ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación.

Maestría en Seguridad Informática Aplicada.

"EVALUACIÓN E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PERIMETRAL PARA UNA INSTITUCIÓN PÚBLICA MUNICIPAL."

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

INGRID DEL CONSUELO PARRALES MORALES

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A Dios por ser mi guía y ayudarme a cumplir todas las metas que me he propuesto.

A mi madre por su amor, su apoyo incondicional y por estar junto a mí en cada momento de mi vida.

A mis amigos porque me ayudaron a levantar y a enfrentar uno de los momentos más difíciles de mi vida, y gracias a ellos pude continuar con mis estudios de maestría.

DEDICATORIA

Para Dios, mi madre la Sra. Juanita Morales y en especial para mi amado padre el Sr. Vicente Parrales ✞, ya que este era su mayor sueño, y es la razón fundamental por quien me he esforzado y he podido culminar mis estudios superiores, aunque no lo vea, sé que está conmigo como mi ángel que me protege y me acompaña siempre, sé que está feliz y orgulloso por mis logros alcanzados.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenín Freire

DIRECTOR MSIA

_____

Mgs. Laura Ureta

PROFESOR DELEGADO

POR LA UNIDADACADÉMICA

_____

Mgs. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDADACADÉMICA

RESUMEN

Proteger la red local de todas las oficinas que pertenecen a la institución pública Municipal del cantón Daule, controlar el ancho de banda para evitar el abuso del personal con el mal uso del internet.

El objetivo es implementar un dispositivo físico más el software especializado para la protección de toda la red informática del Gobierno Autónomo Descentralizado Ilustre Municipalidad del Cantón Daule, ya que en la actualidad no cuenta con un esquema robusto de seguridad informática contra los distintos tipos ataques externos existentes.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BSD	Distribución de Software Berkeley
Dashboard:	Tablero de instrumentos.
DNS:	Domain Name Server. Traducción automática de direcciones de internet a direcciones IP.
Firewall	Pared de Fuego.
FreeBSD	Sistema operativo libre para computadores con CPU basados en la Arquitectura Intel.
G.A.D.I.	Gobierno Autónomo Descentralizado Ilustre
IDS	Sistema de Detección de Intrusos
IPS	Sistema de Prevención de Intrusos.
LAN	Red de área local.
Portal Cautivo	Página Web que se muestra cuando se abre el navegador de internet.
Packetfilter	Define una forma de filtrar paquetes para atributos particulares.
Servidor Proxy	Es un ordenador que sirve de intermediario entre un navegador web e internet.

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El siguiente proyecto tiene como objetivo la evaluación y selección de un equipo de seguridades informáticas para ser implementado como componente de protección perimetral de la red informática del Gobierno Autónomo Descentralizado Ilustre Municipalidad del Cantón Daule. Por ser una institución pública, la adquisición de equipos y software no es inmediata ya que tiene que pasar por algunos procesos internos; por esta razón, se presenta como medida de protección inmediata la implementación un firewall de libre distribución, cuyo nombre es “PFSENSE”, ya que es una herramienta muy útil y cumple con las funcionalidades básicas necesarias.

Se realizará la presentación de los equipos de seguridades de algunas empresas líderes en el mercado, cada uno con sus características y funcionalidades para hacer el análisis y evaluación para luego hacer la selección del que equipo o software que se recomienda sea adquirido para protección de toda la red de datos y para toda la información que administra esta Institución Pública.

CAPÍTULO 1

GENERALIDADES.

1.1 Descripción del Problema.

El G.A.D.I. Municipalidad del Cantón Daule, actualmente no cuenta con un esquema de protección de intrusos ni de seguridad perimetral, siendo una empresa pública debería tener por lo menos un nivel mínimo de seguridad para la red de datos y para toda la información que administra tanto en la cabecera cantonal como en la sede alterna y todas las demás oficinas que se encuentran ubicadas en diferentes lugares del cantón; por lo que la probabilidad de sufrir un ataque externo es muy alta, debido a que sería fácil el acceso desde cualquier red externa, lo cual conduce en un problema muy serio ya que pone en

riesgo la confidencialidad e integridad de la información y la infraestructura del DATA CENTER de la Institución Municipal.

En la actualidad sólo cuenta con un servidor proxy para la conexión a internet y la protección básica del firewall que viene por default en Windows.

Es común en nuestro país que existan muchas empresas e instituciones que no le den la importancia que requiere la seguridad de la información; esto se debe a que todavía es considerada como un gasto y no como inversión. Solamente cuando se presenta un ataque informático o existe perdida de información es que se empieza a pensar en un esquema de seguridad informática.

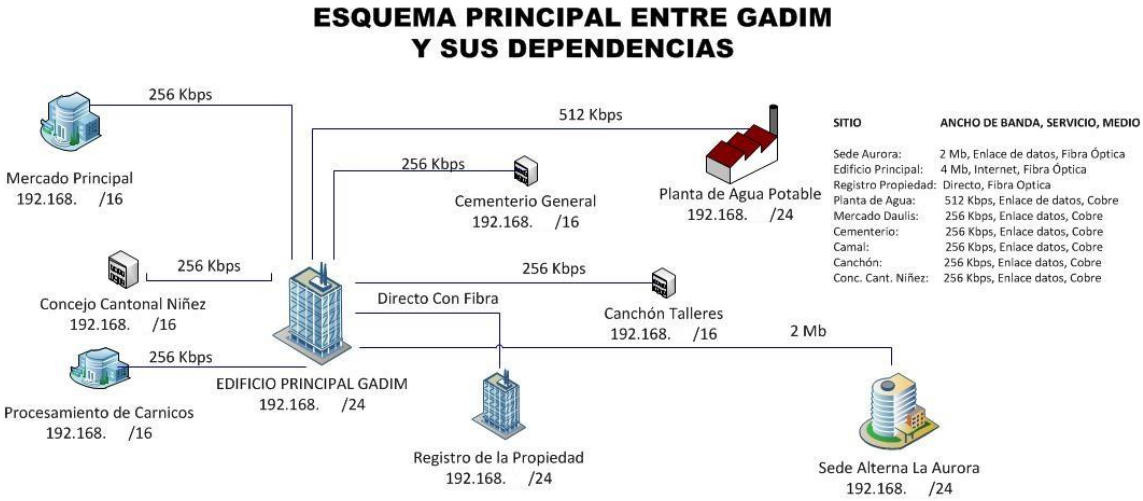

Figura 1.1.- Esquema de las Oficinas del G.A.D.I.M. del Cantón Daule.

