ Receive real-time security updates from FortiGuard® Services

vb platinum SPAM virusbtn.com

Features	Benefits
Deploy appliances or virtual appliances in Transparent, Gateway, or Server modes	All email servers on the market deploy in Server mode, some offering a Gateway mode option. Fortinet is the only vendor to offer Transparent mode, enabling FortiMail to intercept emails without changing DNS MX records, or existing email server network configurations.
Apply Identity-Based Encryption in both push and pull methods	Ensures secure delivery of confidential or regulated content. Extremely easy to deploy – no additional hardware or software to install, no user provisioning, no pre-enrollment for recipient.
Data Loss Prevention and Compliance	Detect accidental or intentional loss of confidential or regulated data. Achieve PCI-DSS or HIPAA compliance by blocking messages containing defined data patterns, or creating policies to enforce encryption of certain emails.
Identify and Block Spamming Endpoints	Prevent blacklisting of legitimate subscribers by identifying and blocking endpoints sending spam, including Smart phones. Ideal for Carriers and Service Providers.
No per-user or per-mailbox pricing	Complete, multi-layered antivirus, antispam, antispyware and anti-phishing protection for an unlimited number of users. Greatly reduces TCO.

SYSTEM

- Transparent, Gateway and Server Mode Deployment Options
- Flexible Interface Configuration Including VLAN and Redundant Interface Support
- Inbound And Outbound Inspection
- Multiple Email Domains With Domain Level Customization
- IPv6 And IPv4 Address Support
- Virtual Hosting Using Source and / or Destination IP Address Pools
- Policy Based Mail Archiving With Remote Storage Options
- SMTP Authentication Support Via LDAP, RADIUS, POP3 And IMAP
- LDAP-Based Email Routing
- Per User Inspection Using LDAP Attributes on a Per Policy (Domains Basis
- Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management
- Mail Queues Management
- Multiple Language Support For Webmail And Admin Interface
- Email Validation
- Maintains Local Sender Reputation List Based on:
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)

MANAGEMENT, LOGGING, AND REPORTING

- QuickStart Setup Wizard
- Basic / Advanced Management Modes
- Role Based Administration Accounts Per Domain
- Comprehensive activity and Incident logging and reporting
- Configuration Change and Management Event Logging
- Built-in Reporting module
- FortiManager and FortiAnalyzer Support for Central Management and Reporting
- Centralised Quarantine for large scale deployments
- SNMP Support Using Standard and Private MIB with Threshold Based Traps
- External or Local Storage Server Support, Including iSCSI devices
- External Syslog support

HIGH AVAILABILITY (HA)

- Supported In all Modes
- Active-Passive Mode
- Configuration Synchronization Mode (Configuration Master and Slave Mode)
- Quarantine and Mail Queue Synchronization
- Device Failure Detection and Notification
- Link Status, Failover and Redundant Interface Support

ANTISPAM PROFILE

- FortiGuard Antispam Service
  - Global Sender Reputation
  - Spam and phishing URIs and email addresses
  - Spam Object checksums
  - Dynamic Heuristic Rules
- Greylisting for IPv4, IPv6 addresses and email accounts
- Local Sender Reputation (IPv4, IPv6 and End Point ID based)
- Deep Email Header Inspection
- Flexible Action and Notification Profiles
- Third party Spam URI and Real Time Blacklists (SURBL/RBL)
- Quarantining, tagging and end user reporting
- PDF Scanning and Image Analysis
- Black/White Lists at Global, Domain, and User levels.
- Bayesian Statistic Filtering

ANTIVIRUS

- FortiGuard Antivirus Service
- Quarantine, Repackage, Replace, and Monitor Actions
- Nested Archive Scanning
- Malware Detection

CONTENT BASED PROTECTION

- Dictionary based filtering in inbound or outbound direction
- Filter by Attachment File Type
- Banned Word Filtering

DENIAL-OF-SERVICE PROTECTION

- Inbound and Outbound Message Rate Limiting
- Recipient Address Attack
- Reverse DNS Check (Anti-Spoofing)
- Forged Sender Address

ENCRYPTION

- Identity-based Encryption for Push/Pull Delivery of Encrypted Messages
- S/MIME Support for Gateway-to-Gateway Encryption
- Support for strong-crypto protocols including HTTPS, SMTPS, SSH, IMAPS and POP3S

