PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

"ANÁLISIS Y DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED PERIMETRAL EN LA EMPRESA ASEGURADORA DEL SUR - MATRIZ"

NOMBRE:

MARGARITA ALEJANDRA BONILLA CONSTANTE

DIRECTOR:

MBA. ING. EDISON MORA

QUITO, MARZO 2016

DEDICATORIA

El presente trabajo de disertación dedico a mi Dios por darme la fortaleza y guiar mi camino a diario, para no desmayar ante problemas y adversidades, encarándolos como una guerrera.

Dedico también a la mejor maestra, amiga, compañera, confidente que puedo tener, por todas sus enseñanzas, mimos, regaños, consejos, amor y esfuerzos que día tras día lo hace por mí, ella es mi muñequita morena.

A mis abuelitos pieza fundamental para mi crecimiento personal y profesional.

A mi Andresito, mi compañero de vida y de clases, mi mejor amigo, por toda su paciencia, ayuda incondicional y por cada locura vivida en la Universidad junto con nuestros grandes amigos.

AGRADECIMIENTOS

Agradezco a mis profesores Ingenieros que más que maestros son amigos por todas las enseñanzas impartidas y por sus consejos durante mi carrera universitaria.

Quiero ofrecer un agradecimiento profundo a todas las personas que estuvieron y están conmigo desde muy pequeña a mi madre, abuelitos, amigos y toda mi familia en general

TABLA DE CONTENIDOS

Contenido

CAPITULO I

1.1. INTRODUCCIÓN

El desarrollo tecnológico, el nivel de competitividad de las compañías, las estrategias de negocios electrónicos y el mercado en general hace que las redes de datos estén expuestas a varios peligros tales como intentos de accesos no autorizados, ataques internos y externos a información confidencial de la compañía, entre otros, siendo esto una gran amenaza que podría afectar parcialmente o completamente a una compañía con la pérdida o modificación de información, perdiendo el nivel de confiabilidad de las redes de datos dentro de las organizaciones y por consecuencia también tendrá repercusión en los resultados y productividad del negocio.

Para sobrellevar el problema de pérdida de información y ataques informáticos en las organizaciones se ha desarrollado un proceso para asegurar las redes de datos que es la seguridad informática, la cual, ayuda a resguardar o proteger la información ante ataques, que cualquier individuo o grupo pueda realizarlo de una manera malintencionada.

La seguridad informática comienza a tomar forma en los años 60´s cuando se empieza a intervenir ilegalmente a los sistemas telefónicos, 20 años más tarde se contaba con un gran número de "*piratas informáticos"* y junto con

ellos aparecen los primeros virus[1] de computadoras, que rápidamente se esparcieron alrededor del mundo, al igual que correos spam, troyanos y gusanos, para 1991 se detectó más de 1000.

En el año de 1999 con el "boom" del Internet, surge el comercio electrónico, donde Amazon, e-Bay, se posicionan en el mercado y varias empresas comienzan a construir su negocio en la web, donde también el *First Internet Bank of Indiana* lanzó por primera vez servicios virtuales, mientras tanto los ataques a sitios web se seguían incrementando exponencialmente debido a la vulnerabilidad en el Internet.

La seguridad informática se encarga de proteger y resguardar toda la información, generada, procesada y transportada a través de los sistemas y equipos.

El objetivo de la seguridad informática es proteger la integridad, autenticidad y confidencialidad de la información y de los sistemas informáticos de una organización de tal manera que los recursos tecnológicos, sean totalmente íntegros y fiables.

La seguridad perimetral es muy importante dentro de una red de datos la cual es la encargada de proteger el perímetro o límites de una red de amenazas externas fortaleciendo a la red como una "muralla de un castillo", con esto se evita que amenazas externas accedan al espacio considerado como privado dentro de una red definida. Uno de los principios de la seguridad perimetral es que toda información que viaja por la red es sospechosa.

[1] Virus: tiene por objetivo alterar el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

La seguridad perimetral ha tenido un desarrollo considerable por lo cual hoy en día implementarla no es tan sencillo, debido a que en la red empresarial no solo se necesita tener conectados a los usuarios en una red de la organización internamente sino desde cualquier parte del mundo.

En las organizaciones a pesar de que se trata de proteger la información de la mejor manera, aún se evidencia que las seguridades se implementan con carácter reactivo y no preventivo, es decir, se corrige el problema cuando éste ya ha ocurrido, para ello se plantea realizar el **Análisis y diseño de un sistema de seguridad de red perimetral en la empresa Aseguradora del Sur - Matriz,** considerando como un factor crítico incrementar la seguridad para proteger la información importante de la Institución.

1.2. JUSTIFICACIÓN E IMPORTANCIA

En el Ecuador se ha venido impulsando proyectos para incrementar la seguridad de datos, principalmente en datos que se encuentran en el gran mundo del Internet, como por ejemplo datos bancarios, que se considera un sector sensible y vulnerable a ataques. En los años 80 aparecen los primeros cajeros automáticos, en 1995 los bancos comenzaron a sufrir clonaciones de tarjetas de crédito por lo cual se obligó a los bancos mejorar el sistema de seguridad, sin embargo en el año 1996 lanzan a la web sus servicios de banca electrónica, por lo cual llegan a ser más vulnerables a ataques, a partir de ahí se buscó implementar sistemas de seguridad que puedan proteger los servicios bancarios como firewalls, filtros de spam para servicios de correo, seguridad perimetral, entre otras.

La seguridad perimetral en una red de datos es de vital importancia para proteger la integridad, confidencialidad, disponibilidad y autenticidad de la información, si no se aplicara normas de seguridad en el perímetro de la red existirá un riesgo que cualquier momento podría ser aprovechado y podría generar consecuencias y pérdidas muy graves para una empresa.

Es importante conocer a fondo todo el esquema de la red de datos y sus componentes, a partir de lo cual se deberá implementar las condiciones necesarias para bloquear o filtrar los accesos desde redes externas a la red interna o privada, llevando esto a un esquema de seguridad perimetral que deberá ser bien elaborado y analizado, evitando que la compañía se encuentre expuesta a vulnerabilidades logrando tener una red eficiente y segura para las operaciones normales dentro de una empresa.

Para Aseguradora del Sur, una empresa que brinda servicios de seguros y maneja información sensible y confidencial, es prioritario implantar una herramienta de seguridad que garantice el rendimiento, disponibilidad y escalabilidad de su red (seguridad), actualmente en Aseguradora del Sur, existen ciertos puntos de control pero no valoraciones previas que justifiquen dichos puntos, son solo controles implementados esporádicamente, es decir para tener un control de la seguridad e integridad de la información se utiliza Firewall lógico dentro de la red de datos, sin embargo se ha tenido varios inconvenientes y ataques de malware, correos spam, software malicioso, pudiendo perder mucha información importante, sensible e indispensable para el funcionamiento

de la compañía, como base de datos de clientes, base de datos activos, documentación de proyectos, documentos financieros, documentos contables, pólizas, etc.

Además, una de las razones principales para implementar un sistema de seguridad perimetral es que cuenta con aplicaciones web que maneja el **Core** del negocio, transacciones en línea, lo cual es fundamental tenerlo resguardado.

Según lo dicho anteriormente, Aseguradora del sur encontró la necesidad de implementar un departamento de riesgos y seguridad de la información los cuales vieron que el enfoque tradicional que consistía en implementar únicamente firewalls y soluciones de virus ya no es suficiente, adquiriendo la necesidad de implementar un sistema de seguridad perimetral para resguardar su información y evitar actuales y futuros ataques, de ahí nace la importancia y la justificación del presente proyecto de disertación de grado.

1.3. DEFINICIÓN DEL TEMA

"ANÁLISIS Y DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED PERIMETRAL EN ASEGURADORA DEL SUR - MATRIZ"

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

- Analizar y diseñar un sistema de seguridad de red perimetral para la Aseguradora del Sur - Matriz.

1.4.2. OBJETIVOS ESPECÍFICOS

- Investigar y conocer sobre el funcionamiento de las redes de seguridad perimetral y la tecnología de seguridad.
- Analizar el riesgo actual de la red de datos de la Aseguradora del Sur - Matriz.
- Analizar y definir las necesidades de seguridad perimetral, en base a los resultados obtenidos del análisis de riesgo actual.
- Analizar y comparar tipos de hardware y herramientas a utilizar en el diseño de un sistema de seguridad perimetral para la Aseguradora del Sur - Matriz.
- Diseñar el esquema de seguridad definiendo dispositivos de seguridad a utilizarse usando la información del análisis previo sobre las necesidades de seguridad perimetral para la red.
- Describir las conclusiones y recomendaciones.

1.5. TECNOLOGÍA DE SEGURIDAD

Antiguamente se pensaba que la seguridad de la información era un tema que solo se escuchaba en las grandes empresas debido a su alto costo de adquisición o que tan solo estaba a cargo del departamento de TI (Tecnologías de la Información), sin embargo la seguridad de la información es una solución integrada que combina procesos, estrategias, recursos humanos y tecnología, de ahí la importancia de contar con políticas, reglas y responsabilidades acerca de la seguridad de la información, logrando el equilibrio entre la protección y habilitación de acceso a los activos de información.

La manera más efectiva para asegurar un enlace de Internet es poner un firewall entre la red local y el Internet.

Un firewall es un sistema diseñado para prevenir accesos desautorizados a una red privada, es decir, actúan como puertas de seguridad entre las redes internas y externas, dando permisos de autorización o desautorización a paquetes que ingresen a la red.

Desde los primeros Firewalls que se limitan hacer filtrado de paquetes, la tecnología de la seguridad ha evolucionado notablemente, en la actualidad existe una gran cantidad de soluciones al alcance de todos y para implementarlo es muy importante hacer un estudio detenido y adecuado para implementar una solución que esté acorde con el giro del negocio.

1.5.1. STATEFUL INSPECTION

Es una arquitectura de firewall que trabaja en la capa de red(capa 3) del modelo OSI[2], a diferencia de las primeras herramientas de filtrado de paquetes que examina únicamente paquetes de red que se basa en la información contenida en las cabeceras de cada paquete, el *Stateful Inspection* analiza el tráfico, es decir se encarga de analizar o examinar potentemente cada paquete que ingresa a la red, estos paquetes son interceptados en la capa de red, no dejándolos pasar a menos que cumplan con las políticas de seguridad de la red.

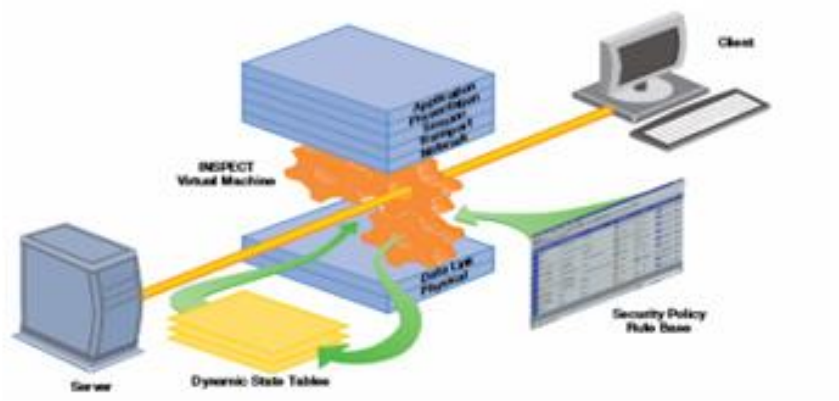


Gráfico1: Statefull Inspection.

Fuente: http://www.hacktimes.com/todo_sobre_checkpoint_fw-1/

[2] Modelo OSI: con sus siglas en ingles Open System Interconenction, es un modelo de referencia con su arquitectura en capas, para los protocolos de red, cuenta con 7 niveles.

1.5.2. DEEP PACKET INSPECTION

El Deep Packet Inspection (Inspección profunda de paquetes), también llamada Complete Packet Inspection (Inspección completa de paquetes), identifica de forma completa situaciones dentro de la red como la falta de cumplimiento de protocolos y todo paquete que tenga comunicación en la misma, el DPI analiza los encabezados y la carga útil de los mismos de esta forma ayuda a equilibrar el paso de tráfico en la red, siendo herramienta fundamental para la administración del ancho de la banda, sistemas de contenido caché, troubleshooting[3] de red, colabora con la clasificación del tráfico de acuerdo a la aplicación que esté siendo establecida, también decide el paso o no de paquetes, a diferencia del Stateful Inspection que solo detecta el encabezado del paquetes, siendo no tan confiable dado a que muchas aplicaciones usan puertos dinámicos o reutilizan puertos que anteriormente eran utilizado por otras aplicaciones para evitar ser detectados.

Es importante tomar en cuenta que el equipo que realice la inspección no debe ser uno que contenga un punto final antes de ingresar a la red.

[3] Troubleshooting: solución de problemas

CAPITULO II: SEGURIDAD PERIMETRAL

2.1. DEFINICIONES

2.1.1. Seguridad

2.1.1.1. Concepto Seguridad de la Información

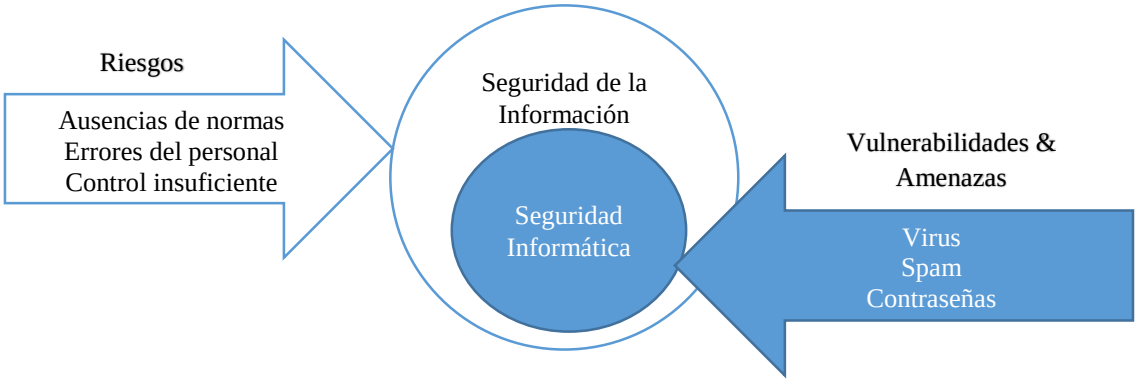
En el capítulo I se habló que la información es un activo muy valioso para impulsar o destruir una empresa, a primera vista se puede decir que **Seguridad de la información y Seguridad informática** pueden parecer exactamente lo mismo, sin embargo, es importante diferenciar estos dos conceptos.

Cuando se habla de Seguridad de la Información se indica que dicha información es muy valiosa y se debe proteger, conociendo, gestionando y minimizando los riesgos o amenazas, con mecanismos o conjuntos de medidas técnicas destinadas a la integridad, confidencialidad y disponibilidad de la información, trazando planes de acción apoyándose en la Seguridad Informática y políticas o normativas de Seguridad de esta manera se protege la información de una organización, independientemente del lugar en que se encuentre, papel, discos duros, memorias portables o medios digitales.

Integridad: Asegura que la información es completa, no modificada y completa, se conoce el autor.

Confidencialidad: Asegura que a la información solo tiene acceso quien esté autorizado debiendo ser legibles y modificables.

Disponibilidad: Asegura que la información siempre sea accesible en un momento necesario.



2.1.1.2. Concepto Seguridad Informática

La seguridad informática se encarga de implementar técnicas de protección, es decir, se refiere a la protección de infraestructuras de las tecnologías de la información y comunicación que soportan la operación de una organización, centrándose en hardware y software, como son antivirus, firewalls, detección de intrusos, entre otros elementos, además, de los enfoques técnicos los especialista en seguridad se manejan con las vulnerabilidades y con amenazas bajo la forma de ataques, para poder mitigar los riesgos, teniendo en cuenta políticas de seguridad para poder

analizar y diseñar posibles responsabilidades y reglas para evitar amenazas o minimizar los efectos.

2.1.2. Amenazas Informáticas

Se define a amenaza a todo elemento o acción que sea capaz de atentar a la seguridad informática, que surgen a partir de la existencia de vulnerabilidades.

La seguridad informática se hizo presente en los años 80's debido que se tenía la necesidad de evitar o contrarrestar los ataques informáticos, y gracias a la utilización del Internet los riesgos y amenazas fueron mayores, afectando a varias empresas y usuarios de la red, ya que la inexistencia de restricciones en el Internet provocó que los virus, troyanos y otros códigos maliciosos se propaguen a través de correos electrónicos, publicidad o páginas web, de esta manera ayuda a que los ataques tomen el control o la información de la empresa o usuario para causar daño.

Basta con ver las estadísticas sobre amenazas informáticas en el año 2014 para darse cuenta de cuan expuestos estamos a ataques en la red, según ESET Security, en Latino América cerca del 70% de las empresas tienen incidentes más recurrentes con accesos indebidos, infecciones de malware y ataques de negación de servicios DoS[4], sin importar el tamaño

[4] DoS(Denial of Service): tiene como objetivo imposibilitar el acceso a los servicios y recursos de un usuario u organización conectados a Internet, por un tiempo indefinido.

de la organización el ciberdelincuente solo le interesa obtener algún tipo de ganancia económica.

En el gráfico 2 podemos observar que casi el 20% de las empresas grandes sufrieron de *fishing* perdiendo información que manejan los empleados y datos sensibles para la empresa.

En el informe emitido por Symantec en la cumbre de la "Organización de los Estados Americanos, en Tendencias de seguridad cibernética en América Latina y el Caribe", publicado en junio del 2014, se estima que en el año pasado se tuvo una suma de USD 113.000 millones en delitos cibernéticos, teniendo a Brasil como el país más atacado por motivos de la copa del mundo, con una cantidad de USD 8.000 millones, seguido por México con USD 3.000 millones y Colombia con USD 464 millones y esto se debe a que los usuarios finales aún tienen una actitud desinteresada cuando se trata de cuidar de su información, y con la adopción de las redes sociales, smartphones, dan mayores oportunidades a los ciberdelincuentes aumentando las estafas a nivel mundial.

En Ecuador se tiene un gran porcentaje de ataques por malware o códigos maliciosos, como indica el gráfico 2, después de Venezuela y Colombia, entre 2008 - 2014 aumentó exponencialmente la cantidad de ataques en

un 203% y 458% respectivamente, donde la mayoría de los ataques, casi el 80%, fueron de skimming[5] y fishing[6].

Si bien es cierto Ecuador no tiene ninguna agencia que estén designado a ser responsable de la seguridad cibernética, una gran cantidad de autoridades como la SENAIN (Secretaria de Inteligencia), mediante su Subsecretaria de Contrainteligencia e Incomunicaciones y El Centro de Operaciones Tecnológicas Estratégicas, implementan medidas de seguridad dentro de las entidades gubernamentales centrales, así como la Superintendencia de Telecomunicaciones es responsable de la formación y posterior operación de un CSIRT nacional, cuyo nombre tentativo es EcuCERT que es tener un plan de respuesta ante emergencias informáticas, sin embargo la responsabilidad principal en la investigación de la ciberdelincuencia y las actividades criminales que involucren a las TIC recae sobre la Unidad de Investigación del Delito Cibernético de la Policía Judicial. El Ecuador ha identificado dos impedimentos que no ayudan a reducir la ciberdelincuencia, el primero se debe a la falta de leyes sobre ciberdelincuencia, y la segunda la falta de conciencia y de recursos educativos para ciudadanos del uso responsable del Internet, redes sociales, correo electrónico y las TIC.

[5] Skimming: Clonación de tarjetas
[6] Fishing: Suplantación de identidad, utiliza ingeniería social.