1.2 Solución Propuesta.

Realizar el análisis y evaluación de los equipos de seguridad de varias empresas líderes en el mercado para que uno de los equipos de seguridades que ellos ofertan, sea adquirido e implementado como firewall perimetral para que cumpla con todas las necesidades de seguridad de la institución municipal. Por tratarse de una institución Pública la adquisición de los equipos tomará su tiempo por los procesos internos que se deben cumplir para la compra de equipos nuevos; razón por la cual, pensando que la información no puede estar desprotegida, como medida de solución inmediata se implementará el “PFSENSE”, que es un firewall gratuito con grandes capacidades, una herramienta muy útil, que trabaja muy bien en muchas áreas.

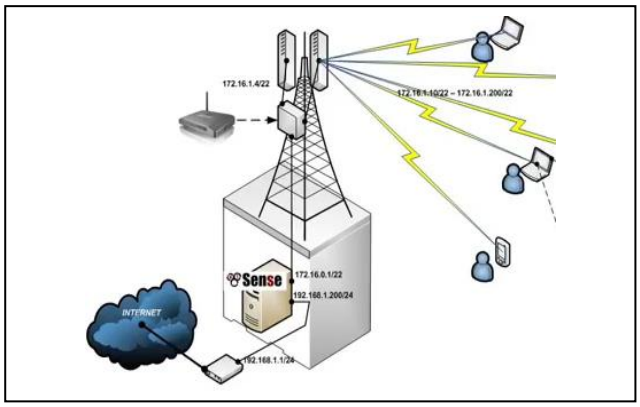

Figura 1.2.- Esquema de Protección para el G.A.D.I.M. del Cantón Daule

1.3 Definiciones Generales.

1.3.1. ¿Qué es el PFSENSE?

El software “PFSENSE”, es una distribución personalizada de FreeBSD, FreeBSD es un sistema operativo libre para computadores con CPU basados en la Arquitectura Intel)adoptado para su uso como Firewall y Router[1], se caracteriza por ser un software de código abierto basado enfiltrado de paquetes, puede ser instalado en una gran variedad de ordenadores y cuenta con una interfaz web sencilla para su configuración, trabaja muy bien en muchas áreas, tales como para la publicación de servidores en interfaces desmilitarizadas (DMZ) y para el control del ancho de banda de redes para las empresas, por lo general las empresas tienen problemas con el abuso del uso del internet por parte del personal, por eso necesitan establecer políticas de seguridad de acceso, de ancho de banda, etc.

Puede funcionar como núcleo de la red, como servidor proxy, como servidor DHCP, reenviador DNS, reenviador NTP, WoL y Access Point también tiene opciones de portal cautivo. Posee funciones de VPN ya que soporta protocolos como IPSec, L2TP, OpenVPN y PPtP, además

soporta NAT1:1 y es muy flexible en NAT saliente. Soporta MultiWAN para Balanceo de cargas y FailOver.

Se puede expandir por medio de módulos o paquetes Servidor Proxy reverso (como alternativa a ISA Server para acceder a Exchange OWA), Asterik para funcionar como Central IP, Antivirus a nivel de Gateway, Filtro AntiSPAM para protección de los servidores de correo, Servidor RADIUS y muchísimas otras funciones.

Como firewall es sumamente flexible, ya que puede trabajar con ALIAS, los cuales facilitan el trabajo con grupos de direcciones IP y dominios.

1.3.2. Características principales del PFSENSE

- Firewall
- Network Address Translation (NAT)
- Balanceo de Carga
- VPN que puede ser desarrollado en IPSec, OpenVPN, y en PPTP.
- Servidor DNS.
- Portal Cautivo.
- Servidor DHCP.
- Gestor de Paquete de datos para ampliar funcionalidades.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.

2.1.- Levantamiento de Información.

El G.A.D.I. Municipalidad del Cantón Daule además de las dependencias que se encuentran en el edificio municipal, tiene a su cargo las siguientes oficinas: Registro de la Propiedad, Sede en Aurora, Mercado Municipal, Canchón, Camal, Cementerio y Planta de Agua, las cuales se encuentran ubicadas en diferentes lugares de la ciudad, en cada una de estas dependencias existe un ruteador, el cual se conecta con el Servidor Proxy para la conexión a internet y se establece la protección básica del firewall que viene por default en Windows. El actual proveedor para el servicio de internet es CNT.