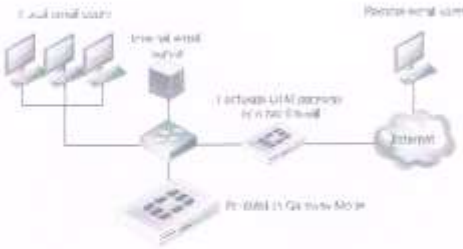
SERVER MODE SPECIFIC FEATURES

- SMTP, IMAP, and POP3 Email Services
- SMTP over SSL Support
- Disk Quota Policy Support for User Accounts
- Secure WebMail Client Access
- User, Group and Alias List Support
- Local Account and LDAP Authentication
- WebMail Calendar
- Email Auto Reply and Forwarding Preference
- Address Book Synchronize with LDAP

FortiMail Deployment Options

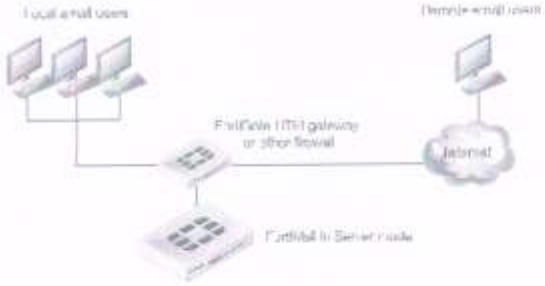
Choose from three modes of deployment – Transparent, Gateway, or Sever mode – to meet your specific messaging security requirements, while minimizing infrastructure changes and service disruptions:

- **Gateway Mode:** Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery.



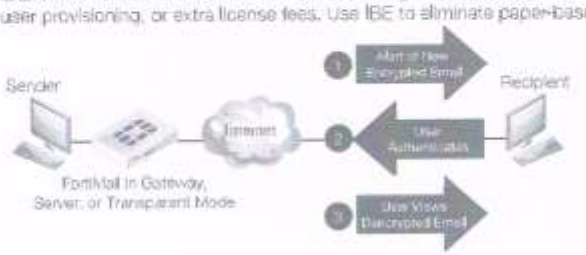
- **Transparent Mode:** Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, then transmits email to the destination email server for delivery. This eliminates the need to change the DNS MX record, or to change the existing email server network configuration.

- **Server Mode:** The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



Identity Based Encryption (IBE)

IBE allows FortiMail to deliver confidential and regulated email securely – without requiring additional hardware, software user provisioning, or extra license fees. Use IBE to eliminate paper-based communications and reduce costs.



- **Policy-Based Encryption:** Automatically encrypt messages for compliance, based on content or recipient.
- **Push or Pull Mode:** Use Push, Pull, or a combination of modes to meet your requirements.
- **Easy to Deploy, Use, and Manage:** Deploy IBE in any mode, including Transparent mode, without user provisioning or additional hardware or software.

Technical Specifications	FortiMail-100C	FortiMail-400C	FortiMail-2000B	FortiMail-3000C	FortiMail-5002B
Hardware Specifications					
10/100 Interfaces (Copper, RJ-45)	1	[illegible]	[illegible]	[illegible]	[illegible]
10/100/1000 Interfaces (Copper, RJ-45)	2	[illegible]	6	[illegible]	2
SFP Gigabit Ethernet Interfaces	0	0	0	2	0
Internal Hard drives / Hot Swappable [illegible] Interfaces	0	0	8	6	0/2
Redundant Hot Swappable Power Supplies	No	No	Yes	Yes	N/A
Storage	1 TB	2 x 1 TB	2 x 1 TB (8 TB Optional)	2 x 1 TB (6 TB Optional)	[illegible]
RAID Storage Management	No	[illegible]	Software [illegible] (Based on Drive Count)	[illegible] (Based on Drive Count)	No
Form Factor	Desktop	Rack Mount Appliance	Rack Mount Appliance	Rack Mount Appliance	ATCA Chassis
System Specifications					
Email Domains	50	100	8,000	5,000	10,000
Recipient-based Policies (Domain / System) - Incoming / Outgoing	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Server Mode Mailboxes	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Antispam, Antivirus, Authentication and Content Profiles per Domain / per System	50 / 60	50 / 200	50 / 600	50 / 600	50 / 300
Centralized Quarantine	Yes	Yes	Yes	Yes	Yes
[illegible]					
Email Routing	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FortiGuard Antispam	[illegible]	[illegible]	1.4 Million	1.8 Million	2.2 Million
FortiGuard Antispam + Antivirus	85,000	185,000	1.2 Million	1.6 Million	2.0 Million
Dimensions					
Height x Width x Length (in)	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Height x Width x Length (cm)	4.4 x [illegible] cm	4.5 x 43.6 x 36.5 cm	[illegible]	9.0 x 44.2 x 66.1 cm	[illegible]
Weight	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Environment					
Power Required	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Power Consumption (AVG)	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Heat Dissipation	[illegible] BTU	[illegible] BTU	[illegible] BTU	[illegible] BTU	[illegible] BTU
Operating Temperature	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Storage Temperature	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Humidity	[illegible] non-condensing	[illegible] non-condensing	[illegible] non-condensing	[illegible] non-condensing	[illegible] non-condensing
Compliance					
	FCC Class A Part 15, UL Mark	FCC Class A Part 15, UL/CUL, C Tick, VCCI	FCC Class A, UL/CUL, C Tick, VCCI, US EPA Energy Star Compliant	FCC Class A, UL/CUL, C Tick, VCCI, US EPA Energy Star Compliant	FCC Class A Part 15, UL/CUL
Certifications					
	[illegible]				FCC 47 CFR Part 15, [illegible]