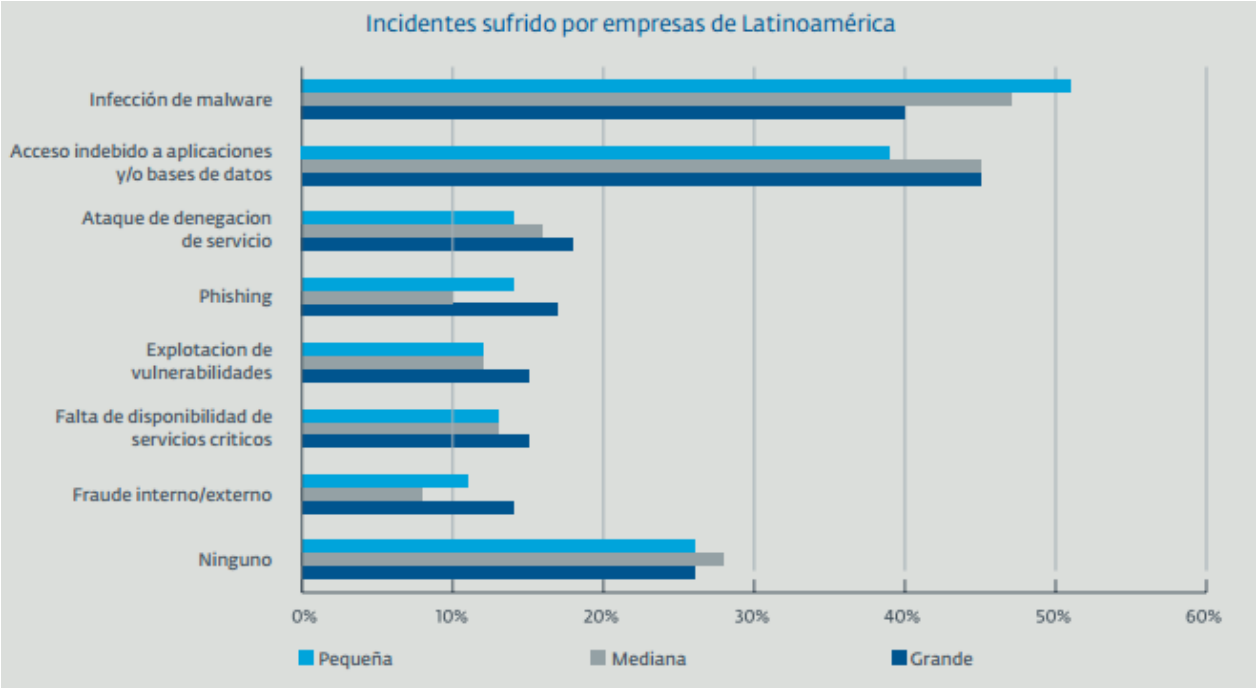


Gráfico 2. Incidentes sufridos en empresas de Latino América. Fuente ESET

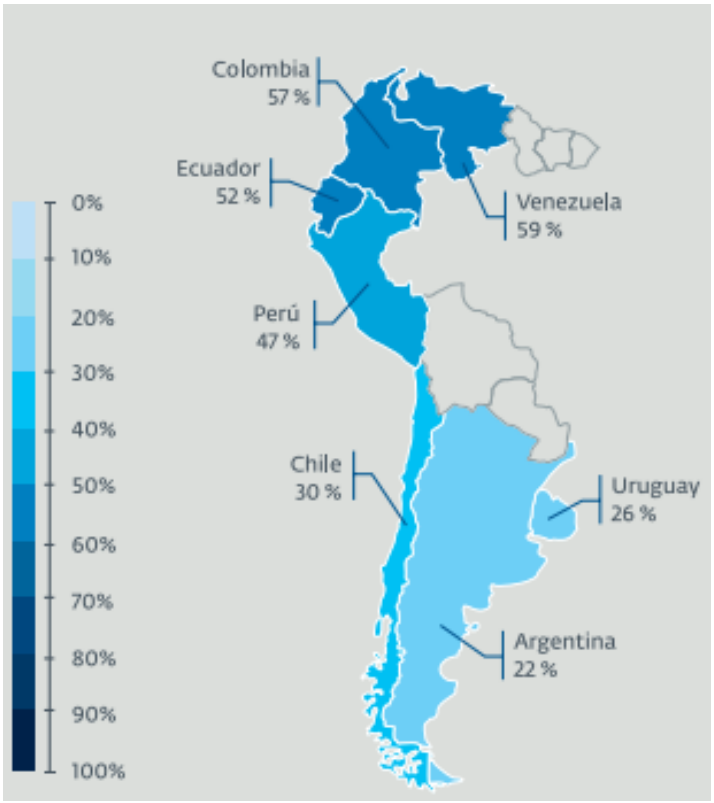


Gráfico 3. Infecciones con malware o código malicioso por país. Fuente ESET

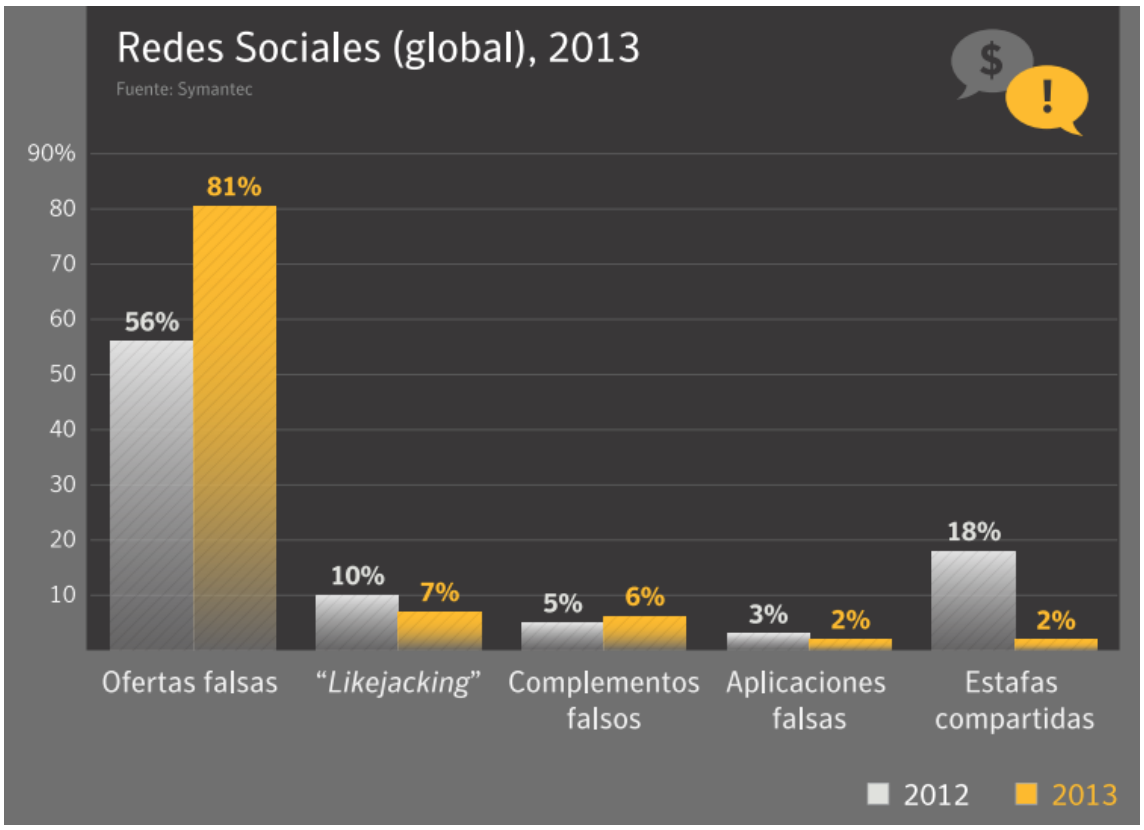


Gráfico 4. Redes Sociales generan estafas y malware en dispositivos móviles.

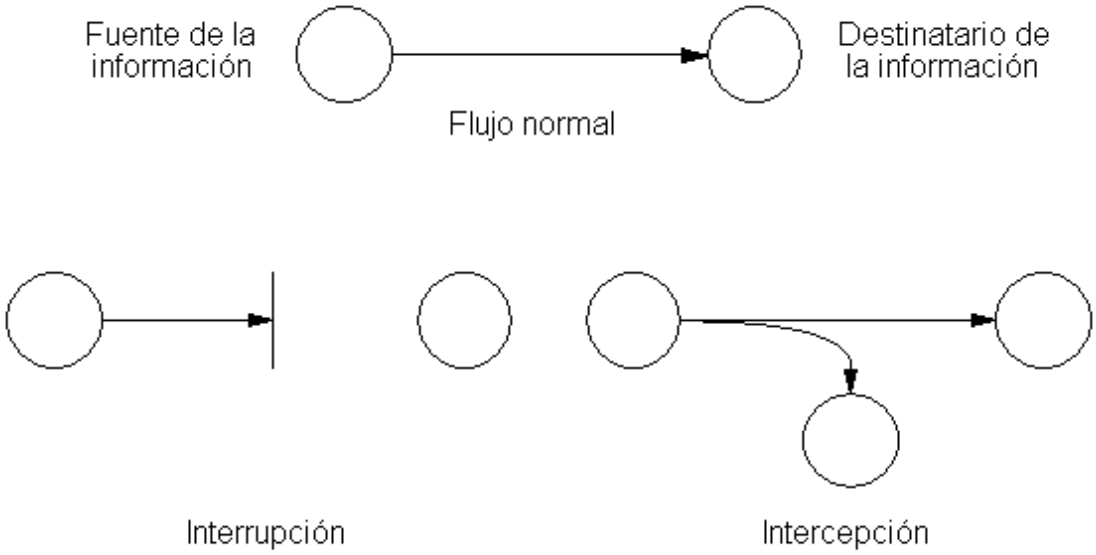
Fuente: Symantec

2.1.2.1. Tipos de ataques informáticos

Se puede definir como ataques a todas las amenazas o acciones que suponen una violación de seguridad de una red que afecta la confidencialidad, integridad o disponibilidad de la información.

Estas acciones se pueden clasificar de varios modos según los efectos causados:

- **Intercepción:** Cuando una persona, un programa o un equipo no autorizado consigue acceso a un recurso y desvía la información a otro punto que no sea el destinatario original, perdiendo confidencialidad de la información.
- **Interrupción:** Un recurso del sistema es destruido o no se encuentra disponible, ataca la disponibilidad de la información, como el ataque de denegación de servicios.
- **Modificación:** Cuando una entidad no autorizada consigue acceder a algún tipo de información, a un sistema o base de datos y es capaz de modificarlo y manipularlo.
- **Fabricación:** Cuando una entidad no autorizada inserta objetos falsos en el sistema, ataca la autenticidad, por ejemplo fishing.



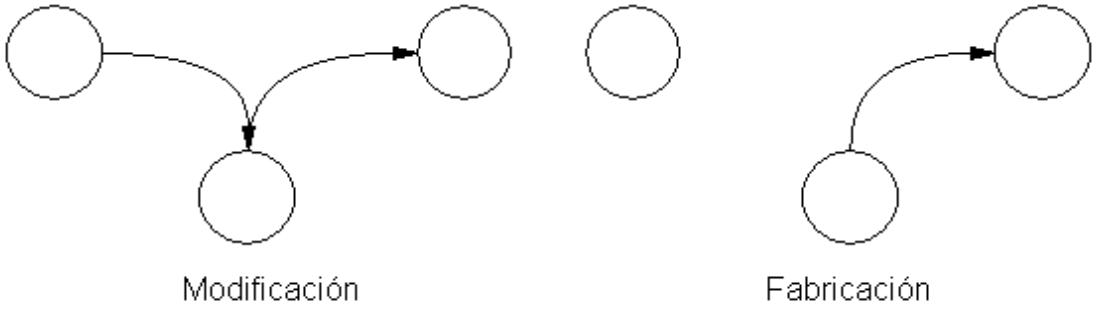


Gráfico 5. Clasificación de ataques en la red. Fuente: Stamp

2.1.2.1.1. Factor Humano

Según la experta en código malicioso y musa de la comunidad informática Joanna Rutkowska de nacionalidad polaca, “La mayoría de ataques explotan el factor humano, esto se debe a la ignorancia del usuario”.

Si bien las empresas de seguridad informática se dedican a tratar de reducir la posibilidad de ser víctimas de ataques, el factor humano es un centro de vulnerabilidades para los ciberdelincuentes, es decir, a pesar de que se ha tratado de minimizar la exposición a las amenazas cibernéticas, existen brechas para los ataques y es un error humano, que no siempre se relaciona con malas intenciones por parte de los usuarios, sino con la falta de información y capacitación sobre temas de seguridad de la información.

Hoy en día la ingeniería social juega un papel importante en cuanto a ataques se refiere, los usuarios finales normalmente caen en este tipo de ataques, ya que es normal ver como ellos utilizan sus smartphones, tablets u otros

dispositivos para acceder a sus cuentas bancarias, redes sociales, correo electrónico, sin ninguna política de seguridad o en redes que posiblemente sean pocas seguras.

En 2013 la DBIR (Data Breach Investigations Report), muestra que los ciberdelincuentes toman al factor humano como el mayor porcentaje de vulnerabilidad atacándolos por medio de ingeniería social, fishing, likejacking[7], que son diseñados para robar credenciales o información personal de los usuarios, la DBIR concluye que 4 de cada 5 incidentes reportados, se utilizó credenciales robadas, tanto en empresas, entidades gubernamentales o en usuarios finales.

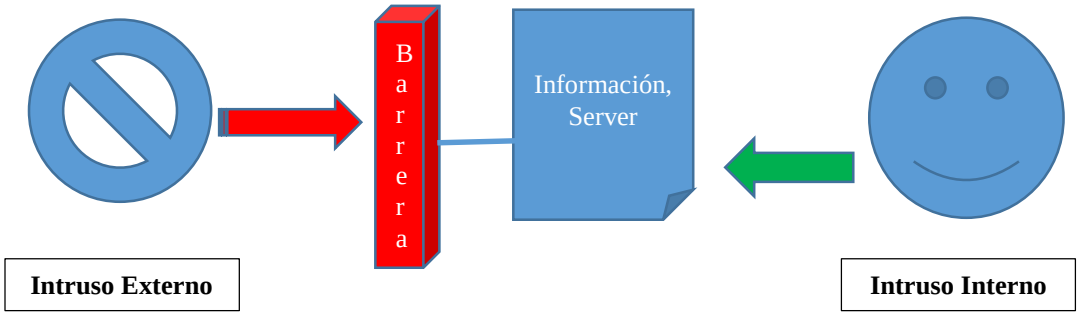
2.1.2.1.2. Ataques internos

Estos ataques son iniciados por individuos o grupos de colaboradores de una empresa que conocen el negocio y tienen accesos autorizados a la red interna o incluso a cualquier Server que quiera atacar, son los más comunes y los más peligrosos.

[7] Likejacking o clickjacking es una amenaza que desde la interfaz de Facebook re direcciona a otras páginas de phishing.

2.1.2.1.3. Ataques externos

Son iniciados desde fuera de la compañía, no tienen un acceso autorizado a la red, siendo más fáciles de detectar y mitigarlos que los ataques internos, su origen es por el Internet, redes de proveedores, accesos remotos.



La red de la Aseguradora del Sur está expuesta a todos estos tipos de ataques, tanto externos como internos y por ser una compañía que se dedica a la venta de seguros y maneja un constante movimiento económico, al no contar con políticas y normas de seguridad de la información es muy vulnerable a ataques, ya que los propios colaboradores pueden acceder a la información sensible y compartirla, además no se puede dejar de lado el factor humano que muchas veces por falta de conocimiento de seguridad muchos colaboradores han infectado sus máquinas, smartphones, tablets o han sido víctimas de la ingeniería social, siendo una amenaza para toda la red interna dentro de la Aseguradora del Sur a nivel nacional.

2.2. CONCEPTO DE SEGURIDAD PERIMETRAL

Teniendo en cuenta que la seguridad y la integridad de la información son primordiales para el funcionamiento de una empresa, y que los ataques y amenazas crecen constantemente ocasionando trastornos económicos, mala imagen, funcionamiento y progreso para la empresa, nace la seguridad perimetral que es una plataforma robusta para controlar el acceso y protección de los servicios informáticos.

La seguridad perimetral no es una tecnología, sino se considera un sistema que se compone de varios elementos de tecnología, de hardware y de software, que actúan de manera conjunta con el fin de vigilar y proteger el perímetro o “borde”, aísla a la red de entradas externas (Internet) o amenazas, defendiendo, al estilo de estrategias militares, un perímetro de seguridad se utiliza mediante el uso de equipamiento especifico configurado para realizar filtros de paquetes de datos, controla todo acceso a la red interna de la empresa.

Se debe tomar en cuenta que la seguridad perimetral es una realización práctica de políticas de seguridad implementadas, sin estos, la seguridad perimetral no sirve de nada.

Gráfico 6. Seguridad Perimetral.

Fuente: http://www.irt.com.mx/servicios.html

2.2.1. Objetivo de la Seguridad Perimetral

Los objetivos de la seguridad perimetral son:

- Controlar el tráfico de red desde y hacia Internet (Firewall).
- Proteger a la red privada contra ataques externos.
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde el Internet.
- Auditar el tráfico entre el exterior y el interior.
- Tomar acciones ante cualquier amenaza antes de que acceda a la red privada.

2.2.2. Componentes de la Seguridad Perimetral

2.2.2.1. Router de Perímetro

Los ruteadores de perímetro también se los conocen como ruteadores de frontera o límite, son aquellos que se encuentran situados entre la red interna y las redes no confiables (el Internet), encargándose de enviar los paquetes de una red confiable a redes no confiables que se encuentren fuera de una organización dirigiendo el tráfico de paquetes de un lado a otro, es por eso que se lo utiliza como un primer y último filtro, siendo críticos para la defensa de nuestra red.

2.2.2.2. Firewalls

Los Firewalls o cortafuegos son una herramienta básica de la seguridad informática, asemejándose a un estilo de muralla, imponiendo una barrera entre un ambiente seguro y un ambiente externo, como el Internet, permitiendo controlar las conexiones de la red tanto a computadoras individuales como a redes empresariales, de intrusos o amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información o denegando los servicios, es decir, el firewall permite el paso y el flujo de datos entre puertos, ya sean clientes o servidores, estableciendo reglas.

El firewall se encuentra en la puerta de enlace entre las dos redes por general una red privada y una red pública, se puede tener varios firewalls en una red privada de esta manera se tiene una mayor seguridad en la red.

Existen varios tipos de filtrados como son, filtro de direcciones, los cortafuegos pueden filtrar paquetes en función de su origen, destino o número de puerto.

También puede filtrar determinados tipos de tráfico de red, permitiendo o rechazando dependiendo del protocolo, utilizado ya sea HTTP[8], TELNET[9], FTP[10], SMTP[11], entre otros, a este filtrado se lo conoce como Protocolo de filtrado.

Un firewall trabaja de dos maneras para denegar accesos, la primera permitiendo todo el tráfico enviado en la red a menos de que cumplan con ciertos criterios o reglas que se establezcan previamente, o se puede denegar todo el tráfico que pase por la red a menos de que cumplan con ciertos criterios o reglas que se establezcan previamente, siendo este último un poco más seguro y eficiente.

[8] HTTP, es un protocolo de transferencia de hipertextos, que utiliza muchas direcciones de internet.
[9] TELNET, es un protocolo de red que nos permite viajar de una maquina a otra para manipularla remotamente.
[10] FTP, es un protocolo de red de transferencia de archivos, entre sistemas conectados a una red TCP.
[11] SMTP, es un protocolo de red que se emplea para enviar y recibir correos electrónicos.

Se debe tomar en cuenta que un firewall no puede evitar la mala conducta de los empleados o de los usuarios, es decir, no se puede ir en contra del factor humano o las políticas ineficientes que se empleen dentro de la compañía, para proteger la integridad de la información.

Existen varias generaciones de Firewalls, desde la generación primera hasta la actualidad que se encuentra la generación quinta, llamada también, Next-Generation Firewall (NGFW), que es el auge en Seguridad perimetral firewall por sus grandes beneficios, como son el control de accesos, control de aplicaciones, filtrado web, entre otros.

2.2.2.3. De NAT (Network address translation)

Con el crecimiento exponencial del número de usuarios que utilizan el Internet, es necesario buscar una solución para no saturar las IP's públicas disponibles en versión IP v4, es por eso que nace el concepto de NAT (Network address translation) o traducido al español Traducción de direcciones de Red, es el proceso donde se utiliza una conexión de pasarela a Internet, que tenga al menos una interfaz de red conectada a la red interna y una a la red externa, realiza un mecanismo de conversión de direcciones IP para poder establecer una comunicación entre ellas. Se puede tener dos tipos de conversiones:

- **Conversión dinámica:** permite que diversos equipos con direcciones privadas compartan una dirección IP enrutable.

- **Conversión estática:** consiste en vincular una dirección IP pública con una dirección IP interna privada en la red.

2.2.2.4. IDS (Intrusion detection system)

Los IDS (Intrusion detection system) o en español Sistema de detección de intrusos, trabaja sigilosamente escucha el tráfico que se encuentra en la red detecta actividades sospechosas, monitorea a una red completa o a un grupo específico de computadores buscando intentos de amenazas, es decir, cualquier intento de comprometer la confidencialidad, integridad y disponibilidad de la red, recoge evidencias que puedan servir al administrador de la red para identificar qué tipo y de donde provienen los intrusos, mostrando las vulnerabilidades en las que se debe trabajar.

Los IDS se pueden integrar con el Firewall formando una herramienta poderosa de seguridad y de bajo costo.

Sus principales funciones son:

✓ Identificación de posibles ataques.

✓ Registro de eventos.

✓ Reportar al administrador de la red de los posibles ataques.

Se tiene tres tipos de IDS:

a) **NIDS (Network Based IDS):** Es un IDS que se encarga de controlar el tráfico en busca de actividades sospechosas.

b) **HIDS (Host Bases IDS):** Es un IDS que protege a un solo equipo, monitoriza cambios en el sistema operativo y aplicaciones.

Métodos de detección:

a) **Detención basada en firmas:** Son modelos que se refiere a cómo los ataques son realizados y cómo pueden ser detenidos, cualquier acción que no sea reconocida como un ataque será considerado aceptable, es decir, este tipo de detección es débil contra nuevos ataques.

b) Detección basada en patrones de comportamiento: Se observa y detecta variaciones del comportamiento esperado por parte de los usuarios y los sistemas, detecta nuevos y desconocidas vulnerabilidades, sin embargo, pueden causar muchas falsas alarmas.

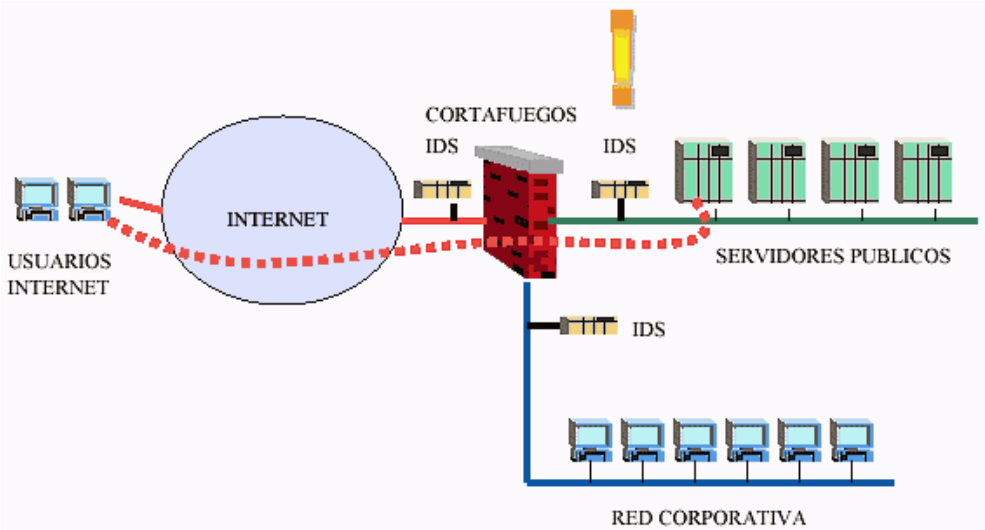


Gráfico 7. IDS.

Fuente: http://www.flu-project.com/2012/02/deteccion-de-intrusiones-en_22.html

2.2.2.5. IPS (Intrusion Prevention System)

El IPS (Intrusion Prevention System) o su nombre en español Sistema de prevención de intrusos, sirve para controlar el acceso de intrusos, transmisión de código malicioso o amenazas a través de la red, en contraposición con los IDS que se encarga de alertar al administrador sobre alguna actividad sospechosa, los IPS cuentan con políticas de seguridad establecidas que tienen la habilidad de bloquear inmediatamente las intrusiones sospechosas en la red, es decir, tiene un tipo de protección proactiva a diferencia de los IDS que son reactiva.

Métodos de detección:

- ✓ Detección basada en firmas.
- ✓ Detección basada en políticas.
- ✓ Detección basada en anomalías.
- ✓ Detección Honeypots[12]: se configura un equipo que sea atractivo para los hackers dejando evidencia de cómo se realizan sus ataques, para después implementar políticas de seguridad.

2.2.2.6. VPN (Virtual Private Network)

Una VPN con sus siglas en español Red Privada, es construida dentro de una infraestructura de red pública, que ayuda a las empresas a ampliar su

[12] Honeypot: Sistema configurado para recoger muestras de ataques y estudiar nuevas técnicas para contra atacar.

conectividad de forma segura, económica y mejora la velocidad de conexión entre ellas, de esta forma aseguran la integridad, autenticación y la confidencialidad de los paquetes. Una VPN permite a un usuario externo conectarse con la red privada aun sin que esté conectado físicamente, utiliza usuarios remotos.

Existen dos tipos de clasificación para las redes VPN:

a) **Sitio a Sitio:** establece la comunicación por medio de un túnel VPN de dos o más ubicaciones. Por ejemplo, Oficina Matriz con una sucursal.

b) **Acceso Remoto:** permite la conexión de usuarios remotos en ubicaciones fuera de la empresa, como, por ejemplo, la casa, el hotel, entre otras.