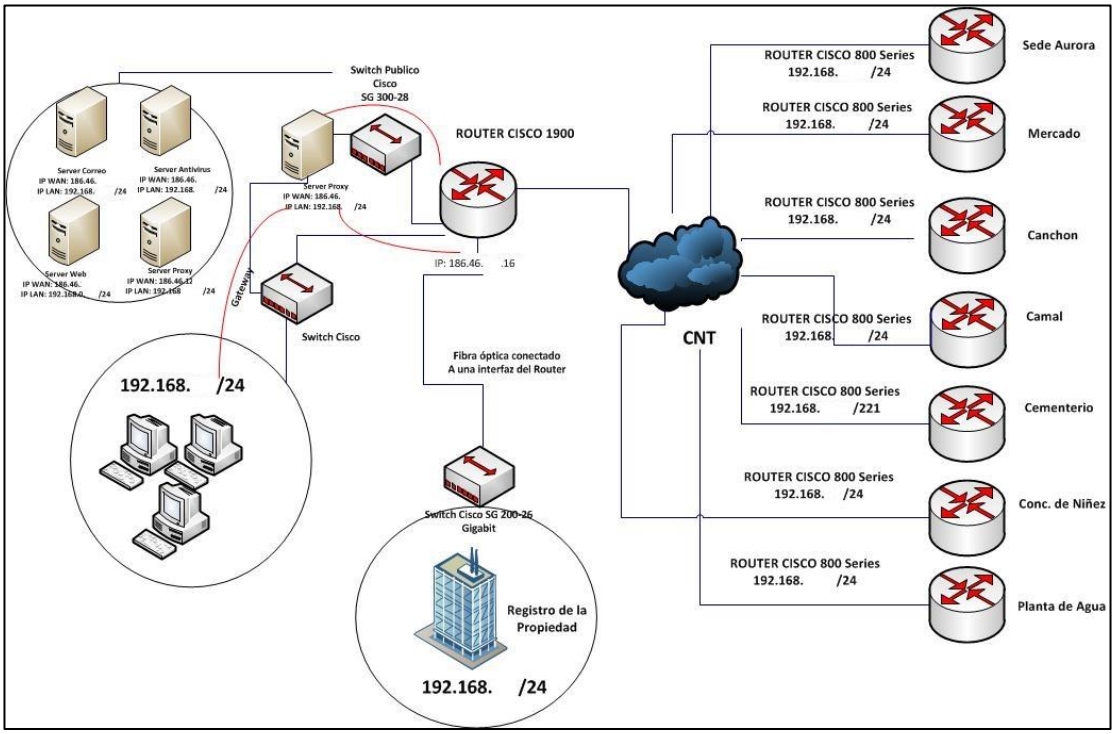

Figura 2.3.- Gráfico de la Red Local actual del G.A.D.I.M. del Cantón Daule

2.2.- Comparación de productos de seguridad a evaluar.

Existen algunas empresas en el mercado centradas principalmente en el desarrollo de Firewalls que cada año van agregando nuevas características que permiten aplicar mejor las políticas de aplicación y control de usuarios, así como también el de detectar nuevas amenazas.

Entre las empresas que integran el mercado de Firewalls tenemos las siguientes:

- Check Point Software Technologies
- Intel Security (McAfee)

- AhnLab
- Barracuda Networks
- Cisco
- Dell SonicWALL
- Fortinet
- Hillstone Networks
- HP
- Huawei
- Juniper Networks
- Palo Alto Networks
- Sangfor
- Sophos
- Stormshield
- WatchGuard

De todas estas empresas quipos los más posicionados en el mercado son las marcas CheckPoint, Palo Alto, Fortinet, Hillstone y Cisco, así se observa en el Cuadrante Mágico de “Gartner”:

Figura 2.4.- Cuadrante Gartner

Por su experiencia, características y posicionamiento en el mercado estas marcas tienen un costo muy elevado, por lo que dificulta la adquisición sobre todo para las empresas públicas, ya que no disponen de presupuesto muy alto; es por ello que la evaluación se la realizará confrontando un modelo y marca que está al alcance del presupuesto de la institución y que brinda la misma seguridad, características y funcionalidades que las marcas más reconocidas tales como:

1. Cisco ASA 5545-X más Modulo IPS con servicios FirePower.
2. Checkpoint 4200 Next Generation Threat Extraction Appliance con blades de IPS, URl filtering, anti-bot, anti-virus, VPN-IPsec para 200 Usuarios, QoS, anit-malware.
3. Fortinet 200D más Fortianalyzer, Fotireporter, Fortisanboxing, adicionalmente se debe de incorporar anti-virus, IPS, URL-Filtering, QoS, VPN-IPsec.
4. Hillstone E1700

A continuación se presenta la tabla comparativa de firewalls que se realizó con respecto a las otras marcas de acuerdo a las características que se necesitan para esta institución pública:

Tabla 1.- Tabla Comparativa de Firewalls seleccionados.

CARACTERISTICAS	HILLSTONE E1700	CISCO	FORTINET	CHECK POINT 4200
Modelo	E1700	ASA 5545-X + Modulo IPS	Fortigate 240D	4200 Next Generation Threat Extraction Appliance
Throughput Multiprotocolo TCP (Gbps)	1.5	1	1.2	1.4
Identificación de Aplicaciones	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
Gestión de ancho de banda	✓	✓	✓	✓
Anti-virus	✓	✓	✓	✓
VPN	✓	✓	✓	✓

Web Page Access Control (Web Filtering)	✓	✓	✓	✓
(IDS/IPS)	**500 Mb**	**900 Mb**	**400MB**	**150 Mb**
Auditoría y Monitoreo	✓	✓	✓	✓
CARACTERISTICAS AVANZADAS DE FIREWALL				
Network	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
Identificación de aplicaciones e identificación de usuario	✓	✓	✓	✓
Índice de Salud de la Red(NHI)	✓			
Índice de Reputación de Comportamiento (BRI)	✓			✓
Prevención de Amenazas Avanzadas Persistentes (APT) contra Malware	✓	✓		✓
Correlación y Análisis de Comportamiento Anómalo de Tráfico	✓			
Numero de tuneles VPN IPsec por defecto incluidos	**2000**	**2500**	**2000**	**200**
Sesiones Concurrentes	**1.000.000**	**750.000**	**3.200.000**	**1.200.000**
Nuevas Sesiones	**20.000**	**30.000**	**77.000**	**25.000**
Balanceo de Enlaces	✓	✓	✓	✓
Balanceo de Carga	✓			
Calidad de Servicio Inteligente (iQoS) y Granular	✓			
Análisis y diagnóstico	✓	✓	✓	✓
Visibilidad Granular de aplicaciones	✓	✓	✓	✓
Registro de auditoría	✓	✓	✓	✓
Alertas personalizables por aplicaciones o servicio.	✓			
Auto Mitigación de ataques.	✓			
Reportes	✓	✓	✓	✓
Capacitación (2 personas)	✓			
Soporte Remoto (3 años) cobertura 5x8xNBD, 8:30 a 17h30	✓	✓		✓
Garantía de Hardware (3 años)	✓	✓	✓	✓
VALOR $:	**20.809,06**	**50.673,75**	**37.278,34**	**41.325,00**

2.3.- Descripción de las características generales de las marcas que serán evaluadas.