FortiMail Virtual Appliances	VM01	VM02	VM04	VM08
[illegible]				
Hypervisors Supported	[illegible]			
Max vCPUs Supported	1	2	4	4
Max vNICs	4	4	4	4
Virtual Machine Storage (Min / Max)	50 GB / 1 TB	50 GB / 1 TB	50 GB / 2 TB	50 GB / 2 TB
Virtual Machine Memory Required (Min / Max)	1 GB / 2 GB	1 GB / 4 GB	1 GB / 8 GB	1 GB / 12 GB
[illegible] Performance				
Email Routing	[illegible]	[illegible]	[illegible] Million	[illegible] Million
FortiGuard Antispam	85,000	234,000	[illegible] Million	1.50 Million
FortiGuard Antispam + Antivirus	77,600	195,400	1.03 Million	1.40 Million

FortiMail Virtual Appliances	VM01	VM02	VM04	VM08
[illegible]				
Email Domains	[illegible]	[illegible]	[illegible]	[illegible]
Recipient-based policies (Domain / System)	60 / 300	[illegible]	1,500 / [illegible]	1,500 / [illegible]
Server Mode Mailboxes	[illegible]	[illegible]	[illegible]	[illegible]
Profiles (Domain / System)	[illegible]	[illegible]	[illegible]	[illegible]
Centralized Quarantine	Yes	Yes	Yes	Yes

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road 20-01, The Concourse
Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

FORTINET

FML-DAT-R22-201201

ANEXO 03 Fortianalyzer 400C

FORTINET

DATASHEET

FortiAnalyzer™

Centralized Logging, Analysis and Reporting

Enhanced Visibility With FortiAnalyzer Platforms

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. They provide organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability management. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet appliances and third-party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Security Event Information Management

You can put time back in your day by deploying a FortiAnalyzer platform into your security infrastructure, creating a single view of your security events, archived content, and vulnerability assessments. FortiAnalyzer platforms accept a full range of data from Fortinet solutions, including traffic, event, virus, attack, content filtering, and email filtering data. It eliminates the need to manually search multiple log files or manually analyze multiple consoles when performing forensic analysis or network auditing. A FortiAnalyzer platform's central data archiving, file quarantine and vulnerability assessment further reduce the amount of time you need to spend managing the range of security activity in your enterprise or organization.

Choice of Form Factor

Very few organizations use 100% hardware IT infrastructure or 100% virtual IT infrastructure today, creating a need for both hardware appliances and virtual appliances in your security strategy. FortiAnalyzer can be deployed as either hardware or a virtual appliance to fit your environment, which may include a mix of virtual and physical IT infrastructure. FortiAnalyzer will log events from FortiOS-based hardware appliances, virtual appliances, or a combination of both.

The FortiAnalyzer Difference

A FortiAnalyzer platform delivers complete security oversight with granular graphical reporting. Its breadth of data collection functions eliminate blind spots in your security posture. Its unique forensic analysis tools provide you with the ability to discover, analyze, and mitigate threats before perimeter breach or data loss. The FortiAnalyzer system's forensic analysis tool enables detailed user activity reports, while the vulnerability management tool automatically discovers, inventories and assesses the security posture of servers and hosts within the network infrastructure.

FortiAnalyzer systems come with a one-year limited hardware warranty and 90-day limited software warranty.