2.2.2.7. SSL VPN's (Security Socket Layer Virtual private network)

La VPN basada en SSL es una forma de acceder a una red privada por medio de un navegador de Internet, es decir, la SSL VPN no requiere una instalación previa en el computador, Tablet, smartphone del usuario final, tan solo para acceder es necesario tener un navegador web, ofreciendo una mayor versatilidad de conexión en cualquier plataforma en cualquier lugar, los paquetes enviados son encriptados por el protocolo SSL o TSL de esta manera asegura la seguridad de la integridad y autenticidad de los mismos.

2.2.2.8. DMZ (Zonas desmilitarizadas)

Las Zonas desmilitarizadas son un tipo de diseño en el cual los servidores que puedan comprometer a la integridad de la compañía al ser consumidos desde un acceso público se colocan en un segmento separado de la red, asegurándose que los servidores de acceso público no puedan comunicarse con otros segmentos de la red privada.

Utilizada para servicios públicos como pueden ser correos electrónicos, servidores ftp, entre otros.

Para implementar un DMZ es necesario contar con un firewall el cual proporcione de las políticas necesarias de seguridad para proteger las redes locales de una DMZ.

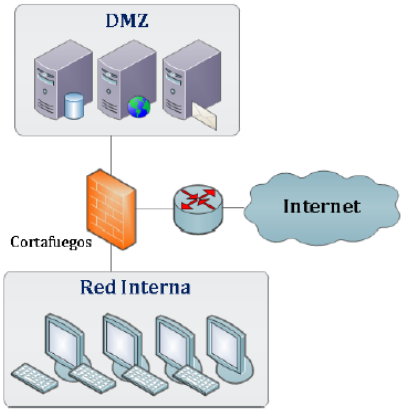


Gráfico 8. DMZ. Fuente: intypedia creative commons, Madrid, España 2011

2.2.2.9. Antivirus perimetral

Es un programa que detecta la presencia de virus informáticos, encontrando la traza de los programas maliciosos mientras el sistema se encuentre

funcionando eliminándolos o reparándolos, y notificando al usuario o administrador de posibles incidencias de seguridad.

Se puede tener antivirus personales o antivirus corporativos en el cual se puede administrar las reglas y políticas que se va a utilizar dentro de la compañía, como por ejemplo se puede bloquear el recibir .exe

Existen varios métodos de detección y tipos de vacunas:

- ✓ **Solo detección:** Son vacunas que tan solo detectan archivos infectados y no pueden eliminarlos o desinfectarlos
- ✓ **Detección y desinfección:** Detectan archivos infectados y pueden desinfectarlos.
- ✓ **Detección y aborde de la acción:** Detectan archivos infectados y detienen las acciones que causa el virus.
- ✓ **Comparación por firmas**: Compara las firmas de otros archivos sospechosos.
- ✓ **Invocado por el usuario:** Vacunas que son activadas manualmente por el usuario

2.2.2.10. Anti-spyware

Los Anti Spyware o anti espías es un conjunto de herramientas que ayuda a proteger la red o nuestro equipo evita anuncios emergentes o publicidad, rendimiento lento o cualquier amenaza de seguridad causadas por spyware, los cuales recopilan información como claves, correos electrónicos, dirección IP, páginas web frecuentes, cuentas de banco,

compras realizadas, claves de tarjetas de crédito sin el consentimiento del usuario que este ocupando el computador infectado.

2.2.2.11. Anti Bot

Un Bot es el diminutivo de (Robot), siendo este un programa malicioso que permite tomar el control del equipo infectado, siguiendo las órdenes de su "amo" volviendo a su víctima en un "zombie", todo el mundo puede ser víctima de este tipo de vulnerabilidad en la red, los ciberdelincuentes que controlan estos Bots son cada vez más numerosos, es por eso que aparecen los Anti Bots, los cuales son módulos muy ligeros que se encargan de la eliminación de Bots sin necesidad de la interacción de los usuarios finales, sus objetivos son:

- Impedir el envío de spams automáticas.
- Proteger la navegación sin dejar rastro o cache en las páginas.
- Evitar la denegación de servicios DoS
- Evitar que roben la información privada y personal del usuario
- Evitar los fraudes mediante Clics.
- Ser más fiables que una trampa honeypot.

2.2.2.12. Geo Protection

El Geo Protection es una función que permite a los administradores gestionar el tráfico en la red, es decir, monitorear, permitir y prevenir el tráfico desde el lugar de origen de origen o país de destino, tomando la dirección IP ayuda a supervisar o denegar accesos de trafico de red de países con

ubicaciones que no son de confianza (lista negra), como también permitiendo el tráfico para países que se encuentran en la lista de confianza (lista blanca).

2.2.2.13. Filtrados web y aplicaciones

Muchas veces el acceso a Internet hace que el ancho de banda sea mal utilizado, por múltiples razones que no se deberían usar en ambientes laborales, el filtrado web y de aplicaciones permite bloquear y administrar de mejor manera los recursos que brinda el Internet, limitando o bloqueando aplicaciones como redes sociales, mensajería, entre otros.

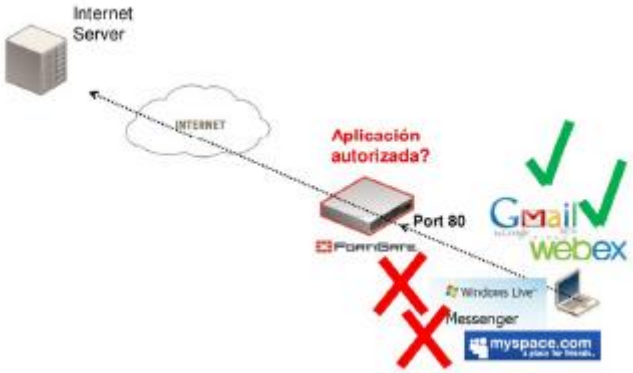


Gráfico 9. Control de Aplicaciones.

Fuente: http://www.solinfra.com/seguridades-informaticas/

2.2.2.14. Inspección https

El tráfico cifrado con el protocolo SSL que utiliza HTTPS, puede ser descifrada e inspeccionada por el IPS, el cual lo examina para descubrir malware o código malicioso, también puede limitar el acceso a algunas páginas web a los usuarios que no sean inherentes a la actividad de la empresa, inspecciona el tráfico HTTPS (puerto 443).

A la vez se puede tener varias formas de administrar la inspección https como por ejemplo se puede permitir el acceso a todas las paginas https sin necesidad de realizar una inspección previa, se puede validar todos los certificados de sitios HTTPS.

2.2.2.15. DLP (Data Loss Prevention)

La DLP con sus siglas en inglés (Data Loss Prevention) o Prevención de perdida de datos es un tema muy importante dentro de una empresa ya que no solo previene la perdida de datos, además la protege, es por eso que no se la debe ver como una opción sino como una iniciativa importante para proteger el activo más importante dentro de una empresa.

DLP es una estrategia para asegurar que los usuarios finales no envíen información crítica o sensible fuera de la red corporativa, utiliza reglas o políticas para clasificar la información confidencial, para que usuarios no autorizados, no puedan compartir de forma accidental o maliciosa datos cuya divulgación pudiera poner en riesgo a la empresa, como por ejemplo información financiera, datos de tarjetas corporativas, líneas del negocio, si se trata de enviar estos archivos que son propios del negocio fuera del dominio corporativo se negara el permiso.

2.2.2.16. WAF (Web Application Firewall)

WAF (Firewall de aplicaciones Web), es un dispositivo físico que analiza el tráfico web, entre el servidor web y WAN, que ofrece una protección contra ataques a las aplicaciones web, emite alertas y bloquea amenazas antes

de alcanzar los servidores de origen, filtra todo el tráfico HTTP y HTTPS de entrada, por medio de controles configurables en capas de red y aplicación.

Los parámetros de seguridad del WAF se basan en el ModSecurity que es un conjunto extremadamente confiable de reglas que detecta y previene técnicas de exploración comunes como SQL injection[13] y Cross Site Scripting[14].

Entre sus beneficios están:

- Aumenta la confiabilidad, integridad y disponibilidad del website.
- Reduce el tráfico de ataques y costos relacionados, como infraestructura, recursos operativos.
- Mitiga los riesgos de fishing.

Sin embargo, existen riegos al aplicar un sistema WAF ya que al no estar bien configurados se puede detectar muchos falsos positivos, denegando muchas transacciones y teniendo una pérdida de capital, por lo tanto, se puede tener clientes insatisfechos y jefes molestos.

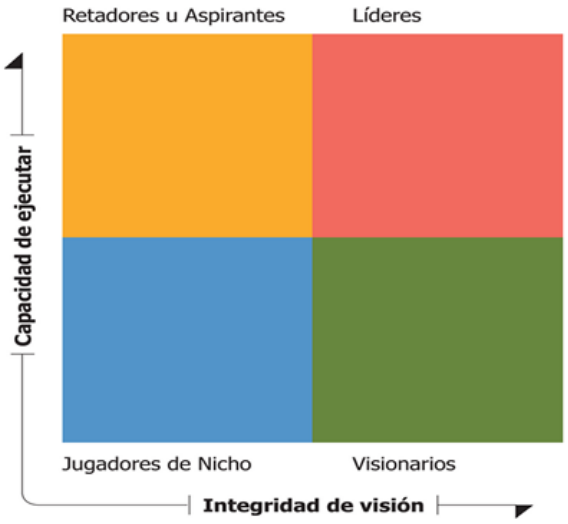
[13] SQL injection, es un método de infiltración de código malicioso que ataca una vulnerabilidad informática.
[14] Cross-Site scripting, agujero de vulnerabilidades muy común en aplicaciones web.

2.2.3. EQUIPOS DE SEGURIDAD PERIMETRAL

2.2.3.1. Cuadrante de Gartner

Gartner es una empresa dedicada a la consultoría, exclusivamente a investigar el sector tecnológico, analiza tendencias del mercado para poder elaborar un ranking de soluciones tecnológicas y productos.

En el desarrollo de proyectos de TI, se puede desplegar varias inquietudes, como saber cuál es la mejor opción en tecnología, producto o solución de diversos fabricantes, para ayudar a responder esas preguntas el Cuadrante mágico de Gartner es una representación gráfica de la situación del mercado de un producto, tecnología o solución en un determinado periodo de tiempo, el gráfico está dividido en cuatro partes, de ahí su denominación “cuadrantes mágicos”:



Leaders (líderes): Esta categoría es catalogada, como, la mejor. Si se está situado en este cuadrante significa haber tenido los mejores puntajes, teniendo por parte de los proveedores una solución tecnológica o producto, completa, amplia y madura.

Visionaries (Visionarios): En esta categoría se encuentran los proveedores que tienen una integridad de visión muy alta, sin embargo, en la capacidad de ejecución muy baja, es decir, entran proveedores que tienen una muy buena visión de alguna solución o producto tecnológico acorde con el mercado actual, pero no tienen la capacidad para implementar esas buenas ideas.

Challengers (Aspirantes): En este cuadrante los proveedores están bien posicionados y ofrecen altas posibilidades de éxito a la hora de implementar la solución, sin embargo, los proveedores suelen ofrecer poca variedad o muchas veces se centran en un único aspecto en la demanda del mercado.

Niche Players (Jugadores de Nicho): Son proveedores que no logran tener un buen puntaje para posicionarse en uno de los otros cuadrantes, sin embargo, no quiere decir que sus soluciones no tengan calidad.

El eje X del cuadrante de Gartner significa, el conocimiento de los proveedores sobre cómo se puede aprovechar el momento actual del mercado para generar valor a los clientes.

El eje Y del cuadrante de Gartner trata de medir las posibilidades de los proveedores para ejecutar con éxito sus visiones en el mercado, como por

ejemplo que tan rápido es su respuesta ante cambios de tendencias o actualizaciones.

En la Aseguradora del Sur, se va a implementar una solución tecnológica para resguardar la confiabilidad, integridad y fiabilidad de su información, por lo cual, el análisis y diseño de la solución que se realizará en el capítulo III y IV, se tomara como referencia la información entregada por el Cuadrante de Gartner de los mejores proveedores en seguridad perimetral o Firewalls, en abril 2015, como muestra el gráfico 10, los proveedores para la tecnología de seguridad que se encuentran en el cuadrante de líderes son Check Point Software Technologies y Palo Alto Networks, los cuales serán analizados sus ventajas y desventajas, para su posible implementación.

En conclusión, se debe tomar en cuenta que el Cuadrante de Gartner, es empleado, únicamente como una referencia, ya que las decisiones para adquirir una solución o algún producto tecnológico, se lo debe hacer de acuerdo a las necesidades del negocio, realizando varios análisis, por ejemplo, económicos, soporte, escalabilidad, rendimiento, facilidad de adquisición, entre otros.

Gráfico 10: Cuadrante de Gartnet Firewalls.

Fuente: Gartnet, Abril 2015.

2.2.3.2. Características de equipos

2.2.3.2.1. FIREWALL

Se toma en cuenta el Cuadrante de Gartnet y se selecciona dos marcas líderes en el mercado de Seguridad Perimetral, para realizar el análisis para una posible implementación.

Check Point Software Technologies: Es el indiscutible líder mundial en seguridad de perimetral y aseguramiento del Internet. Establecida en 1993 y desde entonces enfocada 100% a seguridad. En la actualidad cuenta

con decena de miles de clientes, entre los cuales se muestran las empresas más grandes y prestigiosas del mundo.

Palo Alto Networks, Inc: al igual que Check Point lidera el cuadrante de seguridad, con su innovadora plataforma que permite proteger las redes y habilitar de forma segura las aplicaciones que cada vez son más complejas.

Entre sus ofertas está el firewall de nueva generación que brinda visibilidad y control sobre las aplicaciones, usuarios y contenidos, que usa una arquitectura de hardware y software altamente optimizada.

Para dimensionar el equipo/modelo a utilizar en la posible implementación de seguridad perimetral, se realizó una entrevista al cliente y junto con la ayuda de un partner de las marcas ya antes nombradas, se realizó el análisis de vulnerabilidades dentro de Aseguradora del Sur y además se realizó las siguientes preguntas:

- ¿Con cuánto ancho de banda cuenta Aseguradora del Sur?
  - Cuenta con 26 MB
- ¿Cuál es el número de usuarios en la LAN?
  - Alrededor de 350 usuarios

- Througput[15]
    - Se realizó una evaluación de la tasa de transferencia de paquetes en la LAN, entre un servidor y un equipo conectado al mismo switch al que se encuentra conectado dicho servidor, donde se obtuvo lo siguiente:

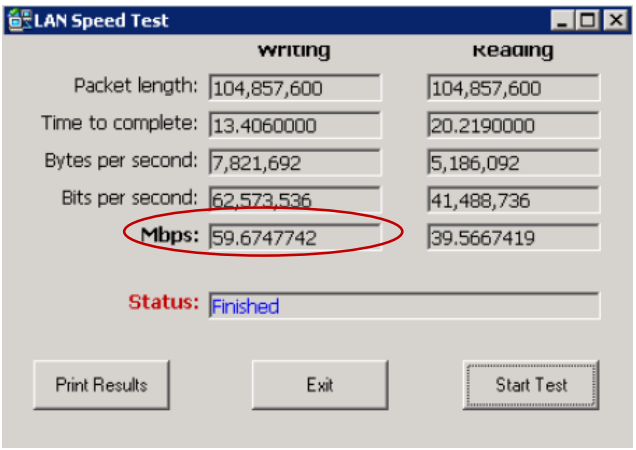


Gráfico 11: Throughtput ADS. Fuente: LAN Speed Test, Enero 2016

Donde se identificó que el throughtput requerido en el Firewall a utilizar debe ser de mínimo 60 Mbps, sin embargo, se debe tomar en cuenta 80 Mbps, es decir, 10 MB.

- ¿Cuál es el número de aplicaciones web con las que cuenta Aseguradora del Sur?
    - Se cuenta con varias aplicaciones web, de las cuales 5 son las más importantes (Visual Time, People Soft, Digital Easy, Correo Electrónico Gmail, Portal Web)

[15] El Througput es la capacidad efectiva de transferencia de datos sobre el enlace.

Es importante notar que no se debe seleccionar un equipo que cumpla al 100% con las necesidades actuales de la empresa, debido que los equipos pueden quedar obsoletos en el lapso de un tiempo, por la escalabilidad del negocio con la tecnología, es por eso que es importante escoger un equipo por lo menos 30% más de los recursos requeridos.

En el informe entregado sobre el análisis de vulnerabilidades donde se calificó el nivel de seguridad sobre 100, siendo un 50% de la calificación relacionada con vulnerabilidades y el 50% con exposición de la infraestructura ante ataques. Es decir, Aseguradora del Sur obtuvo una calificación final de:

Gráfico 12. Análisis de Vulnerabilidad de ADS. Fuente: Radical 2015.

Después de haber realizado los análisis respectivos, se recomendó a la Aseguradora del Sur implementar una solución de seguridad que proteja la información almacenada y archivos críticos, por lo cual se recomendó un equipo de Seguridad perimetral donde su principal función será manejar el control de los accesos perimetrales, junto con todas estas recomendaciones y se toma en cuenta el ancho de banda, número de usuarios en la LAN, el número de aplicaciones web, se recomendó los siguientes equipos:

- **Check Point 4800 NGFW**

Este modelo ofrece todo lo necesario para garantizar que la red de la empresa se encuentre con seguridad en un solo equipo, combina tecnologías de red con capacidades multi-core de alto rendimiento, proporciona el más alto nivel de seguridad, evita comprometer la velocidad de la red para mantener los datos, la red y los usuarios seguros.

Las características del equipo fueron tomadas de la *hoja técnica*[16] de la página oficial de Check Point (Anexo 1):

- 673 SecurityPower™
- 5.8 Gbps production firewall througput
- 1.1 Gbps production IPS througput
- Up to 16 10/100/1000 Base-T ports
- Up to 4 1GbE or 2 10GbE Fiber ports
- Lights-Out-Management (LOM)

[16] https://www.checkpoint.com/downloads/product-related/datasheets/4800-appliance-datasheet.pdf

Especificaciones Técnicas:

Base Configuration
8 x 10/100/1000Base-T RJ45 ports
4 GB memory
250 GB hard disk drive
One AC power supply
Slide rails (22" to 32")
LOM card
Network Expansion Slot Options (1 slot)
4 x 10/100/1000Base-T RJ45 ports
8 x 10/100/1000Base-T RJ45 ports
2 x 1000Base-F SFP ports
4 x 1000Base-F SFP ports
2 x 10GBaseF SFP+ ports
4 x 10/100/1000Base-T Fail-Open NIC
4 x 1000Base-F SX or LX Fail-Open NIC
2 x 10GBase-F SR or LR Fail-Open NIC
Max Configuration
16 x 10/100/1000Base-T RJ45 ports
8 x 10/100/1000Base-T RJ45 + 4 x 1000Base-F SFP ports
8 x 10/100/1000Base-T RJ45 + 2 x 10GBase-F SFP+ ports
8 GB memory
Two redundant hot-swappable power supplies
Production Performance[1]
673 SecurityPower
5.8 Gbps firewall throughput
1.1 Gbps firewall and IPS throughput

RFC 3511, 2544, 2647, 1242 Performance Tests (LAB)
11 Gbps of firewall throughput, 1518 byte UDP
2 Gbps of VPN throughput, AES-128
38,000 max IPsec VPN tunnels
1.5 Gbps of IPS throughput, Recommended IPS profile, IMIX traffic blend
1.7/3.3[2] million concurrent connections, 64 byte HTTP response
70,000 connections per second, 64 byte HTTP response
Network Connectivity
IPv4 and IPv6
1024 interfaces or VLANs per system
4096 interfaces per system (in Virtual System mode)
802.3ad passive and active link aggregation
Layer 2 (transparent) and Layer 3 (routing) mode
High Availability
Active/Active - L3 mode
Active/Passive - L3 mode
Session synchronization for firewall and VPN
Session failover for routing change
Device failure detection
Link failure detection
ClusterXL or VRRP
Virtual Systems
Max VSs: 20 (w/4GB), 25 (w/8GB)
Dimensions
Enclosure: 1U
Standard (W x D x H): 17.25 x 16.14 x 1.73 in.
Metric (W x D x H): 438 x 410 x 44 mm
Weight: 7.6 kg (16.76 lbs.)

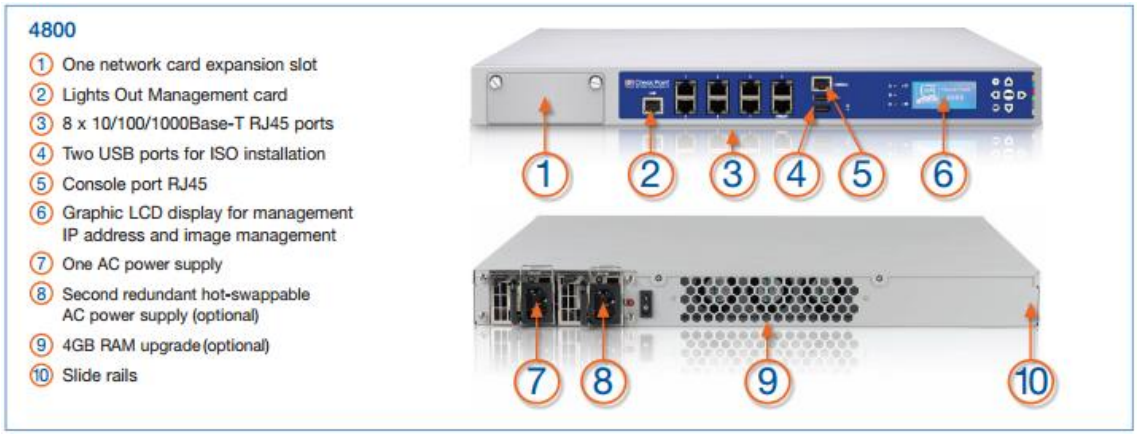


Gráfico 13. Check Point 4800 NGFW.

Fuente: Check Point Software Technologies.

Soluciones de seguridad todo incluido:

Check Point 4800 ofrece una completa y consolidada solución de seguridad en un solo equipo basada en Check Point Software Blade Architecture, disponible con 4 paquetes de software actualizados a diario que son:

- **Next Generation Firewall (NGFW):** Identifica y controla aplicaciones para el usuario y contenido para detener amenazas con el IPS y control de aplicaciones.
- **Next Generation Secure Web Gateway (SWG):** Permite navegar de manera segura en la Web en tiempo real, gracias al Application Control, URL filtering Antivirus y SmartEvent.
- **Next Generation Data Protection (NGDP):** Protege la información sensible.
- **Next Generation Threat Prevention (NGTP):** Aplica capas de protección para prevenir ataques o amenazas con IPS, control de aplicaciones, Antivirus, Anti-Bot, URL filtering.

Acceso Remoto:

El equipo Check Point 6800 permite conectar a 5 usuarios remotamente siempre y cuando exista un equipo firewall del otro lado y no necesariamente debe ser CheckPoint.

- **Palo Alto 3020 (PA-3020)**

El modelo está destinado a la implementación de gateways de Internet de alta velocidad, además, gestiona el flujo de tráfico de red utilizando recursos de computación dedicados para el networking, la seguridad, prevención de amenazas y la gestión.