CHECK POINT.

Su cartera incluye firewall de próxima generación, [2]prevención de amenazas, la seguridad Web, cliente final, la seguridad móvil, la seguridad en la nube y soluciones contra la denegación distribuida de servicio (DDoS). Incluye una línea de 17 dispositivos de firewall y 2 chasis para cuchillas de expansión con la capacidad de expansión de hasta 4 Gbps. Dicha expansión puede ser dada por software o por chuchillas adicionales.

Fortalezas:

- Mejor base de clientes empresariales.
- Soporta todos sus clientes a través de los numerosos aliados de negocio que posee a nivel mundial.
- Se adapta fácilmente a las necesidades de crecimiento de la empresa.

- Posee un equipo interno dedicado a la función de servidor de seguridad de desarrollo.
- Ha fusionado los componentes de la red y las aplicaciones en una política unificada para su administración y control.

CISCO.

Cuenta con un amplio portafolio de productos de seguridad de red a través de cortafuegos / IPS, web de seguridad y seguridad de correo electrónico, [3]la oferta de firewalls es principalmente a través de Adaptive Security Appliance (ASA). ASA más los servicios de FIREPOWER equivalen a ASA con protección avanzada contra malware (AMP).

Fortalezas:

- Valor agregado por el acuerdo de Licencia de empresa (ELA) para el software y hardware de seguridad.
- Clientes de Gartner califica constantemente la red de apoyo de Cisco como excelente.

- Posee fuertes canales de distribución y amplia disponibilidad que otros productos de seguridad.
- Cisco ofrece una amplia variedad de plataformas de firewalls.
- La integración de las funciones de reputación a través de los productos CISCO es fuerte.

FORTINET.

Fortinet se ha centrado mucho en el uso de hardware especialmente diseñado para fabricar Firewalls Empresariales y Appliances UTM con un amplio rango de características con excelentes opciones de precio/rendimiento[4]. Ofrece un amplio portafolio de equipos de seguridad y tiene presencia en infraestructura de redes. Esta combinación ha permitido que los firewalls empresariales puedan satisfacer la mayoría de las necesidades de seguridad de grandes empresas.

FORTINET sigue avanzando dentro de la base de datos de Clientes de Gartner, especialmente en sucursales o minoristas y cada vez es más difundido a nivel empresarial. Es competitivo y de alto rendimiento.

Fortalezas:

- FORTINET tiene un gran equipo de desarrollo de hardware y software, el cual utiliza para ingresar en el mercado de ventas más rápidamente debido a la mejora continua de sus chipset.
- Posee una estrategia bien articulada con respecto a la virtualización, nube pública y SDN y tiene una prometedora asociación con VMware NSX.
- Es muy utilizado por ISP, Data Centers, proveedores de servicios y empresas distribuidas.

Hillstone Networks.

Su portafolio de firewall lo componen tres líneas de productos, la serie T (3 modelos), la serie E (13 modelos) y el X-Series (dos chasis), con rendimientos de firewalls que van desde 1 a 360 Gbps[5]. Hillstone ha añadido la característica de detección de anomalías en el

comportamiento de la red de en sus firewalls y ofrece versiones virtuales tal como Virtual Elastic Firewall Architecture (Vefa).

Fortalezas:

- Hillstone tiene una fuerte presencia en China, y ofrece modelos de firewall dedicados para este mercado.
- Los clientes encuestados en China dan excelente puntuación a esta marca.
- Integra políticas basadas en el comportamiento, con las cuales lo llaman Firewall Inteligente de Próxima Generación (Intelligent Next-Generation Firewall).

CAPÍTULO 3

RESULTADOS DE LA EVALUACIÓN.

3.1.- Solución de Hardware seleccionada para implementación en G.A.D.I. Municipalidad del Cantón Daule.

Como se puede apreciar en la tabla comparativa, en el que se evalúan las diferentes características de los firewalls de última generación, podemos indicar que todas las marcas evaluadas cumplen casi con todos los parámetros de evaluación, pero, se detecta una diferencia muy marcada en el equipo ofertado de marca HILLSTONE.

El equipo cumple con todas los servicios requeridos por el G.A.D.I. Municipalidad del Cantón Daule, no está de más destacar que este

equipo posee el mejor precio en el mercado local. Por lo tanto se procederá con la compra del equipo mencionado.

Figura 3.5.- Solución de Hardware seleccionada.

3.2.- Implementación del Firewall perimetral PFSENSE.

Previo a la implementación del software PFSENSE, es necesario tener disponible el listado de las direcciones IP, subredes, el mapa de toda la red dividido por departamentos, listado de jefaturas y direcciones, direcciones ip de enlaces de comunicación, rutas estáticas, etc. de tal forma estén identificados los puntos de cables de red correspondientes a cada una de las interfaces de administración y control. Una vez revisados todos los equipos o instalaciones, se procede a la instalación del Software PFSENSE, el cual será instalado en un ordenador que cuente con 4 interfaces de red como mínimo, el proceso de instalación es muy sencillo, se puede instalar de varias formas, al más común es la

utilización de un CD-ROM o DVD AUTO-ARRANCABLE, o mediante red utilizando el estándar PXE.

