CAPÍTULO IV

4. SEGURIDAD INFORMÁTICA DE LA RED DE DATOS

4.1. INTRODUCCIÓN

La parte más importante de una empresa, sea esta estatal o privada, es la información que esta maneja sobre sus clientes y productos. Cualquier amenaza que atente contra la integridad, autenticidad y disponibilidad de esta información, le significa a las empresas pérdida de tiempo y dinero.

El crecimiento que ha experimentado el uso de Internet en todo el mundo, a originado que exista una mayor cantidad de servicios disponibles por esta red, así como acompañado de otro fenómeno mundial, la globalización, a obligado a que se dé una evolución en los sistemas informáticos y principalmente en los sistemas de comunicación, así es común encontrar redes de área extendida (WAN) y redes de área metropolitana (MAN) al uso de empresas e instituciones públicas o privadas.

Esta apertura a nuevas tecnologías de comunicación, también ha conllevado a que la información e infraestructura de red de las empresas se encuentren expuestas a personas interesadas en la información que circula por estas redes, tomando en cuenta estos antecedentes, las empresas hoy en día,

se han visto obligadas ha implementar sistemas de seguridad, para poder proteger su información de intrusos y estafadores, que están husmeando en la redes externas o en el mismo Internet (la red menos segura del mundo).

Para que la seguridad informática sea efectiva, se requiere conseguir un equilibrio entre el grado de protección y el nivel de disponibilidad, que a menudo son dos aspectos que se entienden como contrapuestos, sin olvidar otro aspecto que tiene mucha importancia, como es la inversión económica que conlleva el implementar un sistema de seguridad informática.

Las instituciones tienen implementadas diversas medidas de protección de ataques en las redes de datos, por lo que es muy importante señalar el nivel que tienen implementado y observar la meta en cuanto a seguridad informática a la que deben llegar de acuerdo a su plan estratégico, la siguiente tabla indica los niveles de madurez de la seguridad informática:

Nivel	**Proceso**	**Tareas Realizadas**
Nivel 1	Sentido Común	Controles básicos: antivirus, cortafuegos, copias de seguridad, definición de usuarios y contraseñas
Nivel 2	Cumplimiento Legislación sobre seguridad informática	Clasificación de información en pública y privada Adaptación a la ley de comercio electrónico
Nivel 3	Gestión del proceso de seguridad informática	Planes directores de seguridad Políticas, procesos y procedimientos de seguridad Procesos de respuesta a incidentes
Nivel 4	Gestión global de riesgos de los sistemas	Análisis de Riesgos Gestión centralizada de la seguridad Planes de continuidad del negocio
Nivel 5	Certificación	Certificación de sistemas y procesos Certificación de actividades de comercio electrónico Sellos de confianza

Tabla 4.1: Niveles de madurez de la Seguridad Informática

A continuación se presenta el resultado del análisis realizado en las instalaciones del Municipio Metropolitano de Quito, en base a esa realidad se presenta una propuesta de seguridad informática para la red de datos del Municipio de Quito, de tal forma que cualquier agente externo que trate de atentar contra la integridad, autenticidad, y disponibilidad de la información del Municipio sea mitigado de manera proactiva por dispositivos que serán ubicados de forma estratégica.

4.2. SITUACIÓN ACTUAL

La red de datos del Municipio del Distrito Metropolitano de Quito esta conformada por redes LAN implementadas en las dependencias municipales que se encuentran geográficamente dispersas por todo el Distrito Metropolitano de Quito e interconectadas hacia la red principal ubicada en la Dirección Metropolitana de Informática, mediante redes de área metropolitana MAN.

Al tener la red de datos del Municipio de Quito esta realidad y hablando estrictamente desde el punto de vista de seguridad informática, se hace necesario evaluar individualmente cada red LAN para garantizar que están adecuadamente protegidas y así avalar que la red de datos global del Municipio lo está también.

Para realizar este análisis de seguridad informática de las redes LAN y MAN, se utiliza una metodología sistemática que ayuda a controlar las diferentes fases, de una manera organizada y práctica, siendo indispensable la participación del personal que administra los sistemas informáticos en cada red

LAN y el personal del departamento de redes de la Dirección Metropolitana de Informática, para cumplir esta tarea es necesario realizar determinadas tareas y estimaciones de forma totalmente imparcial y lo más objetiva posible:

Análisis de Riesgos

- Inventariar los activos e identificar las amenazas sobre estos activos
- Identificar las vulnerabilidades presentes en los activos
- Estimar el impacto en el funcionamiento de la red de datos del Municipio si ciertas amenazas se hacen efectivas.