El elemento de control del firewall de nueva generación PA-3020 es PAN-OS™[17]

Las características del equipo fueron tomadas de la *hoja técnica* de la página oficial de Palo Alto Networks (Anexo 2):

Rendimiento y Capacidad[18]	**PA-3020**
Rendimiento del firewall (con App-ID)	2 Gbps
Rendimiento de la prevención contra amenazas	1 Gbps
Rendimiento de VPN IPSec	500 Mbps
Número de sesiones nuevas por segundo	50.000
Número máximo de sesiones	250.000
Interfaces de túnel/túneles VPN IPSec	1.000
Usuarios simultáneos GlobalProtect (SSL VPN)	1.000
Sesiones de descifrado SSL	7.936
Certificados para SSL entrante	25
Routers virtuales	10

[17] Sistema operativo orientado específicamente a la seguridad, utiliza App-ID, User-ID, Content-ID, WildFire.

[18] El rendimiento y la capacidad fue probado en condiciones ideales usando PAN-OS 5.0 como sistema operativo.

Sistemas virtuales (base/máx.2)	1/6
Zonas de seguridad	40
Número máximo de políticas	2.500

Seguridad

- **Firewall**
  - Control de aplicaciones, usuarios y contenidos basados en políticas.
  - Protección de paquetes fragmentados.
  - Protección de escaneos de reconocimiento.
  - Protección frente a denegación de servicios DoS y denegación de servicio distribuido DDoS.
  - Descifrado: SSL (entrante y saliente), SSH.
- **Wildfire**
  - Identifica y analiza los archivos específicos y desconocidos, reconociendo hasta 100 conductas maliciosas.
  - Genera y ofrece una protección automática contra malware recién descubiertos.
  - Actualización de firmas en menos de 1 hora.

- **Filtrado de archivos y datos**
  - En transferencia de archivos hace un control bidireccional sobre más de 60 tipos de archivos.

- En transferencia de datos hace un control bidireccional sobre transferencias no autorizadas como tarjetas de banco, información que pueda comprometer al usuario o compañía.
- Protección contra descargas.

- **Integración de usuarios (USER - ID)**
  - Integración con Microsoft Active Directory, Sun One.
  - Microsoft server 2008/2003r2, Microsoft Exchange Server 2007/2010.
  - Microsoft Terminal Services.

- **VPN IPSEC (Site to Site)**
  - Intercambio de claves: clave manual, IKEv1.
  - Cifrado: AES, 3DES.
  - Autenticación: MD5, SHA-1, SHA-256, SHA-512, SHA-384.
  - Creación de túneles VPN dinámicos.

- **Prevención de amenazas (Se requiere suscripción)**
  - Protección contra exploits de las vulnerabilidades del S.O y aplicaciones.
  - Protección basada en flujos contra virus, spyware y gusanos.

- **Filtrado de URL (se requiere suscripción)**
  - Categorías de URL predefinidas y personalizadas.

- Memoria cache para los URL visitados.
- Información del tiempo de navegación.

- **Calidad de servicio (QOS)**
  - Control de tráfico en la red basado en políticas por usuario, origen, interfaz, túnel VPN, aplicación, etc.
  - Supervisión de ancho de banda en tiempo real.

- **VPN/Acceso Remoto SSL**
  - Gateway GlobalProtect.
  - Soporte de cliente de terceros: Apple iOS, Android 4.0 y posterior, Linux.

- **Administración, generación de informes, herramientas de visibilidad**
  - Interfaz gráfica web integrada, en varios idiomas.
  - REST API, basada en XML.
  - Resumen gráfico de aplicaciones, categorías de URL, amenazas, datos.
  - Generación de informes totalmente personalizables al usuario.

ESPECIFICACIONES DEL HARDWARE

E/S

- (12) 10/100/1000, (8) puertos SFP ópticos Gigabit

GESTIÓN DE E/S

- (1) puerto de administración fuera de banda 10/100/1000, (2) alta disponibilidad 10/100/1000, (1) puerto de consola RJ-45

CAPACIDAD DE ALMACENAMIENTO

- Unidad de estado sólido (SSD) de 120 GB

FUENTE DE ALIMENTACIÓN (CONSUMO ELÉCTRICO MEDIO/MÁXIMO)

- 250 W (150 / 200)

BTU/H MÁXIMO

- 683

VOLTAJE DE ENTRADA (FRECUENCIA DE ENTRADA)

- 100-240 VAC (50-60 Hz)

CONSUMO MÁXIMO DE CORRIENTE

- 2A a 100 VAC

PREPARADO PARA MONTAJE EN BASTIDOR (DIMENSIONES)

- 1U, bastidor estándar de 19" (4,45 x 43,18 x 43,18 cm – 1,75 x 17 x 16.75 pulgadas)

DIMENSIONES (SOLO DISPOSITIVO/DISPOSITIVO PREPARADO PARA ENVÍO)

- 6,8 Kg / 9,07 Kg

SEGURIDAD

- UL, CUL, CB

INTERFERENCIA ELECTROMAGNÉTICA

- Clase A de FCC, Clase A de CE, Clase A de VCCI, TUV

CERTIFICACIONES

- ICSA

ENTORNO

- Temperatura de funcionamiento: De 0 a 50 ºC (de 32 a 122 ºF)
- Temperatura de almacenamiento: De -20 a 70 ºC (de -4 a 158 ºF)

CONEXIÓN A RED

MODOS DE LOS INTERFACES

- L2, L3, Tap, Virtual Wire (modo transparente)

ENRUTAMIENTO

- Modos: OSPF, RIP, BGP, estático
- Tamaño de la tabla de reenvío (entradas por dispositivo/por VR): 5.000/2.500 (PA-3050), 2.500/2.500 (PA-3020)
- Reenvío basado en políticas
- Protocolo punto a punto sobre Ethernet (PPPoE)
- Tramas Jumbo: tamaño máximo de trama de 9.210 bytes
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, y v3

ALTA DISPONIBILIDAD

- Modos: Activo/Activo, Activo/Pasivo
- Detección de fallos: monitorización de ruta, monitorización de interfaz

ASIGNACIÓN DE DIRECCIONES

- Asignación de direcciones por dispositivo: cliente DHCP/PPPoE/Estática
- Asignación de direcciones por usuarios: servidor DHCP/Relay DHCP/Estática

IPV6

- L2, L3, Tap, Virtual Wire (modo transparente)
- Funciones: App-ID, User-ID, Content-ID, WildFire y descifrado SSL

VLAN

- Etiquetas VLAN 802.1q por dispositivo / por interfaz: 4,094/4,094
- Número máximo de interfaces: 2.048 (PA-3050), 1.024 (PA-3020)
- Interfaces de agregado (802.3ad)

NAT/PAT

- Número máximo de reglas NAT: 1.000
- Número máximo de reglas NAT (DIPP): 200
- Intervalo de direcciones IP y puertos dinámicos: 254
- Intervalo de direcciones IP dinámicas: 16,234
- Modos NAT: NAT 1:1, NAT n:n, NAT m:n
- Sobresuscripción DIPP (direcciones IP de destino único por dirección IP y puerto de origen): 2
- NAT64

VIRTUAL WIRE

- Número máximo de Virtual Wires: 10
- Tipos de interfaz asignados a Virtual Wires: físicos y subinterfaces

REENVÍO DE NIVEL 2

- Tamaño de tabla ARP por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)
- Tamaño de tabla MAC por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)
- Tamaño de tabla de vecino de IPV6: 2.500 (PA-3050), 1500 (PA-3020)

PA-3020

Gráfico 14. PA-3020. Fuente: Palo Alto Network Data Sheets.

2.2.3.2.2. WAF (Web Application Firewall)

Se toma de referencia el Cuadrante de Gartnet para seleccionar las dos marcas líderes en el mercado de Seguridad en aplicaciones Web, para realizar el análisis para una posible implementación.

Gráfico 15. Cuadrante de Gartnet WAF.

Fuente: Gartnet, Julio 2015.

.

- **Imperva**

Imperva Incapsula es el pionero en el mercado de seguridad web, ofrece seguridad y flexibilidad a las empresas que necesitan asegurar sus aplicaciones Web críticas para el negocio de los ciber-delincueltes y optimizar el rendimiento de las aplicaciones Web.

Imperva se asegura de que el tráfico malicioso no llegue a los sitios web protegidos, bloquea ataques a las aplicaciones web y evita que usuarios maliciosos afecten negativamente a las aplicaciones del negocio como muestra la siguiente imagen:

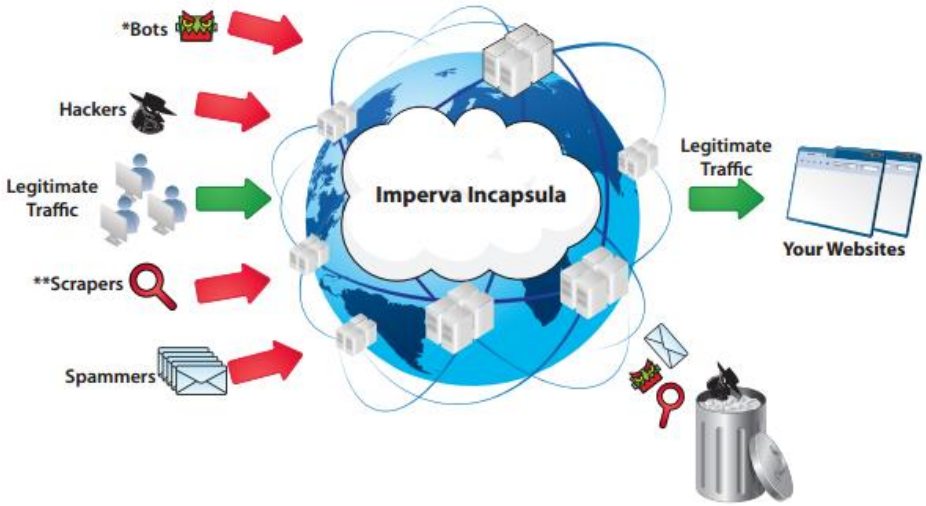


Gráfico 16. Imperva Incapsula. Fuente: Data Sheet Imperva.

El WAF brinda las siguientes ventajas:

- Protege las aplicaciones web y datos críticos.
- Validación de ataques correlacionado.
- Opciones de implementación flexible.
- Inteligencia de amenazas profunda.
- Parches virtuales.

- **BIG-IP Application Security Management - F5**

BIG-IP Application Security Management de F5 es el firewall de aplicaciones web más flexible que asegura las aplicaciones web en entornos tradicionales, virtuales y de nube privada.

Proporciona protección incomparable que ayuda a asegurar aplicaciones web contra vulnerabilidades desconocidas, permite un manejo de la información confiable y segura.

Se tiene un control de políticas en sitios web, que son muy diversos, complejos y se encuentran en constante cambio, lo cual requieren de políticas con cientos o miles de reglas claras y precisas. BIG-IP ASM ayuda a los administradores de seguridad a gestionar cambios y a mantener controles de seguridad y dar acceso a usuarios legítimos.

El WAF brinda las siguientes ventajas:

- Garantiza la seguridad de aplicaciones y su disponibilidad.
- Reducción de costos.
- Mejora la seguridad y rendimiento de las aplicaciones.
- Cuenta con mejores medidas de detección de Bots.

Gráfico 17. BIG-IP ASM. Fuente: Data Sheet F5.

2.2.4. Comparación de equipos

CARACTERÍSTICAS EQUIPOS FIREWALL

EQUIPOS	CheckPoint 4800	Palo Alto 3020
PERFORMANCE		
Firewall throughput	5.8 Gbps	2 Gbps
IPsec VPN throughput	n/d	500 Mbps
Threat prevention throughput	n/d	1 Gbps
IPsec VPN tunnels	38000	1000
Maximum SSL VPN users	n/d	1000
Concurrent connections (Sessions???)	50000	250000
PORTS		
Fixed Ethernet interfaces	8 x 10/100/1000	12 x 10/100/1000
puerto SFP	0	8
Network Connectivity	IPv4 - IPv6	IPv4 - IPv6
Network I/O slots	1	1
POLITICAS		
Max policies	*	2500

EFECTIVIDAD NGF		
Exploit Block Rate (NSS Labs)	98,50%	92,50%
Sistema Operativo		
Versión del Sistema Operativo	Check Point GAiA™	PAN-OS 5.0

Estos datos fueron tomados de las hojas técnicas de cada uno de los fabricantes, que se encuentran en anexos.

2.2.4.1. Beneficios de los equipos

- **Checkpoint 4800 NGFW**

Se propone el equipo Check Point 4800 gracias a beneficios que brinda como son:

✓ Escalabilidad, es decir, esta solución permite crecer en un futuro tanto en infraestructura como en licenciamiento, pues tiene la capacidad de configurarse en alta disponibilidad con otro equipo de idénticas características.

✓ Solución integral, cuenta con la capacidad de gestionar los blades (servicios) desde la única consola de administración.

✓ Compatibilidad, el firewall de Check Point permite integrarse con el resto de componentes de la infraestructura de la red de Aseguradora del Sur.

✓ Integración con Active Directory o Directorio Activo que maneja Aseguradora del Sur.

- **Palo Alto Networks – PA 3020**

Se propone el equipo PA 3020 gracias a beneficios que brinda como son:

- ✓ Cumplimiento de políticas basadas en aplicaciones, es decir, el control será según el acceso a la aplicación debido a que es mucho mejor cuando las aplicaciones no se basan únicamente en el protocolo y puerto, bloquea aplicaciones de alto riesgo, como el intercambio de archivos.
- ✓ Identificación de usuarios (User - ID), este equipo puede comunicarse con varios servidores de dicterio, como Active Directory, SunOne, entre otros, permitiendo aplicar políticas de seguridad basada a usuarios o grupos.
- ✓ Prevención de amenazas, ante virus, gusanos, spyware y algún otro trafico mal intencionado que trate de ingresar en la red.
- ✓ Filtrado URL, las conexiones salientes se pueden filtrar de esta forma impidiendo el acceso a páginas web no adecuadas.
- ✓ Versatilidad de red y velocidad, el PA320 puede añadirse o sustituir o cualquier otro firewall que haya estado anteriormente.
- ✓ GlobalProtect, protege a los equipos que se encuentren fuera de la LAN.
- ✓ Funcionamiento a prueba de fallos, es decir, ofrece alta disponibilidad tolerante a fallos automáticamente desde cualquier interrupción de Hardware o Software.

CAPITULO III: ANÁLISIS DE LA SITUACIÓN ACTUAL DE ASEGURADORA DEL SUR

3.1. Reseña histórica de Aseguradora del Sur

Aseguradora del Sur, fue fundada el 11 de febrero de 1990 en la ciudad de Cuenca, por el Ing. Rodrigo Cevallos Breilht, como una compañía de seguros y reaseguros cien por ciento con capital ecuatoriano, con el único objetivo de brindar a los ecuatorianos la mayor protección, en todo momento y en todo lugar, contando con un respaldo incondicional y bajo los conceptos de fortaleza y solidez, Aseguradora del Sur es una empresa confiable, estable y segura, estando ya en el mercado 26 años.

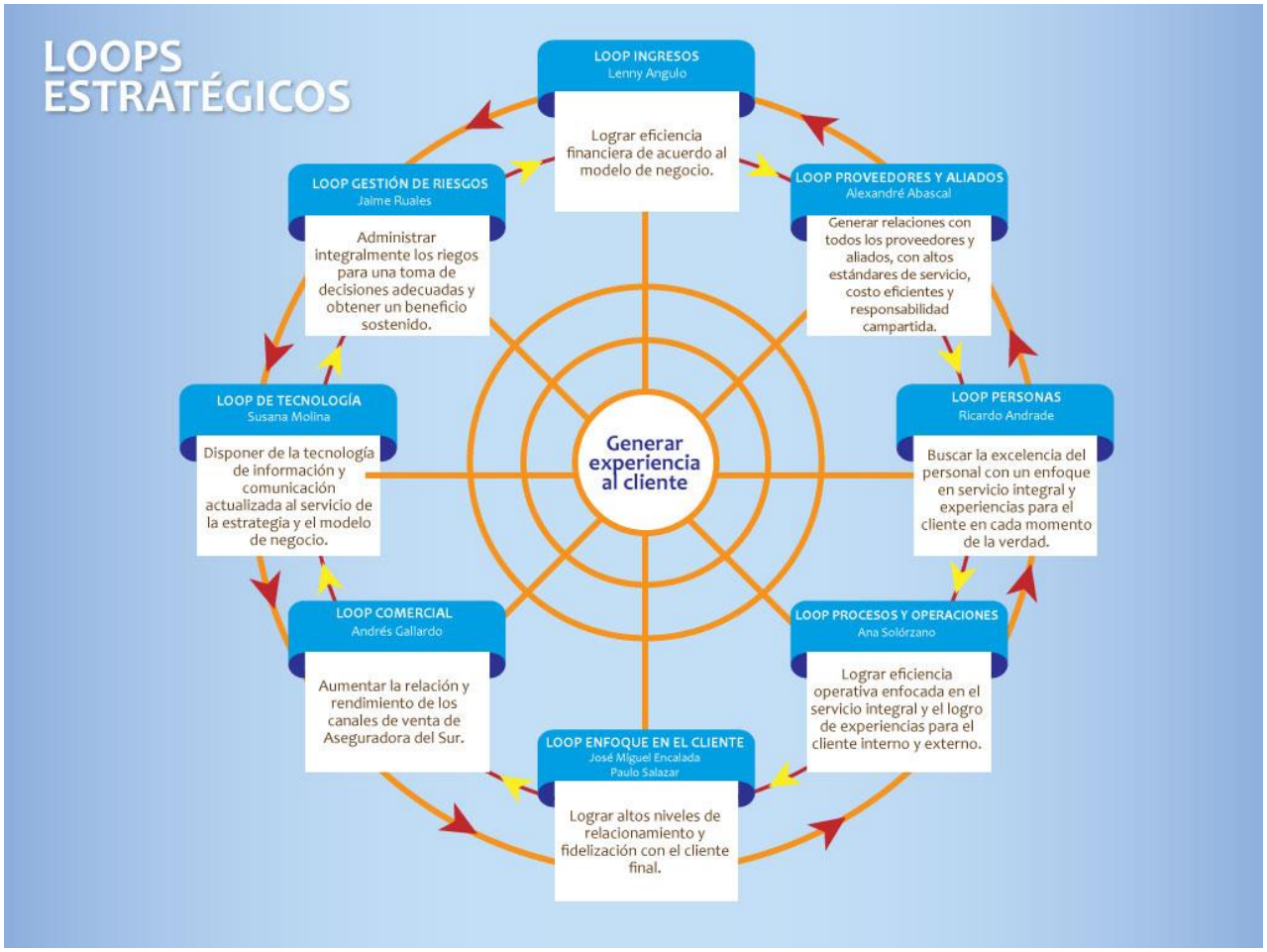
En el año 1994, Aseguradora del sur, transfiere su matriz a la ciudad de Quito, con un gran crecimiento en el mercado ecuatoriano, en el año 1997 hasta el año 2010, gracias a la gran trayectoria que caracteriza a Aseguradora del Sur en el mercado de los seguros, se inauguraron nuevas sucursales en Ibarra, Ambato, Cuenca, Loja, Machala, Manta, Portoviejo, Riobamba, el Coca y Santo Domingo, cubriendo las zonas del centro – Sur y Costa del país, actualmente cuentan con 11 sucursales a nivel nacional.

Los últimos años han sido muy importantes para la compañía, pues han mostrado un gran crecimiento que tiene como base la seriedad y profesionalismo que se demuestra frente a sus asegurados y proveedores. Todo esto gracias a la calidad del trabajo de sus colaboradores, que con su compromiso y entrega

continua hacen una empresa cada día más eficiente, estable y segura en el mercado ecuatoriano.

3.2. Why Empresarial

3.3. Loops Estratégicos



3.4. Antecedentes

3.4.1 Situación Actual de la infraestructura en la empresa

Hoy en día la información es el activo más valorado en las empresas, por lo tanto se debe proteger ante riesgos existentes en el entorno, tanto interno como externo.

Actualmente en la Aseguradora del Sur existe mucha información importante, sensible e indispensable para el funcionamiento de la misma, como base

de datos de clientes, base de datos activos, documentación de proyectos, documentos financieros, además la razón principal para implementar un sistema de seguridad perimetral es que se cuenta con aplicaciones web que maneja el **Core** del negocio, transacciones en línea, lo cual es fundamental tenerlo resguardado, hoy en día en Aseguradora del Sur se tiene un cierto nivel de vulnerabilidad en todo lo relacionado con virus, malware's, saturación de servicios de la red, correos maliciosos, entre otros.

La infraestructura actual de la red no fue planeada con un enfoque de seguridad a futuro, ya que concuerda con el esquema típico de una red, que consiste en la protección con un firewall lógico para toda la red privada junto con un antivirus, además se cuenta con proxy's[19] para manejar el acceso a la web, actualmente se cuenta con 7 proxy's, sin embargo, el crecimiento tecnológico de Aseguradora del Sur llevó a la modificación del esquema de red actual, siendo necesario tomar en cuenta para realizar actualizaciones planeadas o estimadas de la infraestructura TI.

En Aseguradora del Sur no existe un esquema de seguridad perimetral establecido y previamente analizado para suplir las necesidades de seguridad de la red actual; existen ciertos puntos de control pero no valoraciones previas que justifiquen dichos puntos, son solo controles implementados esporádicamente, es decir para tener un control de la seguridad e integridad de la información se utiliza Firewall lógico dentro

[19] Punto intermedio entre un ordenador conectado a Internet y el servidor.

de la red de datos, sin embargo se ha tenido varios inconvenientes y ataques de malware, correos spam, software malicioso.