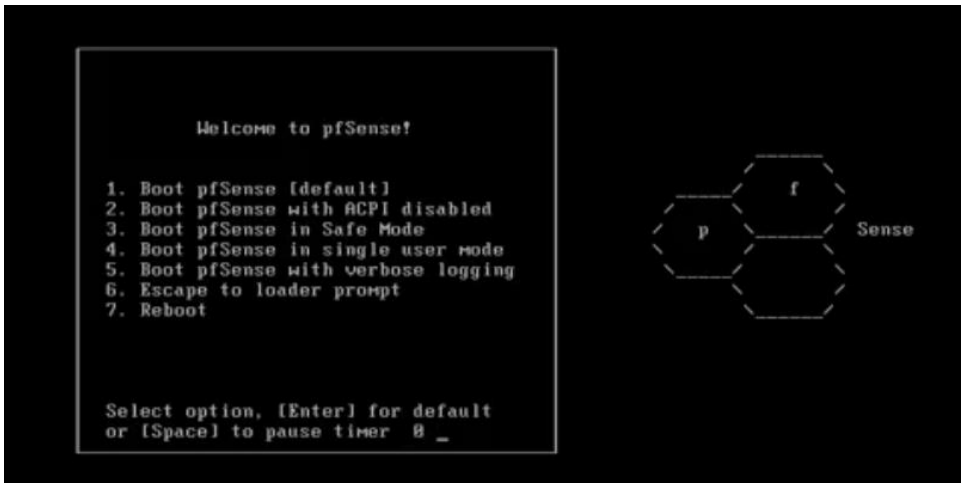

Figura 3.6.- Pantalla de Instalación del PFSENSE

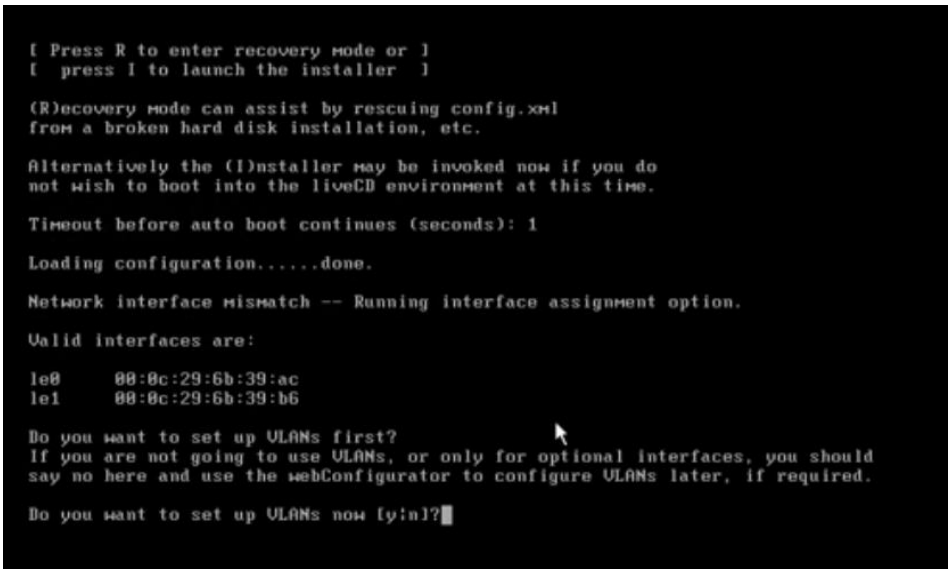

Figura 3.7.- Pantalla de Instalación del PFSENSE

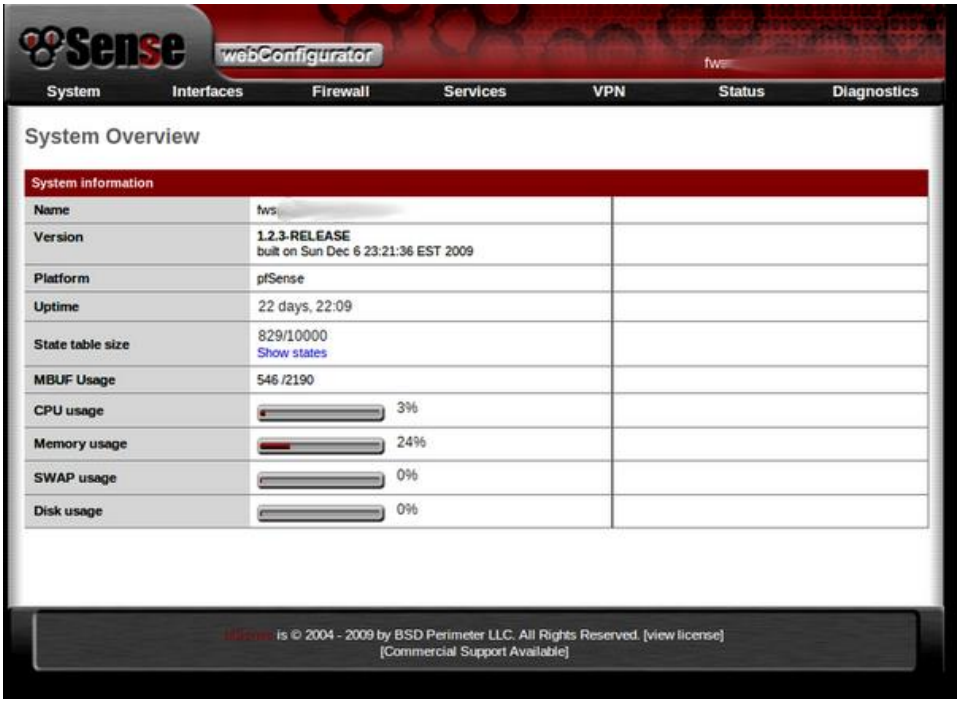

Figura 3.8.- Pantalla de inicialización de aplicación de PFSENSE

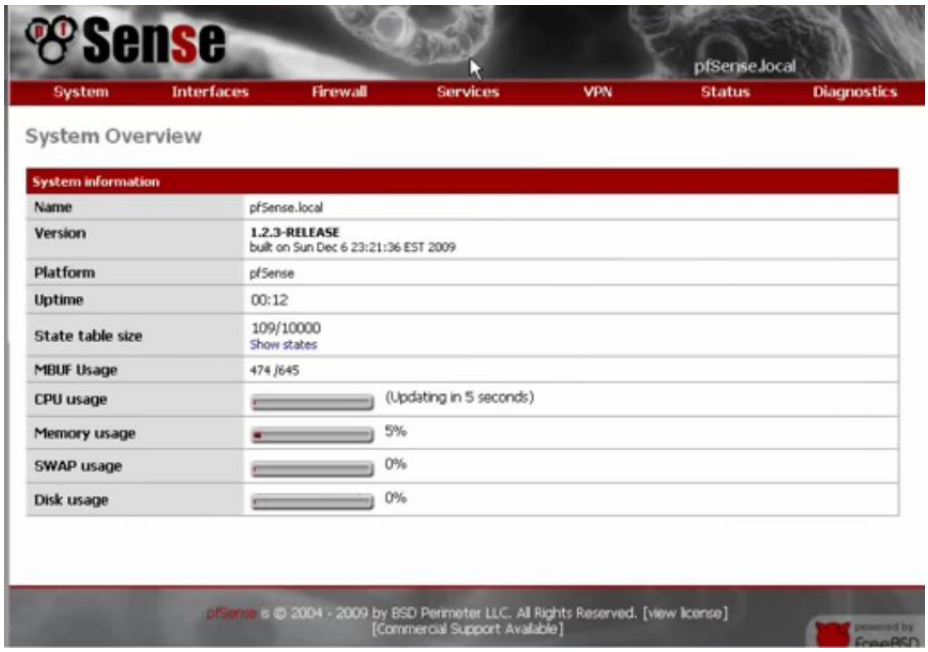

Figura 3.9.- Pantalla de estadísticas de aplicación de PFSENSE

Un vez que termina la instalación inicial del firewall PFSense es necesario instalar los diferentes paquetes de servicios adicionales que posee este software, tal como Servidor PROXY, Dashguardian, Servidor DHCP, etc.

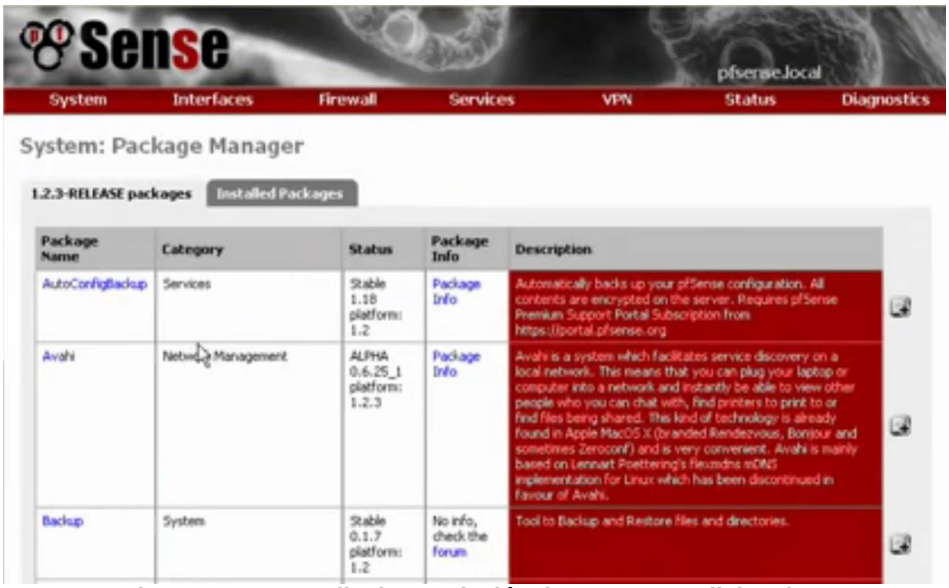

Figura 3.10.- Pantalla de Instalación de Paquetes Adicionales.

Es muy importante que el servidor físico reconozca las “n” tarjetas de red que sean instaladas físicamente en él, esto es, debido a que cada interfaz podrá configurarse dependiendo del uso que se le vaya a dar, por ejemplo una interfaz para los enlaces de la red LAN, otro para los enlaces de la red WAN y de igual manera otra interfaz para configurar un puerto DMZ.

Para llegar a esta configuración de varios puertos de red, fue necesario adquirir una tarjeta de red gigabit con 4 puertos ethernet marca HP modelo NC364T PCI-express. Con esta tarjeta de red, más una tarjeta de red PCI

adicional y la tarjeta de red del CPU se completan un total de 6 puertos de red configurables por PFSense.

Figura 3.11.- Tarjeta de Red Multi-puerto HP NC364T PCI-e.