Features	Benefits
Network Event Correlation	Allows IT administrators to quickly identify and react to network security threats across the network.
Graphical Summary Reports	Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third party devices.
Scalable Performance and Capacity	FortiAnalyzer family models support thousands of FortiGate and FortiClient™ agents, and can dynamically scale storage based on retention/compliance requirements.
Centralized Logging of Multiple Record Types	Including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.
Seamless Integration with the Fortinet Product Portfolio	Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.
Choice of Standalone, Collector or Analyzer mode	Can be deployed as an individual unit or optimized for a specific operation (such as Store & Forward or Analytics).

FortiAnalyzer provides the following features

General System Functions

Profile-Based Administration
Secure Web Based User Interface for Encrypted Communication & Authentication Between FortiAnalyzer Server and FortiGate Devices
Mail Server Alert Output
Connect / Sync FortiAnalyzer SNMP Traps
Syslog Server Support
RAID Configurations, Change / View RAID Level
Support For Network Attached Storage (NAS)
Launch Management Modules
Launch Administration Console
Configure Basic System Settings
Online Help
Add/Change/Delete a FortiGate Device
View Device Groups
View Blocked Devices
View Alerts / Alert Events
Alert Message Console
View FortiManager Connection Status
View System Information / Resources
View Statistics
View Operational History
View Session Information
Backup / Restore
Restore Factory Default System Settings
Format Log Disks
Migrate data from FortiAnalyzer to another
Per-ADOM Dashboard

DLP Archive / Data Mining

All Functions of Log Analysis & Reporting with additional tools to detect and analyze data losses
View by Traffic Type
View Content including: HTTP (Web URLs), FTP (Filenames), Email (Text), and Instant Messaging (Text)
View Security Event Summaries
View Traffic Summaries
View Top Traffic Producers

Network Analyzer

Real-Time Traffic Viewer
Historical Traffic Viewer
Customizable Traffic Analyzer Log
Search Network Traffic Logs

Log Analysis & Reporting

View/Search/Manage Logs
Automatic Log Watch
Profile-Based Reporting
Over 450 Predefined Reports plus customization
Example Reports Include:

- Viruses: Top Viruses Detected, Viruses Detected by Protocol
- Events: By Firewall, Overall Events Triggered, Security Events Triggered, & Events Triggered by Day of Week
- Mail Usage: Top Mail Users by Inbound and Outbound Web Usage Reports
- Web Usage: Top Web Users, Top Blocked Sites, and Top Client, Attempts to Blocked Sites
- Bandwidth Usage: Top Bandwidth Users, Bandwidth by Day and by Hour, and Bandwidth Usage by Protocol Family
- Protocols: Top Protocols Used, Top FTP Users, & Top Telnet Users
- Wan-Opt log information

Log Aggregation to Centralized FortiAnalyzer
FortiClient Specific Reports
SQL Database Integration
SQL support for all features – including alerts, dashboard widgets, log viewer, FortiClient, and FortiMail
SQL Query / Schema tools

Central Quarantine

Configure Quarantine Settings
View Quarantined Files List
Quarantine Release API
Quarantine Summary by type of file, reason it was detected, first and last detected times, total unique quarantine files, and total number of detections for each type and reason

Forensic Analysis

E-Discovery
Track User Activities by Username, Email Address, or IM Name
Supports FortiGuard Web Filtering Reports to Show Web Site Access And Blocked Web Sites Per User
Configurable Report Parameters including: Profiles, Devices, Scope, Types, Format, Schedule and Output
Customized Report Output
Reports on Demand
Report Browsing

Log Browser And Real-Time Log Viewer

Web 2.0 Style, Real-Time Log Viewer
Historical & Custom Log Views
Log Filtering, Search, and Rolling
View Web, Email and/or FTP Traffic
View Instant Messaging and P2P Traffic
Filter Traffic Summaries
Device Summary
Traffic Reports including: Event (Admin Auditing), Viruses Detected, Attack (IPS Attacks), Web Content Filtering, Email Filtering, Content (Web, Email, IM)

Graphic Reporting

FortiAnalyzer systems empower the network or security administrator with the knowledge needed to secure their networks through a comprehensive suite of standard graphical reports and the total flexibility to customize custom reports. Network knowledge can be archived, filtered and mined for compliance or historical analysis purposes.

Granular Information

The FortiAnalyzer User Interface (UI) enables administrators to drill deep within security log data to provide the granular level of reporting necessary to understand what is happening on your network. Historical or real-time views allow administrators to analyze log and content information, as well as network traffic. The advanced forensic analysis tools allow the administrator to track user activities to the content level.

Real-Time Log Viewer

The ability to monitor network, traffic and user events in real-time or browse historical data for specific events provides powerful insight into network security threats, performance and user behavior.

Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiWeb Web Application Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device