El segmento de red para Aseguradora del Sur se maneja con un servicio DHCP para Ethernet como para la red inalámbrica en su Matriz Quito, sin embargo, para Sucursales se utiliza IP's estáticas en el adaptador de Ethernet y red inalámbrica:

Sucursal	**Segmento de Red**	
Matriz	VLan Inicial	172.16.50.x
	VLan Básico	172.16.51.x
	VLan Intermedio	172.16.52.x
	VLan Avanzado	172.16.53.x
	VLan Full	172.16.54.x
	VLan Sistemas	172.16.55.x
Ambato	172.16.8.x	
Riobamba	172.16.6.x	
Cuenca	172.16.4.x	
Loja	172.16.18.x	
Quito – Sur	172.16.24.x	
Machala	172.16.12.x	
El Coca	172.16.22.x	
Ibarra	172.16.14.x	
Manta	172.16.10.x	
Portoviejo	172.16.2.x	

Santo Domingo	172.16.16.x

El acceso a Internet y enlaces de datos se tiene con los siguientes proveedores:

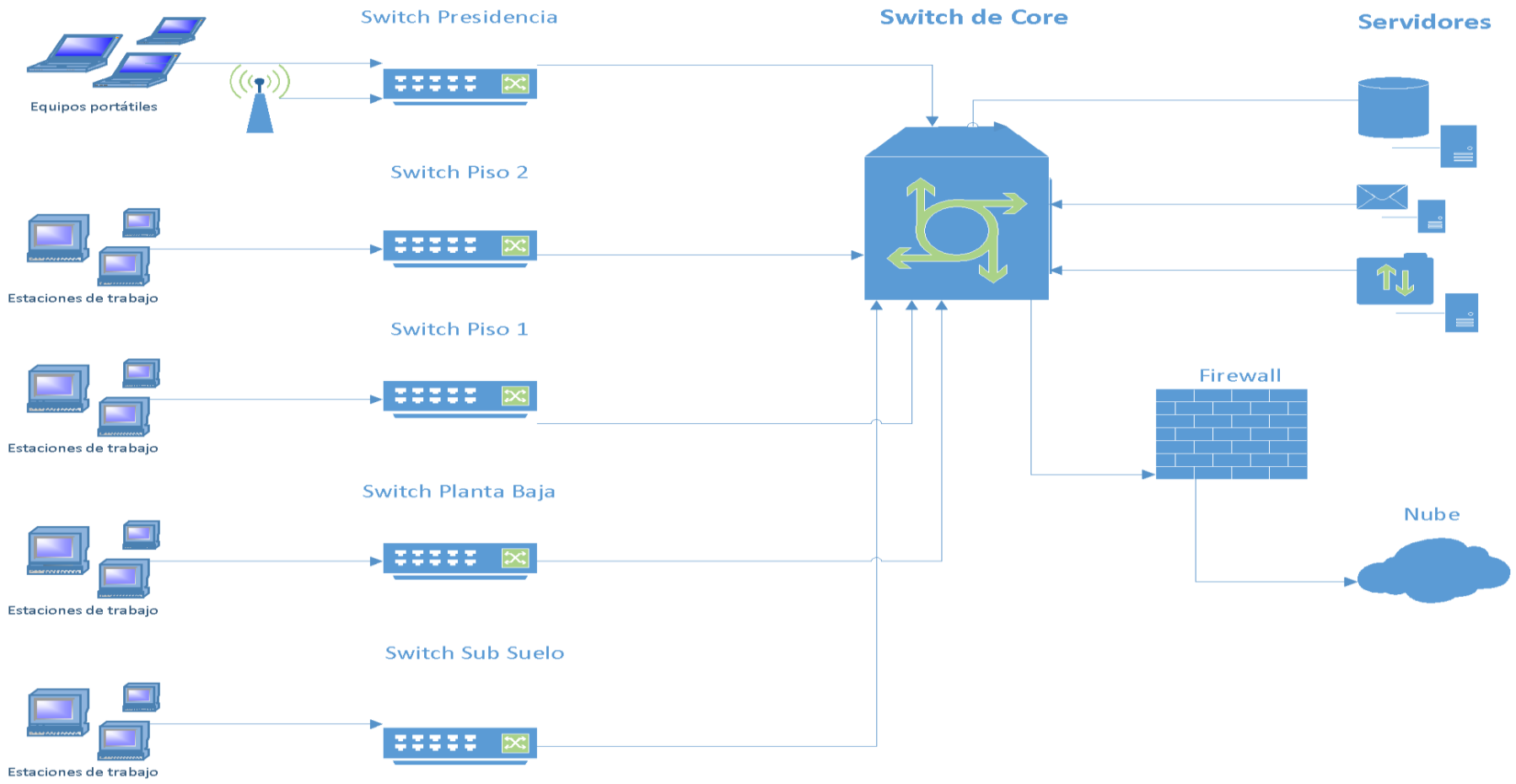
Proveedor	Sucursal
LEVEL3	Machala, El Coca, Matriz
Telconet	Ambato, Cuenca, Riobamba, Santo Domingo, Portoviejo, Manta, Ibarra, Riobamba
CNT	Quito Sur

Se tiene un tipo de enlace de datos por medio de MPLS[20], para poder comunicarse entre las sucursales, en forma de telaraña red multipunto o multienlace.

El acceso físico al Data Center y los cuartos de mando en cada piso del edificio, está restringido a todo el personal de Aseguradora del Sur excepto a los Ingenieros de Infraestructura y Gerente de Sistemas, además en el data center principal y en cada cuarto de mando cuentan con dispositivos de detención de humo, sensores, extintores que contienen PSQ[21], para evitar daños en los equipos, aire acondicionado adecuado para mantener el aire a una temperatura fría. Se dispone de sistemas de UPS para garantizar la disponibilidad y funcionamiento continuo de los servidores y estaciones de trabajo lo que evita perdida de información en algún corte de energía.

[20] Multiprotocol Label Switching, es un mecanismo de transporte de datos, tráfico de voz.
[21] Polvo Químico Seco para incendios

3.4.2. Topología Actual



En Aseguradora del Sur existe una red de datos de tipo LAN, esta es de topología de estrella, es decir, todas las estaciones (servidores, switches o estaciones de trabajo) están conectadas a un solo concentrador o switch de core.

Tienen puertos definidos de entrada y salida:

- Puertos de salida 25 (Correo SMTP), 110 (Correo POP3
- Puertos de entrada 80 (Portal Web HTTP), 443 (Portal Web SSL)

3.4.3 Análisis de la situación actual de la seguridad informática en Aseguradora del Sur

Es importante realizar un análisis de la situación actual de seguridad informática en Aseguradora del Sur para conocer más a fondo las vulnerabilidades y amenazas que sufre la red en la compañía y de esta manera contrarrestarlas, aumentando el nivel de disponibilidad, integridad y fiabilidad, garantizando la confidencialidad de la información que se maneja a diario en las oficinas de Aseguradora del Sur, además conocer el estado actual de la empresa, permite definir una estrategia para la posible solución de seguridad.

Según la entrevista con el Ingeniero Fernando Suárez Jefe de Infraestructura, indicó que la empresa identifica muchas vulnerabilidades y amenazas tanto en los servidores, estaciones de trabajo y dispositivos de red.

Aseguradora del Sur para reconocer a sus dispositivos en la red, utiliza la herramienta como WhatsUp Gold de IPSWITCH, con el cual monitorean a los servidores físicos, y para monitorear a los servidores virtuales se utiliza la herramienta de gestión de VMWare. En el caso de que cualquier intruso se encuentre en la red, basan su análisis en logs del switch de CORE, comprometiendo a la red debido que los logs tan solo servirán como un análisis forense postmorten, un ejemplo de aquello es que existen ACL´s[22] creadas a través de las cuales, cuando existe un alto tráfico no autorizado en el switch, este lo bloquea el puerto deshabilitando la telefonía IP y otras aplicaciones que dependen del puerto, es decir existe un alto porcentaje de denegación de servicios.

Actualmente no existen sistemas de seguridad que ayuden a sobrellevar las vulnerabilidades y amenazas que puedan comprometer la información en base de datos, infraestructura y aplicaciones.

Se realizó un análisis de vulnerabilidades a un equipo conectado a la red de Aseguradora del Sur, con la herramienta OpenVas – Linux, es una

[22] Access control list – lista de control de accesos, usado para determinar los permisos de acceso a un determinado objeto.

herramienta multiplataforma sencilla y fácil de usar, donde se obtuvo los siguientes resultados (Anexo 3).

El análisis fue realizado al firewall lógico con IP 172.16.1.10 con la que cuenta actualmente en la empresa, el miércoles 20 de enero, 2016 a las 17h30, evitando algún conflicto de red en horarios laborables.

El análisis de las vulnerabilidades que pueda tener el servidor es clave para la seguridad de toda la red, ya que una única vulnerabilidad puede ser un punto de entrada en la red para un atacante.

Dentro de los resultados del análisis de vulnerabilidades se considera lo siguiente:

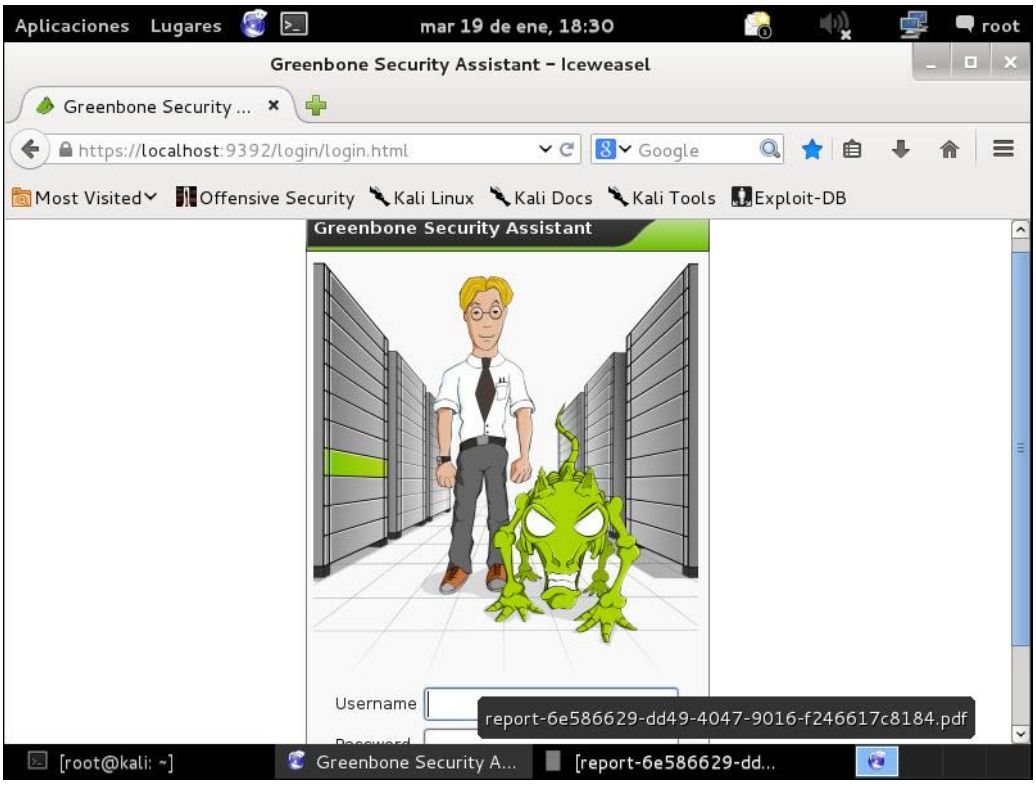
Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
general/CPE-T	Log
22/tcp	Log
111/tcp	Log

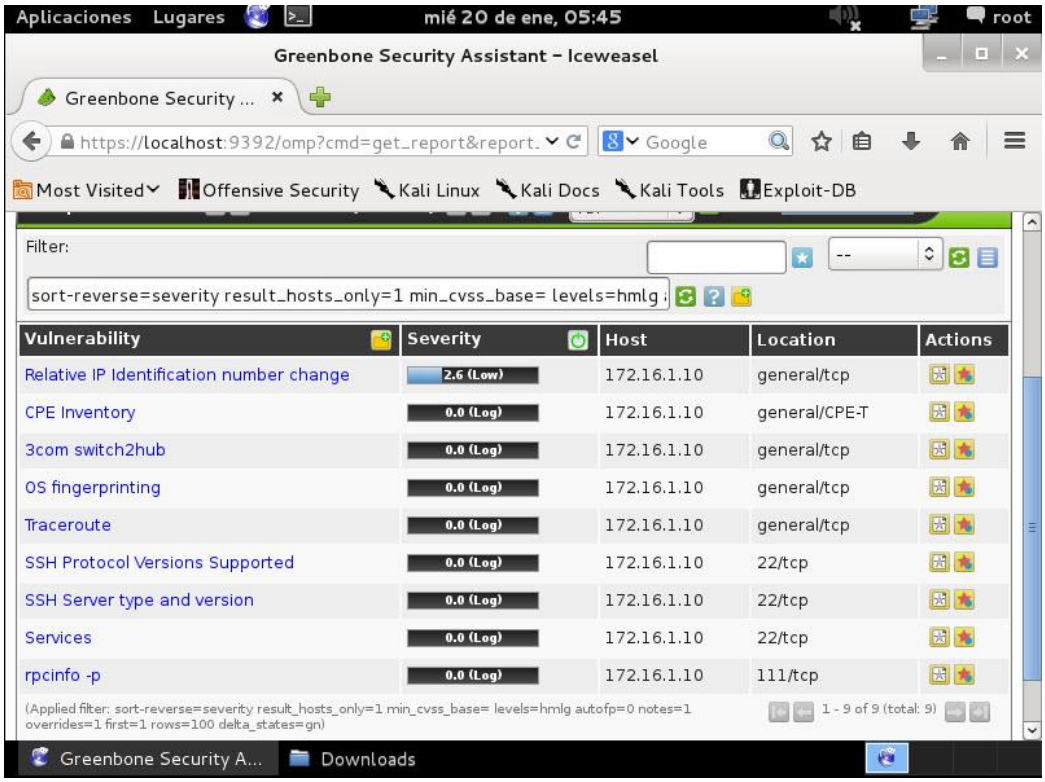
Gráfico 18. Análisis de Vulnerabilidad Firewall. Fuente: OpenVas

En el cuadro anterior se puede observar el nivel de amenazas dentro del servidor Firewall, siendo vulnerable en el manejo de paquetes enviados a través del servidor y en la entrada de paquetes recibidos por el servidor, es posible que no sea fácil identificar los paquetes que se envían al servidor debido a que no se cuenta con ninguna herramienta adicional como un IPS o IDS para ayudar a la identificación de amenazas, sirviendo a un

atacante esta característica para identificar patrones de tráfico en la red, rastreo de puertos en la red e inyectar algún código malicioso, malware, bot, entre otros.

Siendo el Firewall, la puerta de seguridad entre la red interna LAN y el Internet se puede notar la gran falla de seguridad con la que cuenta Aseguradora del Sur, ya que basta con un solo ataque para poder denegar servicios que sean indispensables para el manejo del negocio o en el peor de los casos dejar sin servicio de red a toda la empresa.





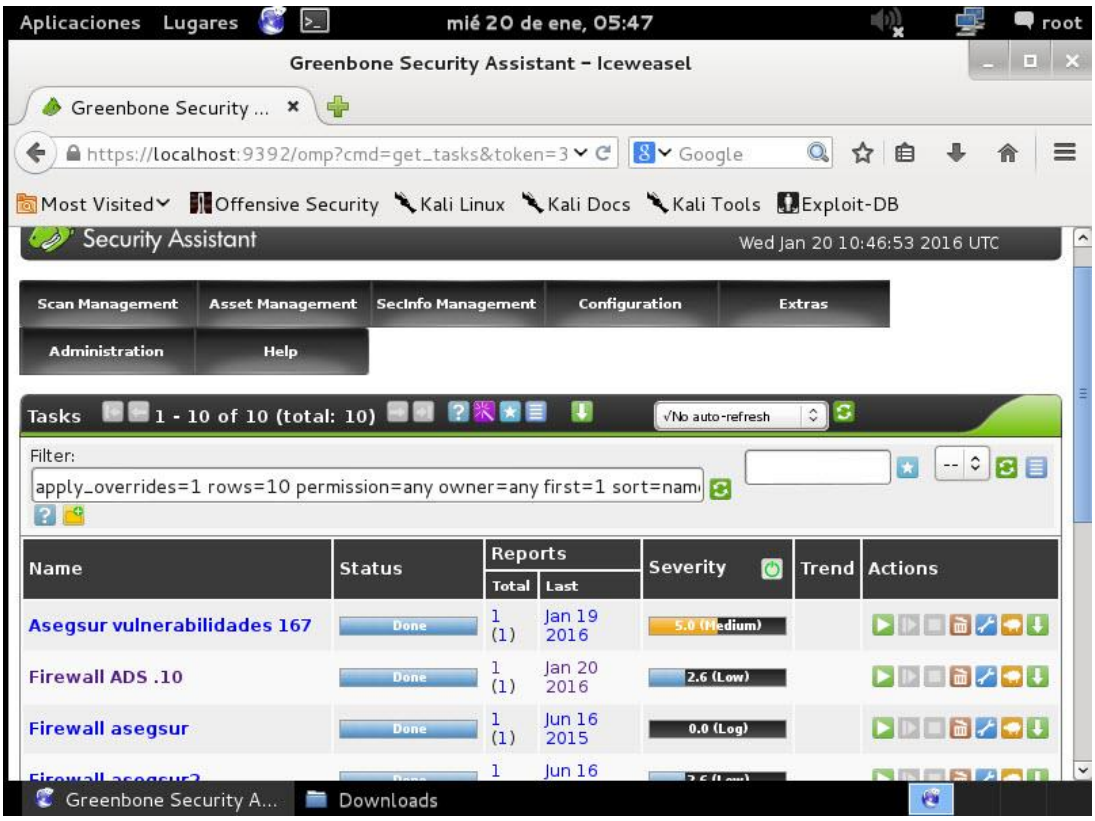


Gráfico 19. Herramienta OpenVas. Fuente: OpenVas

Se realizó un segundo análisis de vulnerabilidades con una empresa experta en seguridad de perimetral, se calificó el nivel de seguridad sobre 100, siendo un 50% de la calificación relacionada con vulnerabilidades y el 50% con exposición de la infraestructura ante ataques, donde se obtuvo:

Gráfico 20. Análisis de Vulnerabilidad de ADS. Fuente: Radical 2015.

Según el informe emitido por el personal de Radical de todos los puntos que fueron analizados, 50 puntos lo califica en dos ponderaciones vulnerabilidades de alto riesgo donde se encuentra en riesgo las sesiones SSL, vulnerabilidades en Oracle y de medio riesgo que incluyen comunidades SNMP[23] y vulnerabilidades en MySQL.

Treinta (30) puntos fueron deducidos por tener 236 servicios no esenciales habilitados en la red, es decir, esto aumenta sin necesidad la posibilidad de ser atacados por vulnerabilidades en estos servicios.

[23] SNMP, es un protocolo simple de administración de red, permite administrar dispositivos de red y diagnosticar problemas.

Diez (10) puntos fueron deducidos por permitir tráfico UDP[24] no necesario. En las exploraciones de exteriores, una presencia en Internet no suele requerir UDP con la excepción de DNS manejado en el puerto 53. UDP es un riesgo para la seguridad, debido que es un protocolo de transporte común para negación popular de servicios (DoS) y programas de puerta trasera.

Con respecto a los aplicativos que maneja parte del **Core** del negocio, existe 21 vulnerabilidades en PeopleSoft, 13 en Servicios en línea y 26 en Visual Time, tomando en cuenta que 8 de ellas son altamente críticas.

En el cuadro se muestra el resumen de vulnerabilidades por puerto:

Top 15 Hosts with Vulnerabilities

System	High	Medium	Low	Informational
SERBIPRO, 172.16.1.112	4	6	0	32
www.aseguradoradelsur.com.ec, PORTAL, 172.16.1.8	2	3	3	26
172.16.52.203	0	2	2	29
SERVTPR1, 172.16.1.196	0	0	0	25
BCESARF, 172.16.52.180	1	0	0	13
172.16.1.202	0	1	0	12
IVIN-HP, 172.16.52.182	0	0	0	12
ADRIANA-PC, 172.16.52.177	0	1	0	11
172.16.52.253	1	2	0	9
FERNANDO-HP, 172.16.52.10	0	0	0	10

Gráfico 21. Resumen de Vulnerabilidad por puerto. Fuente: Radical 2015.

[24] UDP, es un protocolo del nivel de transporte en el modelo OSI que se basa en el intercambio datagramas.

La infraestructura más importante y esencial para la Aseguradora del Sur está en las bases de datos Oracle, donde también se encontró vulnerabilidades sobre Oracle en el servidor 172.16.1.8 perteneciente a un servidor Windows 2008 donde también se cuenta con el PORTAL de Aseguradora del Sur www.aseguradoradelsur.com.ec, medio por el cuál un hacker pudiera ejecutar código malicioso sobre las bases de datos.

Existen aplicaciones personalizadas para Aseguradora del Sur (SOS)[25], al momento de salir a producción en las aplicaciones la seguridad no está considerada, es decir que existe un riesgo, estos aplicativos son modulares, cliente servidor, es decir se tiene varios módulos uno para Fianzas, uno para Comerciales, Producción, Renovaciones, entre otros, estos módulos se da funcionalidad dependiendo del perfil del colaborador en la compañía.

En Visual Time se tiene un control de acceso dentro de los roles de las aplicaciones ya que es escrito sobre .NET; PeopleSoft es un software que está por salir a ser parte de Aseguradora del Sur, en cual se quiere levantar políticas de seguridad que aún no se las tiene.

[25] SOS, Sistema de Operaciones de Seguros, actual sistema Core de Aseguradora del Sur.

3.4.4 Seguridad de la red y Protección de la información

En esta sección se idéntica las capacidades tecnológicas que Aseguradora del Sur tiene para proteger su red y los sistemas que manejan.

Actualmente, Aseguradora posee seguridad de Endpoint Symantec como antivirus, con consola central. El firewall es un servidor con listas de acceso ACL's a nivel de red, basados en Linux.

Las formas de acceder a los servidores físicos primero se utilizan SSL para acceso y SSH para la consola.

En cuanto a la protección de la información se cuenta con políticas de seguridad establecidas que realizan un convenio de confidencialidad con el empleado que es firmado en su contrato, sin embargo, no existe un control y auditoria sobre si las políticas se cumplen dentro de la compañía.

Para prevenir fuga de información, Aseguradora del Sur actualmente utiliza políticas de Active Directory que bloquea herramientas de almacenamiento extraíble.

Existe clasificación de información en base a la importancia de la misma y del giro del negocio, el líder de cada proceso lo sabe y lo maneja con el departamento de riesgos, el cual indica que información es la más

sensible para cubrirla en base a las posibilidades de la Aseguradora por medio de ACL`s y el Active Directory.

3.4.5 Vulnerabilidades de servicios en línea

Con respecto a los servicios en línea, la aplicación no valida datos ingresados por lo que esto expone a la aplicación a que un atacante proporcione valores inesperados, causando un fallo en el servicio, consumo excesivo de recursos como la memoria y el procesamiento del CPU, por lo cual genera mala imagen para Aseguradora ante sus clientes. También un atacante puede utilizar fishing a los usuarios adquiriendo información personal o aprovechando de una entrada maliciosa para modificar datos.

Otra vulnerabilidad en la aplicación web, es que no se puede verificar de manera adecuada si una solicitud fue valida, debido que un atacante podría realizar operaciones como si fuera la víctima, y mucho peor si la víctima es un administrador o un usuario con privilegios, las consecuencias serian obtener un control completo sobre la aplicación web. Las credenciales son transmitidas sin cifrado por lo que pueden ser fácilmente interceptadas, ni tampoco valida si alguna persona está tratando de adivinar la contraseña por varios intentos.