Una vez configurado el hardware necesario e instalado el software de seguridad PFSENSE, se procede con las configuraciones de las reglas del firewall para establecer las politicas de seguridad necesarias en el G.A.D.I. Municipalidad del Cantón Daule:

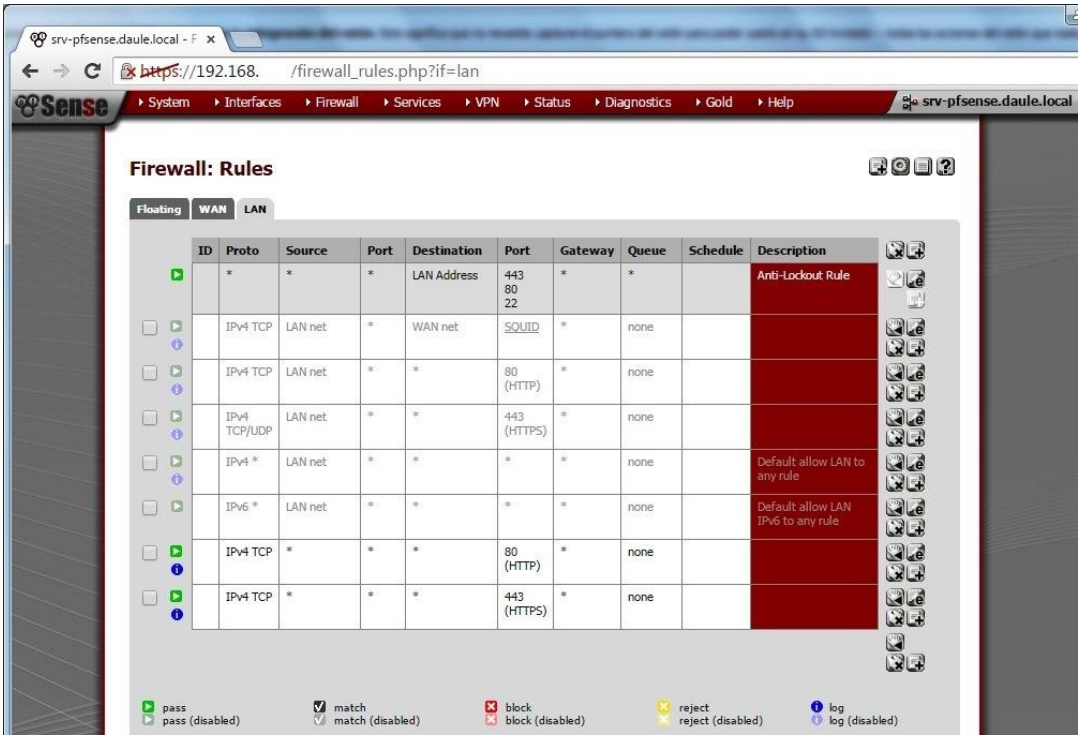

Figura 3.12.- Pantalla de configuración de políticas en red LAN.

Por cada interfaz de red instalada existirá una subcarpeta de configuración individual de cada puerto.

Es necesario tener bien definido el esquema de la red actual en conjunto con el nuevo direccionamiento IPv4 y todas las subredes que serán utilizadas. Para efecto de configuración y compatibilidad será deshabilitado el protocolo IPv6.

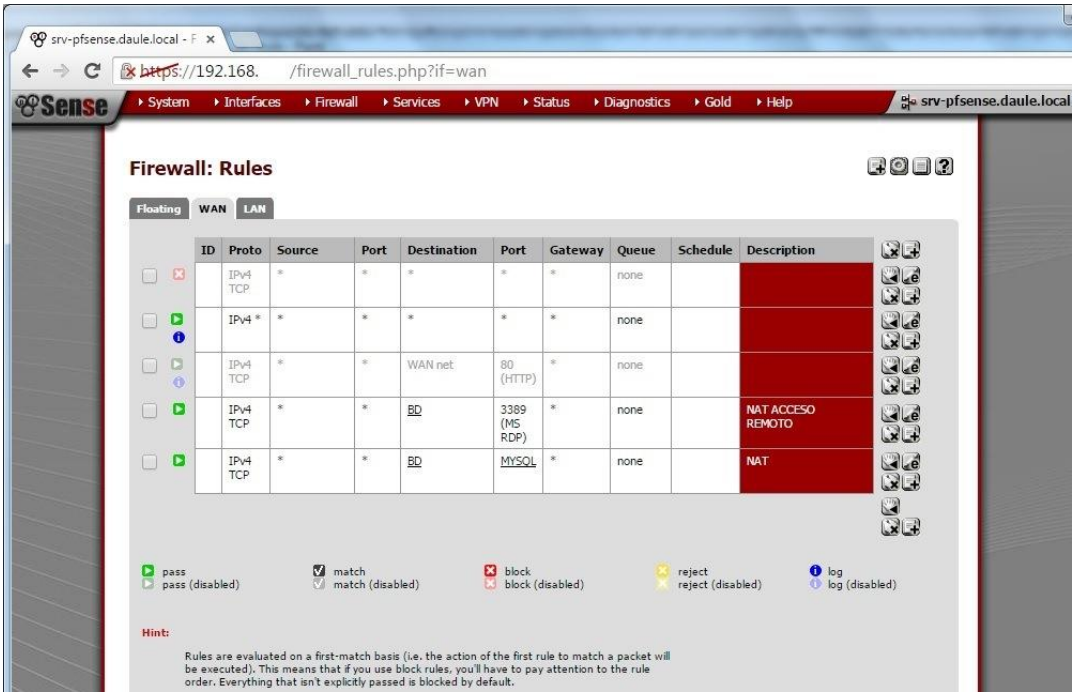

Figura 3.13.- Pantalla de configuración de políticas en red WAN.

Una vez terminada la instalación se presentara la pantalla de Estatus o DASBOARD del sistema PFSense, en esta pantalla apareceran las estadisticas de trafico de red, estatus de los servicios instalados o de los que se desea monitorear, carga de procesamiento, estatus de las interfaces de red instaladas, etc.