Diseño del sistema de seguridad informático de la red de datos

- Arquitectura de red segura
- Arquitectura de Firewall
- Arquitectura del sistema de ANTISPAM, ANTIVIRUS y Navegación.
- Arquitectura de IDS/IPS
- Sistema de administración

4.3. ANÁLISIS DE RIESGOS

Es un procedimiento utilizado para determinar el riesgo a los cuales están expuestos los componentes de la red de datos, una vez conocidos estos riesgos, la Dirección Metropolitana de Informática puede decidir que medidas tomar dependiendo de una serie de factores (costos de la implementación de controles que reduzcan los riesgos vs. costos derivados de las consecuencias de la materialización de estos riesgos).

4.3.1. Inventariar los Activos e Identificar las Amenazas

Primeramente determinar los activos que poseen las redes de datos de las dependencias municipales, en cada uno de estos activos, se identifican las amenazas que pueden afectar su correcto funcionamiento, y se determina las salvaguardas que se pueden implementar para mitigar estas amenazas.

Todas las salvaguardas que se mencionan en la tabla serán parte de las políticas de seguridad informática que se pondrán a consideración del Comité de Seguridad Informática del Municipio del Distrito Metropolitano de Quito para su implementación.

El primer activo que dispone una red de datos LAN es el medio de comunicación, es decir es sistema de cableado, el atacante puede cortar el cable y dejar sin funcionamiento un dispositivo o un segmento de red, este peligro está presente en el caso de las dependencias municipales ya que ciertas oficinas son de acceso público y al no disponer de elementos de protección el cableado se vuelve vulnerable. Además los paneles de conexión y los equipos de comunicación en la mayoría de redes LAN no se encuentran protegidos adecuadamente dentro de racks de telecomunicaciones cerrados, siendo fácil su acceso para conexiones no autorizadas.

Elemento	**Amenazas**	**Salvaguardas**
Cableado	• Corte de cable • Estableciendo conexión no autorizada • Robo	• Enrutamiento adecuado de cableado • Paneles de conexión en rack cerrados • Sistema cableado protegido en racks cerrados con cerradura
Switch capa 2 No Administrable	• Desbordamiento de CAM • Switch Spoofing – VLAN hopping • Manipulación STP	• Ninguna • Ubicar el equipo dentro de racks cerrados con cerradura

	• Robo	
Switch capa 2 Administrable	• Desbordamiento de CAM • Switch Spoofing • VLAN hopping • Manipulación STP • Configuraciones desatendidas • Robo	• Implementar Storm Control • Implementar Seguridad por puerto • Deshabilitar auto trunking para todas las interfaces • VLAN`s dedicada para trunking • Configurar adecuadamente el equipo • Capacitación al personal técnico • Ubicar el equipo dentro de racks cerrados con cerradura
Switch capa 3 Administrable	• Denegación de servicios DoS • Switch Spoofing • VLAN hopping • Manipulación STP • Configuraciones desatendidas • Robo	• Actualizar sistema operativo • Actualizar parches de seguridad • Deshabilitar auto trunking para todas las interfaces • VLAN`s dedicada para trunking • Configuración de todos los puertos • Capacitación al personal técnico • Ubicar el equipo dentro de racks cerrados con cerradura
Router	• Denegación de servicios DoS • Puertas traseras abiertas • Configuraciones desatendidas • Robo	• Actualizar sistema operativo • Capacitación al personal técnico • Ubicar el equipo dentro de racks cerrados con cerradura
Computador Personal	• Virus • Troyanos • Gusanos • Malware • Spyware • Fallas en Sistemas Operativos • Fallas en Utilitarios Oficina	• Antivirus, Antitroyano, AntiSpyware • Parches Sistemas Operativos • Parches paquetes oficina
Servidor	• Virus, Troyanos, Gusanos • Fallas (bugs) en las aplicaciones de servidores • Administración desatendida • Instalación desatendida • Robo	• Herramientas Antivirus Antitroyano, AntiSpyware • Aplicar parches de sistemas • Capacitación al personal técnico • Ubicar el equipo dentro de racks cerrados con cerradura

Tabla 4.2: Inventario de Activos

Los equipos activos de las redes de datos están compuestos por switches administrables y no administrables. Los switches administrables no se encuentran debidamente configurados, es decir no están definidos parámetros para su administración, como son: dirección IP, dirección de correo del

administrador, restricción de manejo, ni siquiera está cambiado el password que viene definido en fábrica del usuario administrador, peor aún parámetros de control de equipos y rendimiento de red, como son: VLANS, tráfico permitido, que trae como consecuencia que estas redes sean inseguras y no tengan el rendimiento adecuado.

Los routers de los proveedores Andinadatos, PuntoNet e Impsat no son administrados directamente por la Dirección Metropolitana de Informática, en estos equipos no se encuentran instalados los últimos parches de seguridad publicados por los fabricantes.