Dirección web:

http://www.aseguradoradelsur.com.ec/srvonline/hloginsvw.aspx

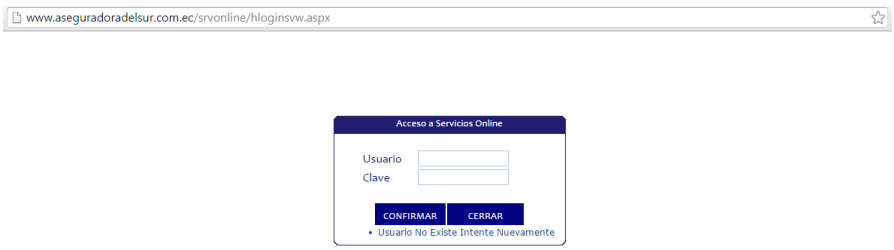


Gráfico 22. Aplicación web. Fuente: ADS 2016.

3.4.6 Vulnerabilidades del Visual Time

Visual Time es un aplicativo web que controla el **Core** de negocio completo, va a ser lanzado en marzo 2016 ya que actualmente cuentan con un software (SOS) cliente servidor, propio de Aseguradora para manejar el **Core** del negocio.

Es vulnerable a ataques de Cross Site Scripting, es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones web inyectando a páginas frecuentadas por el usuario código JavaScript que puedes servir para engañar al usuario y hacer que ingrese información de autenticación o a su vez re direccionar al usuario a una página web controlada por el hacker probablemente con la misma interfaz gráfica que la página web de un inicio.

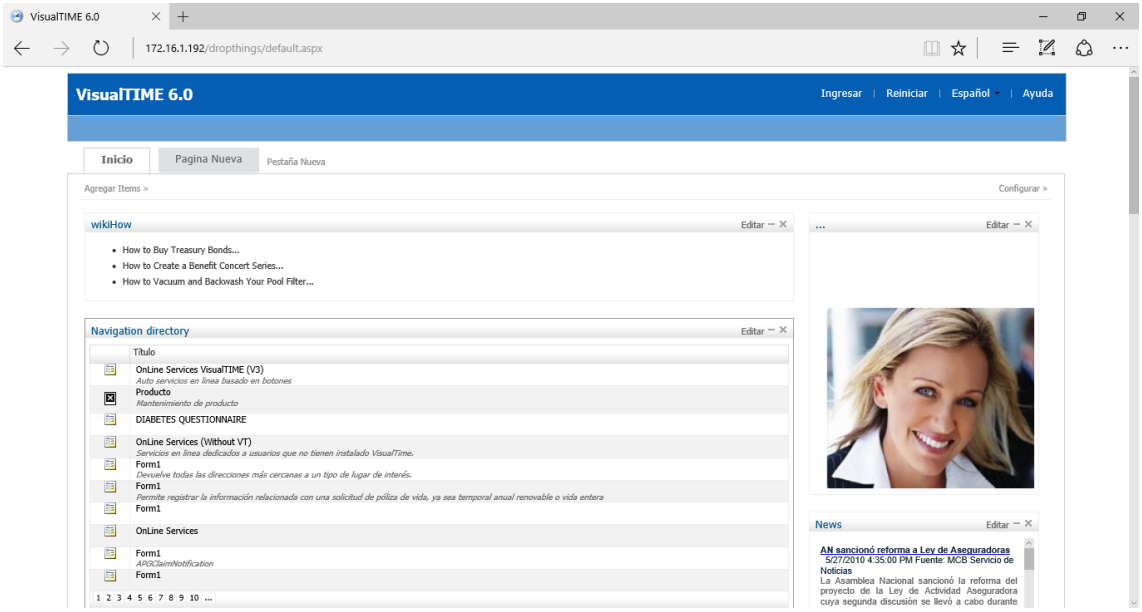
Alerts distribution

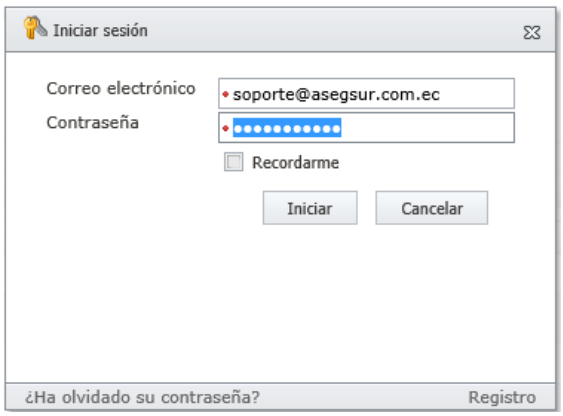
Total alerts found	20
High	8
Medium	4
Low	4
Informational	4

Executive summary

Alert group	Severity	Alert count
Cross site scripting (verified)	High	4
HTTP parameter pollution	High	4
Application error message	Medium	2
HTML form without CSRF protection	Medium	1
User credentials are sent in clear text	Medium	1

Gráfico 23. Vulnerabilidades externas realizadas a Visual Time. Fuente: Radical 2016





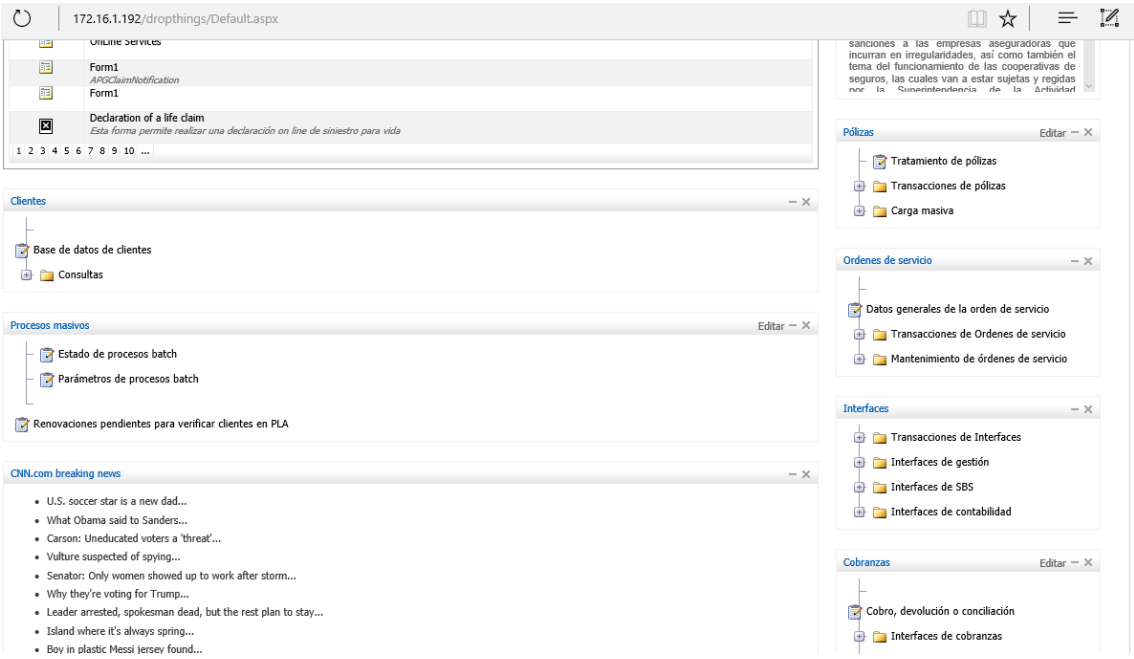


Gráfico 24. Front Visual Time. Fuente: Visual Time 2016

3.4.7 Vulnerabilidades People Soft

La aplicación web de People Soft es un software para manejar la parte financiera y contable de Aseguradora, en donde se maneja cuentas por pagar, activos fijos, cuentas por cobrar, además de tener consolidaciones bancarias.

Sin embargo, esta aplicación web cuenta con vulnerabilidades como, por ejemplo, las credenciales (usuario, contraseña) de cada usuario son transmitidas sin estar cifrados por lo que pueden ser fácilmente interceptadas, también es vulnerable ante ataques de denegación de servicios (DoS).

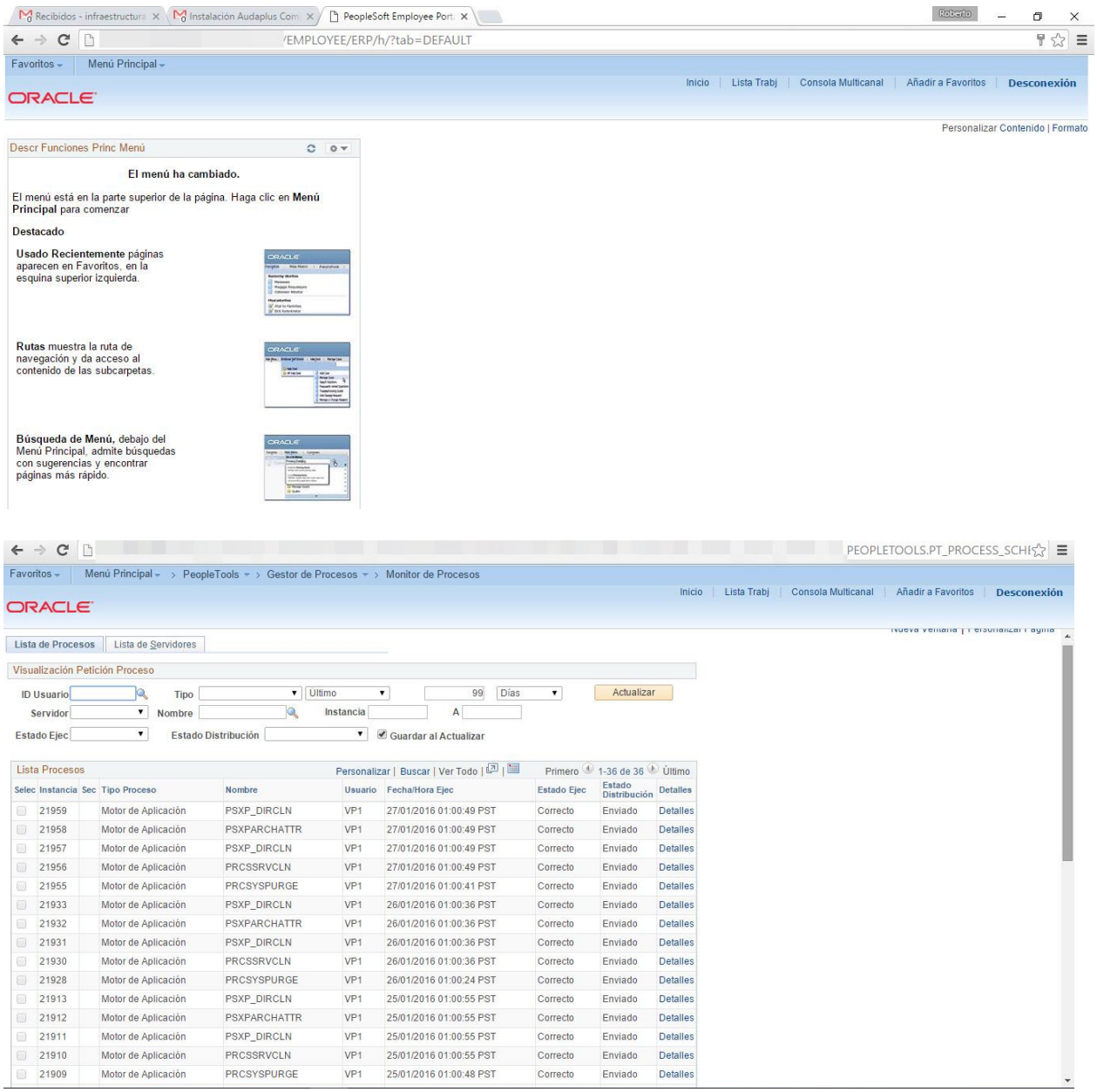


Gráfico 25. Front People Soft. Fuente: People Soft 2016

3.4.8 Requerimientos de seguridad de Aseguradora del Sur.

Aseguradora del Sur ha evidenciado varias vulnerabilidades en su sistema de seguridad tanto en la parte de infraestructura, aplicativos como en el factor humano y aplicación de políticas de seguridad, para lo cual ellos necesitan un sistema de seguridad perimetral.

Se ha tenido varios ataques a sus aplicativos que no pudieron ser prevenidos por no contar con un sistema de seguridad y lo único que podían observar era el postmorten del ataque a través de logs que eran emitidos por el firewall lógico con el que cuentan, por ejemplo, se ha tenido casos de denegación de servicios.

Otro factor importante para implementar un sistema de seguridad perimetral es controlar los accesos a Internet de los empleados y evitar contar con varios proxy's para realizar el control, debido que se genera indisponibilidad de servicios por tráfico o saturación de los servidores, para lo cual con un Next Generation Firewall mejoraría la productividad del empleado mejorando los tiempos de respuesta y controlando su navegación por Internet.

También Aseguradora del Sur tiene gran preocupación en cuanto a la protección de su información en el computador de cada empleado, actualmente se cuenta con políticas internas de seguridad y confidencialidad directamente con el empleado, sin embargo, para el líder del proceso de Riesgos y Seguridad de la Información es indispensable controlar de manera efectiva la fuga de información por parte de los colaboradores.

En cuanto a las nuevas aplicaciones web que van a ser lanzadas se requiere evitar sufrir de ataques como fishing, DoS, entre otros, debido que en esas

aplicaciones se manejara al 100% el giro del negocio y un *downtime*[26] sería una gran pérdida económica para Aseguradora del Sur.

En el siguiente cuadro podemos observar la tecnología a utilizarse para cubrir los requerimientos de Aseguradora del Sur:

Requerimiento	Tecnología a utilizar
Ataques en nuevas aplicaciones web	• Para controlar vulnerabilidades de ataques internos se utilizará un control de aplicaciones con un **Next Generation Firewall.** • Para controlar vulnerabilidades de ataques externos se utilizara un **Web Application Firewall WAF.**
Ataques de fishing al usuario, redirigiendo a una página parecida para conseguir las credenciales	Este requerimiento será solventado con la implementación de un **Web Application Firewall WAF.**
Indisponibilidad de servicios en Internet	Se eliminará la configuración proxy y se manejara el control de accesos con un **Next Generation Firewall.**

[26] Fuera de tiempo en producción

Productividad de los empleados	Se realizará el bloqueo de páginas no necesarias para manejar el giro del negocio con un **Next Generation Firewall.**
Protección de la información custodiada por cada colaborador	En un equipo con **Next Generation Firewall** se cuenta con DLP (Data Loss Prevention), el cual ayuda a prevenir la fuga de información, identificando palabras claves.
Bloqueo de amenazas que quieran atacar a Aseguradora del Sur.	Se contara con un IPS incluido en el **Next Generation Firewall** para detectar vulnerabilidades y aplicar filtros de bloqueos.

3.5. Análisis Económico en la Aseguradora del Sur

3.5.1. Evaluación de las soluciones

Existen dos grandes criterios para evaluar la solución que posiblemente va a ser implementado:

- **Evaluación tecnológica:**

En este punto se contempla que tan bien cumple cada fabricante con los requerimientos de Aseguradora del Sur.

Tomando en cuenta la evaluación tecnológica realizada en el Capítulo II (2.2.3.2) de los equipos de seguridad perimetral, es importante tomar en cuenta que no se debe escoger un equipo que cumpla con los requerimientos mínimos ya que Aseguradora del Sur crece diariamente y se debe elegir un equipo que tenga la opción de escalabilidad, es decir, se debe escoger un equipo que por lo menos ofrezca el 30% más de los requerimientos mínimos, por su gran posicionamiento en el cuadrante de Gartnet y también tomando en cuenta la investigación por parte de la revista ComputerWorld Ecuador lanzada en Enero 2016, del top en seguridad perimetral CheckPoint y Palo Alto, demostraron su alto desempeño y rendimiento en ambientes parecidos a los que Aseguradora del Sur presenta, con una cantidad de 350 usuarios y un promedio de 200 conexiones concurrentes, se debe tomar en cuenta los dos equipos CheckPoint 4800 y Palo Alto 3020 siendo estos Next Generation Firewall con las funcionalidades de antibot, control de aplicaciones, IPS, URL filtering, control de accesos.

Además, se recomienda implementar un Web Application Firewall para controlar toda la seguridad web y sus aplicaciones dentro de la compañía tomando en cuenta la comparación técnica en el capítulo II (2.2.3.2).

- Evaluación económica:

En este punto se muestra que tan atractiva es la propuesta económica enviada por parte del proveedor tanto del Next Generation Firewall como del Web Application Firewall WAF, en sus costos/beneficios, soporte e instalación y puesta en marcha.

COSTOS DE EQUIPOS FIREWALL

EQUIPOS	CheckPoint 4800	Palo Alto 3020
ITEM		
Costo referencial	$39.967,00	$14.930,00
Costo Mantenimiento anual referencial	$5.334,00	$3.211,00
Instalación y puesta en marcha	$1.875,00	$3.000,00

COSTOS DE EQUIPOS WAF

EQUIPOS	IMPERVA X2500	F5 BIG-IP ASM
ITEM		
Costo referencial	$101.114	$34.755
Costo Mantenimiento anual referencial	$8.450	$5.200
Instalación y puesta en marcha	$1.950	$1.950

La valorización de los equipos utilizados en la presente tesis, fue tomada de precios referenciales de proveedores acreditados en Ecuador.

3.5.2. Riesgo del negocio.

En esta sección, se analiza el papel que juega la administración de riesgos en el aseguramiento de la información y la identificación de los riesgos a los cuales están sometidos los activos de la Aseguradora.

Actualmente, los seguros individuales de vehículos conforman el 54% de los ingresos para Aseguradora del Sur, sin embargo, con el alza de aranceles para autos y motocicletas, el mercado ecuatoriano se volcará a la adquisición de vehículos usados, es decir Aseguradora tendrá que realizar un plan muy atractivo en la categoría de precios mayores a 20k (semilujos

y lujos), también en la creación de nuevos planes para vehículos y crecer en otras líneas del mercado.

La idea de Aseguradora del Sur es aumentar de 4 millones de dólares en ventas de productos masivos a 10 millones de dólares en la Matriz – Quito, para ello, el nuevo sistema ERP Visual Time que manejara el giro del negocio será de gran importancia ya que automatizara muchos procesos que con la herramienta actual se los haría manualmente. Otro ingreso para Aseguradora, que se desea optimizar y automatizar, es la gestión de renovaciones de pólizas, en el cual Visual Time también permite manejar ese proceso. Es decir los 10 millones de dólares de inversión tomando, en cuenta el sistema de seguridad perimetral a implementar y los sistemas web (Visual Time, People Soft), se necesita tener un retorno de 7 millones en transacciones masivas y automatizadas, a través de Visual Time, un aproximado seria que en 52 semanas después del lanzamiento la herramienta produciría $326.923 por semana, es decir, $65.384 diarios, según el financiero general de Aseguradora del Sur, si se enfoca en la parte de seguridad se puede dar cuenta que ese sería el costo directo por tener fuera el servicio de la herramienta, por cada ataque informático realizado y que afecte al funcionamiento de Visual Time, ya que también es la fuente de datos del RP Financiero – Contable - Administrativo People Soft, por lo que una falla en Visual Time compromete también a otras áreas del negocio reduciendo la productividad de la empresa.

La mejora en el tiempo de atención a los bróker o vendedores, se obtendrá gracias al acceso web donde se tiene interconexión con concesionarios y asesores de una manera más rápida y ágil, también existirá una mejor respuesta por parte de los ejecutivos comerciales con el nuevo sistema se evita la pérdida de tiempo a los Brokers obviando realizar algunas operaciones manuales como lo era con el SOS, y se mejorará el servicio en la entrega de pólizas en el que se basa Rápido + Simple = "encantamiento del cliente".

El NIST[27] (Instituto Nacional de Normas) Risk Management Guide for Information Technology Systems calculó el valor del gasto por NO invertir en seguridad perimetral con la siguiente formula:

GNIS = W * T * R

Donde:

* W = número de personas afectadas por el daño.
* T = Tiempo de productividad perdido.
* R = Costo por hora promedio de los empleados.

Lo que sería:

GNIS = 10 * 1 * 2000 = $20.000

$20.000 dólares de perdida tomando en cuenta 10 personas de gerencia por un mes.

[27] National Institute of Standards and Technology, promueve la innovación y la competencia industrial de forma que mejoren la estabilidad económica y la calidad de vida.

A continuación, se presenta un cuadro en el cual se muestra el elemento tecnológico, la problemática y la solución o programa actual para su compensación:

Elemento tecnológico	Problemática	Solución o programa
Computadores personales de los empleados	Acceso a reportes, informes, pantallas, pólizas requerido para la operación pero sin monitoreo de las actividades.	El empleado firma un documento de no divulgación de información y existe un comité de ética.
	Salida de información por emails, web, impresión u otro medio extraíble.	USB bloqueadas a través de Active Directory.
	Información descargada de forma masiva en el computador, laptops funcionando fuera de la red de Aseguradora.	Active Directory restringe de cierto modo cambiar las funciones del computador.
Base de datos SQL	Vulnerabilidades de la base.	Se cuenta con un antivirus y firewall lógico. No se tiene acceso a la

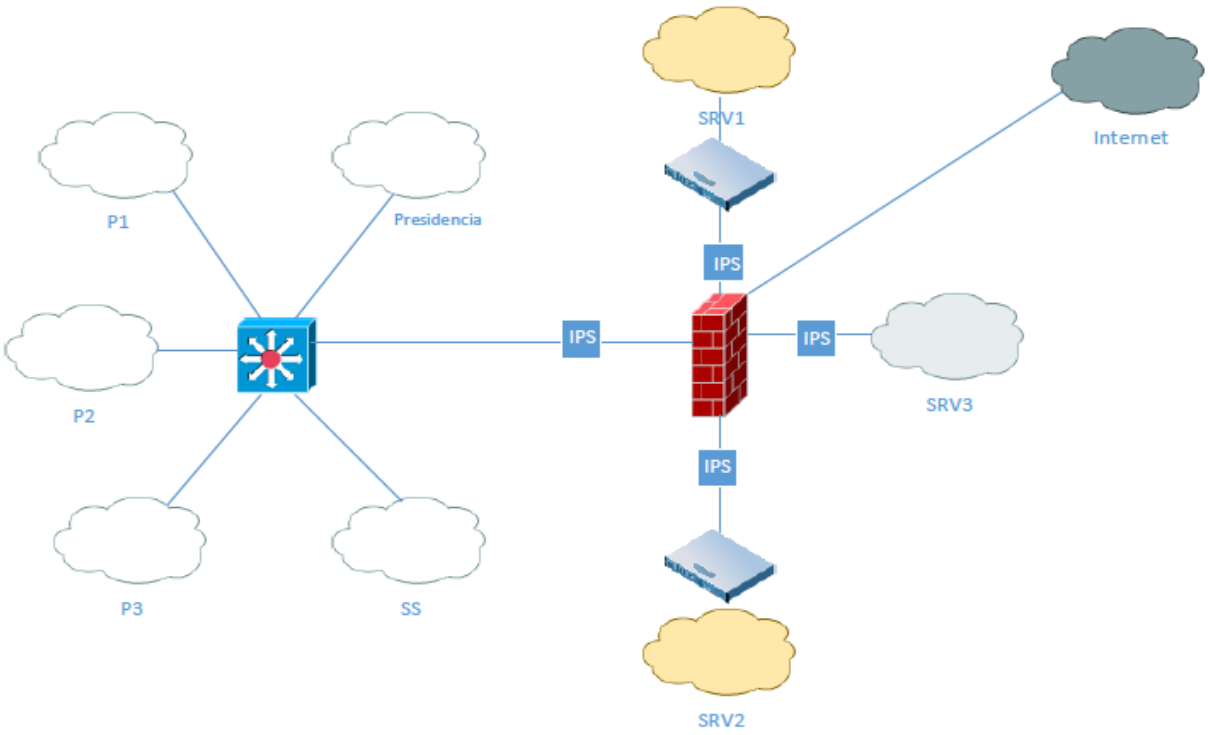
		base, solo la aplicación tiene acceso a la base.
Servidor ORACLE	Ataques directos o indirectos a la red.	Solo se accede a modo consola, bloqueo de puertos no necesarios.
	Modulo SOS, todos los usuarios tienen el ejecutable que accede directamente al Oracle.	Se habilita el acceso a los usuarios dependiendo al proceso que corresponda.
Servidor Virtual Windows 2008 (Aplicaciones del negocio)	Recuperación de desastres en un sitio alterno no se posee Aseguradora.	Manejo de snapshots y replicación de VMWare diario, se cuenta con Data Protector como sistema de cinta tape backup.
	Los usuarios pueden acceder a todo sin restricción.	Se tiene permisos en las capetas compartidas dependiendo al

		proceso que pertenezca el usuario.
	No se maneja ciclos continuos.	Tiene Antivirus, firewall interno, existe perfiles de usuarios para que ingresen los Brokers a ver información restringida.