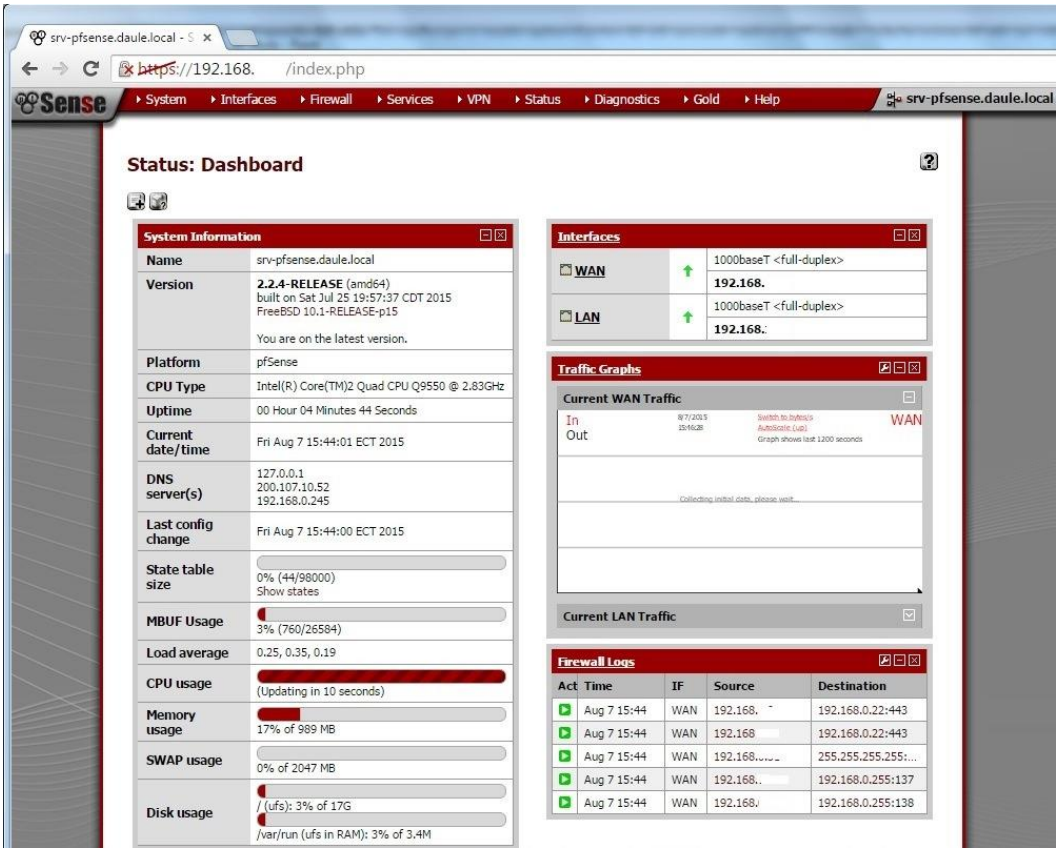

Figura 3.14.- Pantalla principal o DASHBOARD.

CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES

En el mercado local existen algunas soluciones de seguridad perimetral que podría ser implementada, la mejor opción presentada en este análisis es la de la marca HILLSTONE, ya que cubre las expectativas planteadas por el GADI Municipalidad del Cantón Daule.

El personal técnico del proveedor seleccionado es de comprobada experiencia local e internacional en el tema de seguridad de la información, además cuentan con las respectivas certificaciones que avalan esto.

El GADI Municipalidad del Cantón Daule pasara de tener un esquema se seguridad perimetral muy básico a un esquema de seguridad perimetral

robusto, donde tendrá servicios tales como Antivirus, URL Filtering, Firewall Inteligente, IPS y lo más importante "*detección de ataques de día 0*".

Sera minimizado un98% el riesgo de un ataque informático desde el exterior de la red informática municipal lo que garantizaría la continuidad del negocio y la seguridad de la información que reposa en el DATA CENTER Municipal.

Mientras se termina de ejecutar el proceso de compra del equipo de seguridad HILLSTONE, será implementada la versión libre del firewall PFSENSE y una vez adquirida la solución final, este equipo PFSENSE quedara implementado en conjunto con la solución de HILLSTONE

RECOMENDACIONES.

1. Es indispensable que se mantengan al día las actualizaciones de las bases de datos de firmas de antivirus y de ataques informáticos, esto se logra permitiendo el acceso al sitio web del proveedor del equipo de seguridad.

2. De igual manera es muy importante mantener la vigencia del contrato de soporte técnico y actualizaciones de software por parte del proveedor del equipo de seguridad luego del tercer año de funcionamiento.

3. Es necesario considerar que este equipo de seguridad va a proteger la red LAN Municipal de ataques externos, mas no de ataques internos. Por lo tanto, al implementar este equipo es primordial implementar un reglamento de seguridad informática interno donde quede plasmado las políticas y procedimientos que prevengan este tipo de ataques desde la red interna.

4. Mantener actualizadas las listas de distribución de emails para las alertas que se lleguen a presentar en el equipo de seguridad.

5. Adicionalmente es necesario realizar cursos de actualización al personal técnico del GADI Municipalidad del Cantón Daule como mínimo dos veces al año.

6. Realizar y mantener los respaldos correspondientes de la configuración inicial y de las posteriores actualizaciones del equipo de seguridad tanto de las reglas y políticas como del firmware del mismo.

BIBLIOGRAFÍA

[1] PFSense, «PFSense,» Agosto 2015. [En línea]. Available: https://www.pfsense.org/. [Último acceso: Agosto 2015].

[2] Check Point, «Check Point,» Agosto 2015. [En línea]. Available: http://www.checkpoint.com/products-solutions/threat-prevention/advanced-threat-prevention/index.html. [Último acceso: Agosto 2015].

[3] Cisco Next Generation Firewalls, «Cisco,» Agosto 2015. [En línea]. Available: http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html. [Último acceso: 2015].

[4] Fortinet, Agosto 2015. [En línea]. Available: http://www.fortinet.com/products/fortisandbox/index.html. [Último acceso: 2015].

[5] HillStone Networks, «Hillstone Networks,» Agosto 2015. [En línea]. Available: http://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/. [Último acceso: 2015].