CAPITULO IV: DISEÑO DEL ESQUEMA DE SEGURIDAD PERIMETRAL PROPUESTO

4.1. Esquema de seguridad perimetral propuesto para Aseguradora del Sur

4.1.1. Topología Ideal



Según los equipos seleccionados en la evaluación de la solución de seguridad perimetral se propone una topología ideal dentro de Aseguradora del Sur, donde sus componentes son:

- Firewall NGFW de nueva generación (CheckPoint 4800 o Palo Alto 3020)
    - Permite a los administradores de la red proporcionar una protección superior en el área perimetral cubre el nivel físico, de enlace de datos hasta la capa 4 (transporte) del modelo OSI, de ataques externos, controla el acceso a los usuarios, sin embargo, con el equipo Next Generation Firewall se puede tener un control hasta capa 7 (aplicación), con los URL filtering, filtrado web, control de aplicaciones, incentivando la productividad de los empleados.

    - IPS de nueva generación

    - Los IPS permiten una prevención proactiva contra intrusos, utilizando base de datos de amenazas actualizadas permitiendo una protección eficiente en la infraestructura de la empresa.

      Se propone contar con equipos IPS dedicados a cada segmento para evitar los accesos dentro de la LAN y proteger independientemente cada segmento LAN, WAN y DMZ, ya que los paquetes son entregados a la aplicación y el Firewall no controla la seguridad en la capa de aplicaciones, de esta forma se tendría seguridad física y lógicamente.

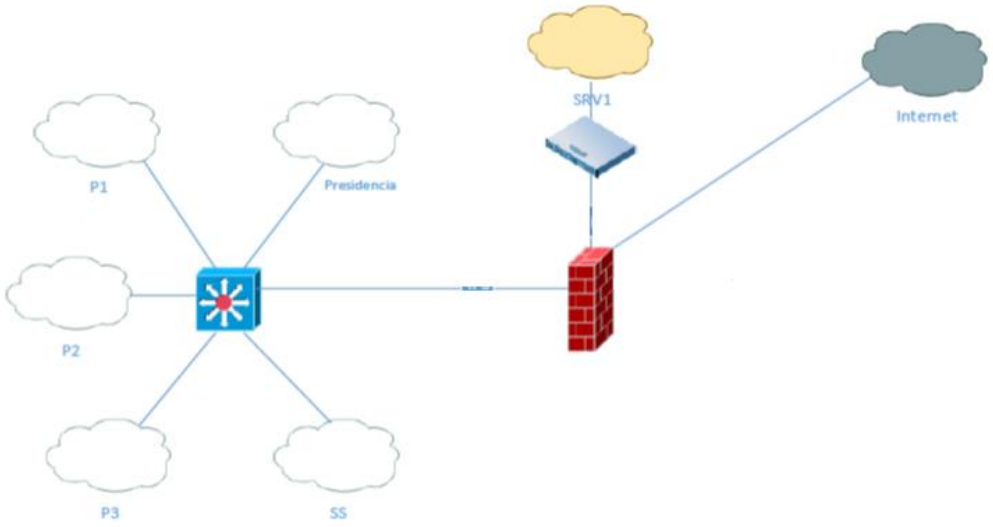
- WAF[28] (Imperva o F5)
    - Protege a todas las aplicaciones web y datos críticos en Aseguradora del Sur, ya que su Core del negocio se encuentra en plataformas web, de esta manera mitiga las posibilidades de downtimes en los servicios en línea o fishing a los usuarios, realiza análisis de vulnerabilidades de aplicaciones web, además genera parches virtuales, cubre la falta de seguridad que deja el Firewall.

- Firewall de base de datos
    - Realiza una auditoria y protección a las bases de datos de Aseguradora del Sur, cubre la necesidad de mantener integra y confiable la información almacenada, alerta y bloquea ataques y actividades no autorizadas en tiempo real. Aplica parches virtuales a las vulnerabilidades de la base de datos Oracle que maneja Aseguradora del Sur.

4.1.2. Topología propuesta

Se propone una topología para Aseguradora del Sur tomando en cuenta factores económicos, servicio de soporte en el país, administración de los equipos, tiempo de respuesta en soporte, instalación y puesta en marcha se presenta la siguiente topología con equipos Next Generation Firewall y Web Application Firewall:

[28] Web Application Firewall, permite proteger los servidores de aplicaciones web de ataques.



Sus componentes serian:

- Next Generation Firewall – CheckPoint 4800 o Palo Alto 3020

El Firewall permite a los administradores controlar de forma segura el acceso a los clientes, servidores y aplicaciones, con una visibilidad detallada de los usuarios, grupos, equipos y tipo de conexión.

Proporciona una protección superior en el área perimetral hasta la capa 4 (transporte) del modelo OSI, cubre de ataques externos, controla el acceso a los usuarios, sin embargo, con el equipo Next Generation Firewall se puede tener un control hasta capa 7 (aplicación), con los URL filtering, control de aplicaciones, incentiva la productividad de los empleados y también ayuda a eliminar los servidores proxy´s que con los que se cuenta actualmente, de esta forma se mejora las conexiones a Internet.

En el Firewall cuenta con IPS, IPSsec VPN, VPN SSL lo cual ayuda a los empleados que trabajan en oficinas externas como por ejemplo concesionarios de vehículos, municipios, entre otros, realiza conexiones seguras y evita la pérdida o manipulación de información.

Con la implementación de un Firewall Next Generation se tendrá un monitoreo continuo y advertencias a detalle de todas las actividades que pasen en la red.

- WAF – Imperva o F5

Se propone la implementación de un equipo WAF para proteger a todas las aplicaciones web y datos críticos en Aseguradora del Sur, debido a que su Core del negocio se encuentra en plataformas web y están expuestas a vulnerabilidades (Visual Time, People Soft, Servicios en línea), de esta manera mitiga las posibilidades de downtimes en los servicios en línea o fishing a los usuarios teniendo una pérdida de información realmente importante para la compañía, de ahí la importancia de un equipo WAF para la protección de dicha información, además ayuda a cubrir la falta de seguridad que deja el Firewall.

- DMZ

Se considera conveniente tener una DMZ para todas las aplicaciones web publicadas como son Visual Time, servicios en línea (Portal), People Soft, los cuales van a estar protegidos por el WAF.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La información que tiene Aseguradora del Sur no está resguardada por ningún mecanismo certero, debido que no es suficiente con políticas o cláusulas de confidencialidad en los contratos a los empleados.

- Luego del análisis realizado en Aseguradora del Sur que se cuenta con varias fallas de seguridad en el aspecto de control de acceso, factor humano y monitoreo en las aplicaciones.

- Los servidores de Aseguradora del Sur poseen vulnerabilidades en el cifrado SSL y permiten bypass de la autenticación.

- Aseguradora del Sur está altamente expuesta a ataques informáticos por su gran porcentaje de vulnerabilidades en sus equipos.

- No es solo necesario contar con un Firewall Next Generation, sino también con un equipo WAF y un equipo Firewall para base de datos.

- En los tres aplicativos analizados (Visual Time, People Soft y servicios en línea) existen vulnerabilidades reales que pueden comprometer a toda la integridad, disponibilidad y confiabilidad de la información, por su

conexión a la base de datos dado que dicha base posee también vulnerabilidades.

- En la actualidad existen muchos cambios simultáneos en la Aseguradora del Sur por lo cual, al no hacer un seguimiento adecuado de toda la seguridad informática a través de herramientas de Seguridad se puede comprometer el éxito y las operaciones en un futuro.

- La presente tesis puede servir a Aseguradora del Sur, como base para la implementación de un sistema de seguridad perimetral en sus instalaciones.

5.2. Recomendaciones

- Implementar una solución de seguridad perimetral con un Next Generation Firewal que tenga funcionalidad de antibot, control de aplicaciones y URL Filtering para facilitar la gestión de la seguridad perimetral. La principal función de este componente será el manejar el control de accesos perimetrales.

- Por la cantidad de servicios no necesarios y la cantidad de vulnerabilidades, se recomienda realizar análisis de vulnerabilidad tanto en la infraestructura como en aplicaciones de manera periódica con un seguimiento de los procesos de remediación a través de métodos cuantificables.

- Implementar una solución que proteja el sistema de archivos en los que se almacena la base de datos y archivos críticos en los servidores de tal forma que se prevenga la fuga de información y se controle el acceso de los usuarios a estos repositorios.

- Es necesario el uso de parches virtuales en base de datos Oracle y en vulnerabilidades tanto en aplicativos como de infraestructura, para lo cual el parche virtual de infraestructura se podría realizar a través de un IPS y el parche virtual para las aplicaciones se debe implementar un WAF creando filtros de bloqueo ante las vulnerabilidades.

- Implementar una solución que resguarde a las nuevas aplicaciones Web que manejaran el Core del negocio (Visual Time, People Soft, Servicios en línea), debido que se es muy vulnerable a ataques de ciber delincuentes, pude arriesgar información sensible o downtimes, siendo esto una pérdida económica alta por cada minuto.

- Es importante al momento de seleccionar un equipo de seguridad verificar su escalabilidad y estar seguro del dimensionamiento, entendiendo y analizando a profundidad el problema de seguridad, para evitar gastos a corto plazo, el presente trabajo de disertación puede servir como referencia o base para la selección del equipo.

- Es importante recordar que hasta la mejor solución de seguridad es inefectiva si no se cuenta con una política de seguridad efectiva con los empleados y el personal que lo administra no tienen los conocimientos necesarios para entender y generar una respuesta ante algún incidente.

- Aseguradora del Sur continuara por los siguientes 2 años manejando el CORE SOS como pieza fundamental en el giro del negocio, junto con Visual Time alimentando la base de datos, se recomienda de manera prioritaria la implementación de un sistema de seguridad perimetral debido a que el SOS tiene una conexión directa cliente – servidor el cual compromete la seguridad e integridad de la base de datos, ya que

actualmente no se cuenta con un monitoreo adecuado para prevenir posibles amenazas.

- Es indispensable contar con una persona capacitada en el manejo de las herramientas que pueda hacer uso de las mismas de una manera adecuada revisando tempranamente cualquier anomalía presentada, registrando y haciendo seguimiento de los incidentes.

BIBLIOGRAFÍA

- Ramos, Xavier. "DPI". *Auben.net*. N.p., 2015. Web. 2 Oct. 2015. http://www.auben.net/index.php/tecnologias/seguridad/dpi

- Inc., Check, and Check Ltd. "Next Generation Firewall For Data/Network Security". *Check Point Software*. N.p., 2015. Web. 20 Nov. 2015.

http://www.checkpoint.com/products-solutions/next-generation-firewalls/index.html

- "ESET Security Report". *ESET* 3 (2015): n. pag. Articulo ESET.

http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

- "Tendencias De Seguridad Cibernética". (2014): n. pag. Web. 1 Jul. 2014.

https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

- Adminso.es,. "4.1.4. Seguridad Perimetral - ASO". N.p., 2015. Web. 13 Aug. 2015.

http://www.adminso.es/index.php/4.1.4._Seguridad_perimetral

- Solusan, "Que Es Una DMZ?". N.p., 2014. Web. 29 Feb. 2014.

http://www.solusan.com/que-es-una-dmz.html

- Unaaldia.hispasec.com,. "Comentarios Sobre Los Antivirus Perimetrales". N.p., 2014. Web. 10 Oct. 2014.

http://unaaldia.hispasec.com/2002/10/comentarios-sobre-los-antivirus.html

- Drupal.org,. "Antibot". N.p., 2013. Web. 8 Sept. 2013.

https://www.drupal.org/project/antibot

- Es.norton.com,. "Bots Y Botnets: Una Amenaza Creciente". N.p., 2015. Web. 19 June 2015. https://www.drupal.org/project/antibot

- Check Point Firewall,. "IPS". N.p., 2015. Web. 17 Oct. 2015. http://www.cpfirewall.com/software-blades/security-gateway-blades/ips/

- Taylor, Jonh. "What Is Data Loss Prevention (DLP)?". *WhatIs.com*. N.p., 2014. Web. 16 July 2014. http://whatis.techtarget.com/definition/data-loss-prevention-DLP

- Symantec.com. "Software Data Loss Prevention (DLP)". N.p., 2015. Web. 18 Mar. 2015. https://www.symantec.com/es/mx/data-loss-prevention/

- Mayler, Mark. "Gartner". *Revista.helpdesktic.com*. N.p., 2015. Web. 5 July 2015. http://revista.helpdesktic.com/cuadrante-magico-de-gartner/

- Hils, Adam, Greg Young, and Jeremy D'Hoinne. "Magic Quadrant For Enterprise Network Firewalls". *Gartner.com*. N.p., 2015. Web. 11 Jan. 2016. https://www.gartner.com/doc/3035319/magic-quadrant-enterprise-network-firewalls

- Rouse, Margaret. "What Is SSL VPN". *SearchSecurity*. N.p., 2013. Web. 30 Feb. 2013. http://searchsecurity.techtarget.com/definition/SSL-VPN

- Dant, Sara. "Palo Alto Networks Vs. Check Point". Blog Smartekh. N.p., 2014. Web. 1 Dec. 2014. http://blog.smartekh.com/palo-alto-networks-vs-check-point/

- Ramos Varón, Antonio Ángel. (2014). Seguridad Perimetral, Monitorización Y Ataques En Redes. España: Ra-Ma Editorial.

➢ ANTIUN. (2013). Seguridad Perimetral (Firewall). 2015, de ANTIUN Sitio web: http://www.antiun.com/servicios-informaticos-it/seguridad-perimetral-firewall

➢ MPSnet. (2014). SEGURIDAD PERIMETRAL. 2015, de MPSnet Sitio web: http://www.mpsnet.com.mx/servicios-administrados/seguridad/perimetral

➢ Alejandro Ramos Fraile. (2011). Seguridad Perimetral. 2015, de intypedia Sitio web: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

➢ Dominio Digital. (2014). Seguridad Perimetral Firewall. 2015, de Dominio Digital Sitio web: http://www.dominiodigital.cl/index.php/productos/seguridad-perimetral-firewall

➢ CISTEC. (2015). Seguridad Perimetral. 2015, de CISTEC Sitio web: http://www.cistec.es/cissecurity/seguridad-perimetral/

➢ NetSecVulns. (2013). Palo Alto Networks vs. Check Point - Did PAN "fix" the Firewall., de NetSecVulns Sitio web: https://www.youtube.com/watch?v=hSCzRfF8ZVQ&feature=youtu.be

➢ NetSecVulns. (2013). Palo Alto Networks vs. Check Point - DLP Comparison., de NetSecVulns Sitio web: https://www.youtube.com/watch?v=8fs8m8-lAp8&feature=youtu.be

➢ NetSecVulns. (2013). Palo Alto Networks vs. Check Point - VPN Management., de NetSecVulns Sitio web: https://www.youtube.com/watch?v=JtAkx694Zc8&feature=youtu.be

- CheckPoint. (2013). Choosing the Right Next Generation Firewall - NGFW Explained., de CheckPoint Sitio web: https://www.youtube.com/watch?v=M98CS6IdDqI&feature=youtu.be

- CheckPoint. (2013). Choosing the Right Next Generation Firewall - Multi-Layer Security., de CheckPoint Sitio web: https://www.youtube.com/watch?v=taKj-LpYl5Y&feature=youtu.be

- EKOS. (Enero 2016). Top Seguridad Perimetral. ComputerWorld, 2, 85.

- Luis Fernando Suarez, (Agosto 2015 – Enero 2016), Información Actual Infraestructura, Aseguradora del Sur – Matriz.

ANEXOS

Anexo 1

Datasheet CheckPoint 4800.

Anexo 2

Datasheet
Palo Alto 3020

Anexo 3

Reporte OpenVas Firewall Aseguradora del Sur.

CHECK POINT 4600 APPLIANCE

CHECK POINT 4600 APPLIANCE

Enterprise-grade security appliances

Product Benefits

- Delivers everything you need to secure your network in one appliance
- Simplify administration with a single integrated management console
- Ensures data security by securing remote access and site-to-site communications
- Extensible with Software Blade Architecture

Product Features

- 405 SecurityPower™
- 3.4 Gbps production firewall throughput
- 630 Mbps production IPS throughput
- Up to 12 10/100/1000Base-T ports
- Up to 4 1GbE Fiber ports

INSIGHTS

Today the enterprise gateway is more than a firewall. It is a security device presented with an ever-increasing number of sophisticated threats. As an enterprise security gateway it must use multiple technologies to control network access, detect sophisticated attacks and provide additional security capabilities like data loss prevention and protection from web-based threats. The proliferation of mobile devices like smartphones and Tablets and new streaming, social networking and P2P applications requires a higher connection capacity and new application control technologies. Finally, the shift towards enterprise private and public cloud services, in all its variations, changes the company borders and requires enhanced capacity and additional security solutions.

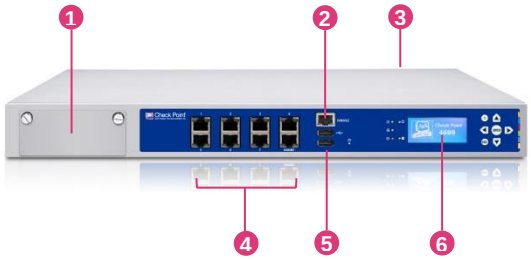
SOLUTION

The Check Point 4600 Appliance delivers everything you need to secure your enterprise network in one appliance. The 4600 combines fast networking technologies with high performance multi-core capabilities - providing the highest level of security without compromising on network speeds to keep your data, network and employees secure.

The Check Point 4600 Appliance offers a complete and consolidated security solution, with leading performance in a 1U form factor. In addition to eight onboard 1 Gigabit copper Ethernet ports, the 4600 also comes with an available expansion slot for the option of adding four 1 Gigabit copper or 2 or 4 fiber Ethernet ports. With 405 SecurityPower Units, real-world firewall throughput of 3.4 Gbps and real-world IPS performance up to 630 Mbps the 4600 is capable of securing any small to mid-size office.

4600

1. Network card expansion slot
2. Console port
3. AC power supply (not shown)
4. 8x10/100/1000Base-T ports
5. USB ports for ISO installation
6. Graphical LCD display



ALL-INCLUSIVE SECURITY SOLUTIONS

The Check Point 4600 Appliances offer a complete and consolidated security solution available in five Next Generation Security Software Blade packages.

Next Generation Firewall (NGFW): identify and control applications by user and scan content to stop threats.
Next Generation Secure Web Gateway (SWG): enables secure use of Web 2.0 with real time protection.
Next Generation Data Protection (NGDP): preemptively protect sensitive information from unintentional loss and educate users on proper data handling policy in real-time.
Next Generation Threat Prevention (NGTP): prevent sophisticated cyber-threats with IPS, Application Control, Antivirus, Anti-Bot, URL Filtering and Email Security.
Next Generation Threat Extraction (NGTX): advanced next-gen zero-day threat prevention, NGTP with Threat Emulation and Threat Extraction

PREVENT UNKNOWN THREATS

Check Point provides complete zero-day threat prevention and alerts when under attack. Threat Extraction delivers zero-malware documents in zero seconds. Threat Emulation inspects files for malicious content in a virtual sandbox. When Threat Emulation discovers new threats, a signature is sent to the Check Point ThreatCloud database which documents and shares information on the newly identified malware with other Check Point customers — providing immediate protection against zero-day threats.

INTEGRATED SECURITY MANAGEMENT

The appliance can either be managed locally with its available integrated security management or via central unified management. Using local management, the appliance can manage itself and one adjacent appliance for high availability purposes.

REMOTE ACCESS CONNECTIVITY

Each appliance arrives with mobile access connectivity for 5 users, using the Mobile Access Blade. This license enables secure remote access to corporate resources from a wide variety of devices including smartphones, tablets, PCs, Mac and Linux.

GAIA—A UNIFIED SECURE OS

Check Point GAiA™ is the next generation Secure Operating System for all Check Point appliances, open servers and virtualized gateways. GAiA secures IPv4 and IPv6 networks utilizing the Check Point Acceleration & Clustering technology and it protects the most complex network environments by supporting dynamic routing protocols like RIP, OSPF, BGP, PIM (sparse and dense mode) and IGMP. As a 64-Bit OS, GAiA increases the connection capacity of select appliances.

GAiA simplifies management with segregation of duties by enabling role-based administrative access. Furthermore, GAiA greatly increases operation efficiency by offering Automatic Software Updates. The intuitive and feature-rich Web interface allows for instant search of any commands or properties.

SPECIFICATIONS

PERFORMANCE

Production Performance[1]

- 405 SecurityPower
- 3.4 Gbps firewall throughput
- 630 Mbps firewall and IPS throughput

RFC 3511, 2544, 2647, 1242 PERFORMANCE (LAB)

- 9 Gbps firewall, 1518 byte UDP
- 1.5 Gbps VPN, AES-128
- 30,000 max IPsec VPN tunnels
- 1 Gbps IPS, Recommended IPS profile, IMIX traffic blend
- 1.2 million concurrent connections, 64 byte HTTP response
- 50,000 connections per second, 64 byte HTTP response

EXPANSION OPTIONS

Base Configuration

- 8 x 10/100/1000Base-T RJ45 ports
- 250 GB hard disk drive
- One AC power supply
- Standard rack mount

Network Expansion Slot Options (1 slot)

- 4 x 10/100/1000Base-T RJ45 ports
- 2 x 1000Base-F SFP ports
- 4 x 1000Base-F SFP ports
- 4 x 10/100/1000Base-T Fail-Open NIC
- 4 x 1000Base-F SX or LX Fail-Open NIC

Max Configuration

- 12 x 10/100/1000Base-T RJ45 ports
- 8 x 10/100/1000Base-T RJ45 + 4 x 1000Base-F SFP ports

Virtual Systems

- Max VSs: 10

NETWORK

Network Connectivity

- IPv4 and IPv6
- 1024 interfaces or VLANs per system
- 4096 interfaces per system (in Virtual System mode)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

CLUSTERING

High Availability

- Active/Active - L3 mode
- Active/Passive - L3 mode
- Session synchronization for firewall and VPN
- Session failover for routing change
- Device failure detection
- Link failure detection
- ClusterXL or VRRP

PHYSICAL

Power Requirements

- AC Input Voltage: 100 - 240V
- Frequency: 50 - 60 Hz
- Single Power Supply Rating: 250 W
- Power Consumption Maximum: 90 W
- Maximum thermal output: 240.1 BTU

Dimensions

- Enclosure: 1U
- Standard (W x D x H): 17.25 x 12.56 x 1.73 in.
- Metric (W x D x H): 438 x 320 x 44 mm
- Weight: 7.5 kg (16.53 lbs.)

Operating Environmental Conditions

- Temperature: 32° to 104°F / 0° to 40°C
- Humidity: 20%-90% (non-condensing)

Storage Conditions

- Temperature: –4° to 158°F / –20° to 70°C
- Humidity: 5% to 95% @60°C

Certifications

- Safety: CB, UL/cUL, CSA, TUV, NOM, CCC, IRAM, PCT/GoST
- Emissions: FCC, CE, VCCI, C-Tick, CCC, ANATEL, KCC
- Environmental: RoHS

[1] Check Point's SecurityPower is a new benchmark metric that allows customers to select security appliances by their capacity to handle real-world network traffic, multiple security functions and a typical security policy.

APPLIANCE PACKAGES

BASE CONFIGURATION[1]	
4600 Next-Gen Firewall (with FW, VPN, ADNC, IA, MOB-5, IPS and APCL) bundled with local management for up to 2 gateways	CPAP-SG4600-NGFW
4600 Secure Web Gateway (with FW, VPN, ADNC, IA, APCL, AV and URLF) bundled with local management and SmartEvent for up to 2 gateways	CPAP-SWG4600
4600 Next-Gen Data Protection (with FW, VPN, ADNC, IA, MOB-5, IPS, APCL, and DLP) bundled with local management for up to 2 gateways	CPAP-SG4600-NGDP
4600 Next-Gen Threat Prevention (with FW, VPN, ADNC, IA, MOB-5, IPS, APCL, URLF, AV, ABOT and ASPM) bundled with local management for up to 2 gateways	CPAP-SG4600-NGTP
4600 Next-Gen Threat Extraction (with FW, VPN, ADNC, IA, MOB-5, IPS, APCL, URLF, AV, ABOT, ASPM, TE and TEX) bundled with local management for up to 2 gateways	CPAP-SG4600-NGTX
4600 Next-Gen Firewall Appliance with 5 Virtual Systems	CPAP-SG4600-NGFW-VS5
4600 Next-Gen Firewall Appliance Bundle, one primary and one HA, with 5 VS	CPAP-SG4600-NGFW-VS5-2

[1] High Availability (HA) and SKUs for 2 and 3 years are available, see the online Product Catalog

SOFTWARE BLADE PACKAGES

SOFTWARE BLADE PACKAGES[1]	
4600 Next-Gen Firewall Software Blade package for 1 year (IPS and APCL)	CPSB-NGFW-4600-1Y
4600 Secure Web Gateway Software Blade package for 1 year (APCL, AV and URLF)	CPSB-SWG-4600-1Y
4600 Next-Gen Data Protection Software Blade package for 1 year (IPS, APCL, and DLP)	CPSB-NGDP-4600-1Y
4600 Next-Gen Threat Prevention Software Blade package for 1 year (IPS, APCL, URLF, AV, ABOT and ASPM)	CPSB-NGTP-4600-1Y
4600 Next-Gen Threat Extraction Software Blade package for 1 year (IPS, APCL, URLF, AV, ABOT, ASPM, TE and TEX)	CPSB-NGTX-4600-1Y
SOFTWARE BLADES[1]	
Check Point Mobile Access Blade for 50 concurrent connections	CPSB-MOB-50
Data Loss Prevention Blade for 1 year (for up to 500 users, up to 15,000 mails per hour and max throughput of 700 Mbps)	CPSB-DLP-500-1Y
Check Point IPS blade for 1 year	CPSB-IPS-1Y
Check Point Application Control blade for 1 year	CPSB-APCL-S-1Y
Check Point URL Filtering blade for 1 year	CPSB-URLF-S-1Y
Check Point Antivirus Blade for 1 year	CPSB-AV-S-1Y
Check Point Anti-Spam & Email Security Blade for 1 year	CPSB-ASPM-S-1Y
Check Point Anti-Bot blade for 1 year - for ultra-high-end appliances and pre-defined systems	CPSB-ABOT-S-1Y

[1] SKUs for 2 and 3 years are available, see the online Product Catalog

VIRTUAL SYSTEM PACKAGES	
10 Virtual Systems package	CPSB-VS-10
10 Virtual Systems package for HA/VSLS	CPSB-VS-10-VSLS
3 Virtual Systems package	CPSB-VS-3
3 Virtual Systems package for HA/VSLS	CPSB-VS-3-VSLS

ACCESSORIES

INTERFACE CARDS AND TRANSCEIVERS	
4 Port 10/100/1000 Base-T RJ45 interface card	CPAC-4-1C
2 Port 1000Base-F SFP interface card; requires SFP transceivers per port	CPAC-2-1F
4 Port 1000Base-F SFP interface card; requires 1000Base SFP transceivers per port	CPAC-4-1F
SFP transceiver module for 1G fiber ports - long range (1000Base-LX)	CPAC-TR-1LX
SFP transceiver module for 1G fiber ports - short range (1000Base-SX)	CPAC-TR-1SX
SFP transceiver to 1000 Base-T RJ45 (Copper)	CPAC-TR-1T
BYPASS CARD	
4 Port 1GE short-range Fiber Bypass (Fail-Open) interface card (1000Base-SX)	CPAC-4-1FSR-BP
4 Port 1GE long-range Fiber Bypass(Fail-Open) interface card (1000Base-LX)	CPAC-4-1FLR-BP
Port 1GE copper Bypass (Fail-Open) interface card (10/100/1000 Base-T)	CPAC-4-1C-BP
SPARES AND MISCELLANEOUS	
Slide rails for 4000 and 12000 Appliances (22”-32”)	CPAC-RAIL
Extended slide rails for 4000 and 12000 Appliances (26”-36”)	CPAC-RAIL-EXT

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

Serie PA-3000

Características principales de los firewalls de nueva generación de la serie PA-3000:

CLASIFICACIÓN DE LA TOTALIDAD DE LAS APLICACIONES, EN TODOS LOS PUERTOS, EN TODO MOMENTO CON APP-ID™.

- Identificación de la aplicación, independientemente del puerto, el tipo de cifrado (SSL o SSH) o la técnica evasiva empleada.
- Utilización de la aplicación, no del puerto, como base para todas las decisiones sobre políticas de habilitación segura: permitir, denegar, programar, inspeccionar, aplicar control de tráfico.
- Clasificación de las aplicaciones no identificadas por medio de políticas, investigación forense de amenazas, creación personalizada de App-ID o captura de paquetes para investigaciones posteriores.

PROPAGACIÓN DE LAS POLÍTICAS DE HABILITACIÓN SEGURA DE APLICACIONES A CUALQUIER USUARIO, EN CUALQUIER UBICACIÓN, CON USER-ID™ Y GLOBALPROTECT™.

- Integración sin agente con Active Directory, LDAP, eDirectory Citrix y Microsoft Terminal Services.
- Integración con NAC, redes inalámbricas y otros repositorios de usuarios no estándar a través de una API XML.
- Implementación de políticas coherentes a usuarios en plataformas Microsoft Windows, Mac OS X, Linux, Android o iOS independientemente de su ubicación.

PROTECCIÓN CONTRA TODAS LAS AMENAZAS, TANTO CONOCIDAS COMO DESCONOCIDAS, CON CONTENT-ID™ Y WILDFIRE™.

- Bloqueo de una amplia gama de amenazas conocidas, como exploits, malware y spyware, en todos los puertos, independientemente de las tácticas comunes de evasión de amenazas utilizadas.
- Limitación de la transferencia no autorizada de archivos y datos sensibles, así como control de la navegación web no relacionada con el trabajo.
- Identificación de malware desconocido, incluyendo el análisis de más de 100 comportamientos maliciosos, así como la generación y distribución de protección automática en la siguiente actualización disponible.

paloalto NETWORKS
the network security company™


PA-3050


PA-3020

La serie PA-3000 de Palo Alto Networks™ se compone de dos plataformas de alto rendimiento: PA-3050 y PA-3020, que están destinadas a implementaciones de gateways de Internet de alta velocidad. La serie PA 3000 gestiona el flujo de tráfico de red utilizando recursos de computación dedicados para el networking, la seguridad, la prevención de amenazas y la gestión.

El backplane de alta velocidad está dividido en un plano para datos y otro para control, garantizando siempre la disponibilidad del acceso a la gestión independientemente de la carga de tráfico. El elemento de control del firewall de nueva generación PA-3000 es PAN-OS™, un sistema operativo orientado específicamente a la seguridad que permite a las organizaciones la habilitación segura de aplicaciones utilizando App-ID, User-ID, Content-ID, GlobalProtect y WildFire.

RENDIMIENTO Y CAPACIDAD[1]	PA-3050	PA-3020
Rendimiento del firewall (con función App-ID)	4 Gbps	2 Gbps
Rendimiento de la prevención contra amenazas	2 Gbps	1 Gbps
Rendimiento de VPN IPSec	500 Mbps	500 Mbps
Número de sesiones nuevas por segundo	50.000	50.000
Número máximo de sesiones	500.000	250.000
Interfaces de túnel/túneles VPN IPSec	2.000	1.000
Usuarios simultáneos GlobalProtect (SSL VPN)	2.000	1.000
Sesiones de descifrado SSL	15.360	7.936
Certificados para SSL entrante	25	25
Routers virtuales	10	10
Sistemas virtuales (base/máx.[2])	1/6	1/6
Zonas de seguridad	40	40
Número máximo de políticas	5.000	2.500

[1] El rendimiento y la capacidad se miden en condiciones de prueba ideales usando PAN-OS 5.0.

[2] Si se añaden sistemas virtuales a la cantidad base, será necesario adquirir una licencia por separado.

Para una descripción completa de las características de los firewalls de nueva generación de la serie PA-3000, visite www.paloaltonetworks.com/literature.

ESPECIFICACIONES DEL HARDWARE

E/S

- (12) 10/100/1000, (8) puertos SFP ópticos Gigabit

GESTIÓN DE E/S

- (1) puerto de administración fuera de banda 10/100/1000, (2) alta disponibilidad 10/100/1000, (1) puerto de consola RJ-45

CAPACIDAD DE ALMACENAMIENTO

- Unidad de estado sólido (SSD) de 120 GB

FUENTE DE ALIMENTACIÓN (CONSUMO ELÉCTRICO MEDIO/MÁXIMO)

- 250 W (150 / 200)

BTU/H MÁXIMO

- 683

VOLTAJE DE ENTRADA (FRECUENCIA DE ENTRADA)

- 100-240 VAC (50-60 Hz)

CONSUMO MÁXIMO DE CORRIENTE

- 2A a 100 VAC

PREPARADO PARA MONTAJE EN BASTIDOR (DIMENSIONES)

- 1U, bastidor estándar de 19" (4,45 x 43,18 x 43,18 cm – 1,75 x 17 x 16.75 pulgadas)

DIMENSIONES (SOLO DISPOSITIVO/DISPOSITIVO PREPARADO PARA ENVÍO)

- 6,8 Kg / 9,07 Kg

SEGURIDAD

- UL, CUL, CB

INTERFERENCIA ELECTROMAGNÉTICA

- Clase A de FCC, Clase A de CE, Clase A de VCCI, TUV

CERTIFICACIONES

- ICSA

ENTORNO

- Temperatura de funcionamiento: De 0 a 50 ºC (de 32 a 122 ºF)
- Temperatura de almacenamiento: De -20 a 70 ºC (de -4 a 158 ºF)

CONEXIÓN A RED

MODOS DE LOS INTERFACES

- L2, L3, Tap, Virtual Wire (modo transparente)

ENRUTAMIENTO

- Modos: OSPF, RIP, BGP, estático
- Tamaño de la tabla de reenvío (entradas por dispositivo/por VR): 5.000/2.500 (PA-3050), 2.500/2.500 (PA-3020)
- Reenvío basado en políticas
- Protocolo punto a punto sobre Ethernet (PPPoE)
- Tramas Jumbo: tamaño máximo de trama de 9.210 bytes
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, y v3

ALTA DISPONIBILIDAD

- Modos: Activo/Activo, Activo/Pasivo
- Detección de fallos: monitorización de ruta, monitorización de interfaz

ASIGNACIÓN DE DIRECCIONES

- Asignación de direcciones por dispositivo: cliente DHCP/PPPoE/Estática
- Asignación de direcciones por usuarios: servidor DHCP/Relay DHCP/Estática

IPV6

- L2, L3, Tap, Virtual Wire (modo transparente)
- Funciones: App-ID, User-ID, Content-ID, WildFire y descifrado SSL

VLAN

- Etiquetas VLAN 802.1q por dispositivo / por interfaz: 4,094/4,094
- Número máximo de interfaces: 2.048 (PA-3050), 1.024 (PA-3020)
- Interfaces de agregado (802.3ad)

NAT/PAT

- Número máximo de reglas NAT: 1.000
- Número máximo de reglas NAT (DIPP): 200
- Intervalo de direcciones IP y puertos dinámicos: 254
- Intervalo de direcciones IP dinámicas: 16,234
- Modos NAT: NAT 1:1, NAT n:n, NAT m:n
- Sobresuscripción DIPP (direcciones IP de destino único por dirección IP y puerto de origen): 2
- NAT64

VIRTUAL WIRE

- Número máximo de Virtual Wires: 10
- Tipos de interfaz asignados a Virtual Wires: físicos y subinterfaces

REENVÍO DE NIVEL 2

- Tamaño de tabla ARP por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)
- Tamaño de tabla MAC por dispositivo: 2.500 (PA-3050), 1500 (PA-3020)
- Tamaño de tabla de vecino de IPV6: 2.500 (PA-3050), 1500 (PA-3020)

SEGURIDAD

FIREWALL

- Control de las aplicaciones, los usuarios y los contenidos basado en políticas
- Protección de paquetes fragmentados
- Protección de escaneos de reconocimiento
- Protección frente a denegación de servicio (DoS) y denegación de servicio distribuido (DDoS)
- Descifrado: SSL (entrante y saliente), SSH

WILDFIRE

- Identifica y analiza archivos específicos y desconocidos pudiendo reconocer más de 100 conductas maliciosas.
- Genera y ofrece una protección automática contra malware recién descubierto a través de actualizaciones de firmas.
- Distribución de actualizaciones de firmas en menos de 1 hora. Logging y generación de informes integrado. Acceso a la API de WildFire para el envío programado de hasta 100 muestras al día y de hasta 250 consultas al día de informes por archivo hash (se requiere suscripción).

FILTRADO DE ARCHIVOS Y DATOS

- Transferencia de archivos: control bidireccional sobre más de 60 tipos de archivo únicos
- Transferencia de datos: control bidireccional sobre la transferencia no autorizada de números de tarjetas de crédito y seguridad social
- Protección contra descargas "drive-by download"

INTEGRACIÓN DE USUARIOS (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One y otros directorios basados en LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- API XML para facilitar la integración con repositorios de usuario no estándar

VPN IPSEC (SITE-TO-SITE)

- Intercambio de claves: clave manual, IKE v1
- Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)
- Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Creación de túneles VPN dinámicos (GlobalProtect)

PREVENCIÓN DE AMENAZAS (SE REQUIERE SUSCRIPCIÓN)

- Protección contra exploits de vulnerabilidades del sistema operativo y de aplicaciones
- Protección basada en flujos contra virus, spyware y gusanos (incluidos los incrustados en HTML, Javascript, archivos PDF y archivos comprimidos)

FILTRADO DE URL (SE REQUIERE SUSCRIPCIÓN)

- Categorías de URL predefinidas y personalizadas
- Memoria caché para las URL a las que se ha accedido recientemente
- Categorías de URL como parte del criterio de coincidencia de las políticas de seguridad
- Información del tiempo de navegación

CALIDAD DEL SERVICIO (QOS)

- Control del tráfico basado en políticas por aplicación, usuario, origen, destino, interfaz, túnel de VPN IPSec, etc.
- 8 clases de tráfico con parámetros de ancho de banda garantizado, máximo y prioritario
- Supervisión de ancho de banda en tiempo real
- Por marcado de Diffserv de política
- Interfaces físicas compatibles con QoS: 6

VPN/ACCESO REMOTO SSL (GLOBALPROTECT)

- Gateway GlobalProtect
- Portal GlobalProtect
- Transporte: IPSec con SSL fall-back
- Autenticación: LDAP, SecurID o base de datos local
- Sistema operativo cliente: Mac OS X 10.6, 10.7 (32/64 bits), 10.8 (32/64 bits), Windows XP, Windows Vista (32/64 bits), Windows 7 (32/64 bits)
- Soporte de cliente de terceros: Apple iOS, Android 4.0 y posterior, VPNC IPSec para Linux

ADMINISTRACIÓN, GENERACIÓN DE INFORMES, HERRAMIENTAS DE VISIBILIDAD

- Interfaz web integrada, CLI o administración central (Panorama)
- Interfaz de usuario en varios idiomas
- Syslog, Netflow v9 y SNMP v2/v3
- REST API basada en XML
- Resumen gráfico de aplicaciones, categorías de URL, amenazas y datos (ACC)
- Visualizar, filtrar y exportar tráfico, amenazas, WildFire, URL y registros de filtrado de datos
- Generación de informes totalmente personalizable

Para una descripción completa de las características de los firewalls de nueva generación de la serie PA-3000, visite www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com

Scan Report

January 20, 2016

Summary

This document reports on the results of an automatic security scan. The scan started at Wed Jan 20 02:09:47 2016 UTC and ended at Wed Jan 20 02:49:38 2016 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.16.1.10	0	0	1	8	0
Total: 1	0	0	1	8	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 9 results selected by the filtering described above. Before filtering there were 9 results.

2 Results per Host

2.1 172.16.1.10

Host scan start Wed Jan 20 02:09:52 2016 UTC
Host scan end Wed Jan 20 02:49:38 2016 UTC

Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
general/CPE-T	Log
22/tcp	Log
111/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: Relative IP Identification number change

Summary

```
The remote host uses non-random IP IDs, that is, it is
possible to predict the next value of the ip_id field of
the ip packets sent by this host.
An attacker may use this feature to determine traffic patterns
within your network.   A few examples (not at all exhaustive) are:
```

... continues on next page ...

... continued from previous page ...

1. A remote attacker can determine if the remote host sent a packet
in reply to another request. Specifically, an attacker can use your
server as an unwilling participant in a blind portscan of another
network.
2. A remote attacker can roughly determine server requests at certain
times of the day. For instance, if the server is sending much more
traffic after business hours, the server may be a reverse proxy or
other remote access device. An attacker can use this information to
concentrate his/her efforts on the more critical machines.
3. A remote attacker can roughly estimate the number of requests that
a web server processes over a period of time.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10201

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Contact your vendor for a patch

Vulnerability Detection Method
Details:Relative IP Identification number change
OID:1.3.6.1.4.1.25623.1.0.10201
Version used: $Revision: 1048 $

[return to 172.16.1.10]

2.1.2 Log general/tcp

Log (CVSS: 7.8)
NVT: 3com switch2hub

Summary
The remote host is subject to the
switch to hub flood attack.
Description :
The remote host on the local network seems to be connected
through a switch which can be turned into a hub when flooded
by different mac addresses.
The theory is to send a lot of packets (> 1000000) to the
port of the switch we are connected to, with random mac

... continues on next page ...

... continued from previous page ...

addresses. This turns the switch into learning mode, where
traffic goes everywhere.
An attacker may use this flaw in the remote switch
to sniff data going to this host
Reference :
http://www.securitybugware.org/Other/2041.html

OID of test routine: 1.3.6.1.4.1.25623.1.0.80103

Vulnerability Detection Result
Fake IP address not specified. Skipping this check.

Solution
Lock Mac addresses on each port of the remote switch or
buy newer switch.

Vulnerability Detection Method
Details:3com switch2hub
OID:1.3.6.1.4.1.25623.1.0.80103
Version used: $Revision: 15 $

Log (CVSS: 0.0)
NVT: OS fingerprinting

Summary
This script performs ICMP based OS fingerprinting (as described by
Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine
remote operating system version.

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

Vulnerability Detection Result
ICMP based OS fingerprint results: (70% confidence)
HP JetDirect

Log Method
Details:OS fingerprinting
OID:1.3.6.1.4.1.25623.1.0.102002

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 43 $

References

Other:
URL:http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0)
NVT: Traceroute

Summary

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Vulnerability Detection Result

Here is the route from 192.168.5.128 to 172.16.1.10:
192.168.5.128
172.16.1.10

Solution

Block unwanted packets from escaping your network.

Log Method

Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 975 $

[return to 172.16.1.10]

2.1.3 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

... continues on next page ...

... continued from previous page ...

Summary
This routine uses information collected by other routines about
CPE identities (http://cpe.mitre.org/) of operating systems, services and
applications detected during the scan.

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

Vulnerability Detection Result
172.16.1.10|cpe:/a:openbsd:openssh:4.3
172.16.1.10|cpe:/h:hp:jetdirect

Log Method
Details:CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 314 $

[return to 172.16.1.10]

2.1.4 Log 22/tcp

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote
SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

Vulnerability Detection Result
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0

Log Method
Details:SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259

... continues on next page ...

. . . continued from previous page . . .

Version used: $Revision: 43 $

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Vulnerability Detection Result

```
Detected SSH server version: SSH-2.0-OpenSSH_4.3
Remote SSH supported authentication: none,password,publickey,hostbased,keyboard-
↪interactive
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.3
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

Solution

Apply filtering to disallow access to this port from untrusted hosts

Log Method

Details:SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: $Revision: 971 $

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on

. . . continues on next page . . .

... continued from previous page ...

another port than 80 and set the results in the plugins
knowledge base.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Vulnerability Detection Result
An ssh server is running on this port

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 69 $

[return to 172.16.1.10]

2.1.5 Log 111/tcp

Log (CVSS: 0.0)
NVT: rpcinfo -p

Summary
This script calls the DUMP RPC on the port mapper, to obtain the
list of all registered programs.

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

Vulnerability Detection Result
These are the registered RPC programs:\
\
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100024 version 1 'status' on port 673/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100024 version 1 'status' on port 670/UDP

Log Method
Details:rpcinfo -p

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.11111
Version used: $Revision: 41 $

[return to 172.16.1.10]