En cuanto a la instalación de software antivirus en los computadores personales de las dependencias municipales se encuentra Symantec, sin el debido licenciamiento ni la debida actualización automática, la actualización hacia el servidor de antivirus depende de la acción del administrador de sistemas.

4.3.2. Vulnerabilidades

Las vulnerabilidades presentes en los equipos de comunicación y de computación nacen por el hecho de que los sistemas operativos presentan huecos de seguridad, producto de fallas de programación que son explotadas por las amenazas creadas con esta finalidad, de igual manera los utilitarios de escritorio también presentan errores en su programación.

Por ejemplo numerosas vulnerabilidades han sido reportadas en diversas implementaciones de SNMP, que permiten el acceso privilegiado no autorizado, ataques de denegación de servicio, o causar un comportamiento inestable del dispositivo, por lo que se recomienda su inhabilitación.

La mayor vulnerabilidad que presentan los dispositivos de red del Municipio de Quito constituye la instalación desatendida, y la falta de precaución en el manejo de los equipos de computación, incluyendo la ubicación inadecuada de servidores.

4.3.3. Estimar el Impacto de Amenazas se hagan efectivas

Se hace referencia a la magnitud de las consecuencias que tiene para el negocio el hecho de uno o varios activos hayan sido comprometido su funcionamiento, debido a que una o varias amenazas hayan explotado las vulnerabilidades de estos activos. El impacto puede producir pérdidas de manera directa o indirecta como:

- Pérdida directa de dinero
- Pérdida de imagen/reputación
- Poner en peligro al personal o a los clientes
- Violación de confianza
- Interrupción de la actividad de negocio

En el caso del Municipio del Distrito Metropolitano de Quito, el impacto que tiene al momento que la red no funcione adecuadamente definitivamente se ven afectados los ingresos que diariamente recoge por pago de impuestos

que realizan los ciudadanos en cada una de las Administraciones Zonales, el sistema es centralizado.

En el caso de la pérdida de imagen que sufre el Municipio del Distrito Metropolitano de Quito, cada vez que se escucha la frase se fue el sistema es alta, ya que el usuario ya no confía en el sistema, y por un momento pensemos que sucedería si existiese otra institución alternativa en la cual podamos cancelar nuestros impuestos y estos valores no pasen al Municipio por esta causa.

4.3.4. Diseño del Sistema de Seguridad Informático de la Red de Datos

En esta sección primeramente se propone una arquitectura de red, de tal forma, que los agentes externos que deseen acceder a la información de la red de datos del Municipio tengan los permisos respectivos, y sean registrados para poder hacer procedimientos a futuro de Auditoria.

4.3.5. Arquitectura de Red Segura

Una arquitectura de red segura depende de el diseño que se tome como referencia, seguiremos basándonos en el modelo Safe de Cisco, en el cual ahora lo único adicional que realizaremos es indicar todas las medidas de seguridad a ser implementadas en cada uno de sus módulos.

4.3.5.1. Módulo Administración

- Implementación de una red fuera de banda OOB, separada de la red de Producción.

- Servicio de Control de Acceso a la Red de Administración
- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas

4.3.5.2. Módulo de Building

- Implementar software antivirus en todas las estaciones de trabajo
- Disponer de software anti-sniffer
- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas.

4.3.5.3. Módulo de Building Distribution

- Control de Accesos
- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas

4.3.5.4. Módulo de Core

- Control de Accesos
- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas.

4.3.5.5. Módulo Edge

- Control de Accesos
- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas.

4.3.5.6. Módulo Server

- Implementación de sistemas de detección de intrusos
- Implementación de servidor de autenticación, autorización y auditorias de usuarios.
- Sistemas Antivirus, Antisniffer

- Implementación de VLANS
- Configuración de Switch de acuerdo a políticas

4.3.5.7. Módulo Internet Corporativo

- Implementación de un sistema de Firewall que cumpla con las políticas de seguridad.
- En la DMZ se deben colocar servidores de acceso público
- Implementar el servicio de restricción de sitios Web
- El acceso hacia Internet debe ser autentificado y autorizado
- Configuración de Router de acuerdo a políticas de seguridad.

4.3.5.8. Módulo WAN

- Configuración de Router de acuerdo a políticas de seguridad.

Debido que la Red del Municipio está compuesta por varias Redes, y dentro de estas están conectadas empresas que son afines y otras que no tienen nada en relación con la Red del Municipio se ha tratado de segmentar las redes remotas con la filosofía de identificar que dependencias son afines y cuales no lo son, esto con el fin de poder definir diferentes niveles de seguridad.

Adicionalmente se tendrá una red interna del Municipio totalmente independizada de las redes remotas, ya que las máquinas que acceden a los aplicativos desde esta red tendrán privilegios distintos a las máquinas que accedan desde las redes remotas.

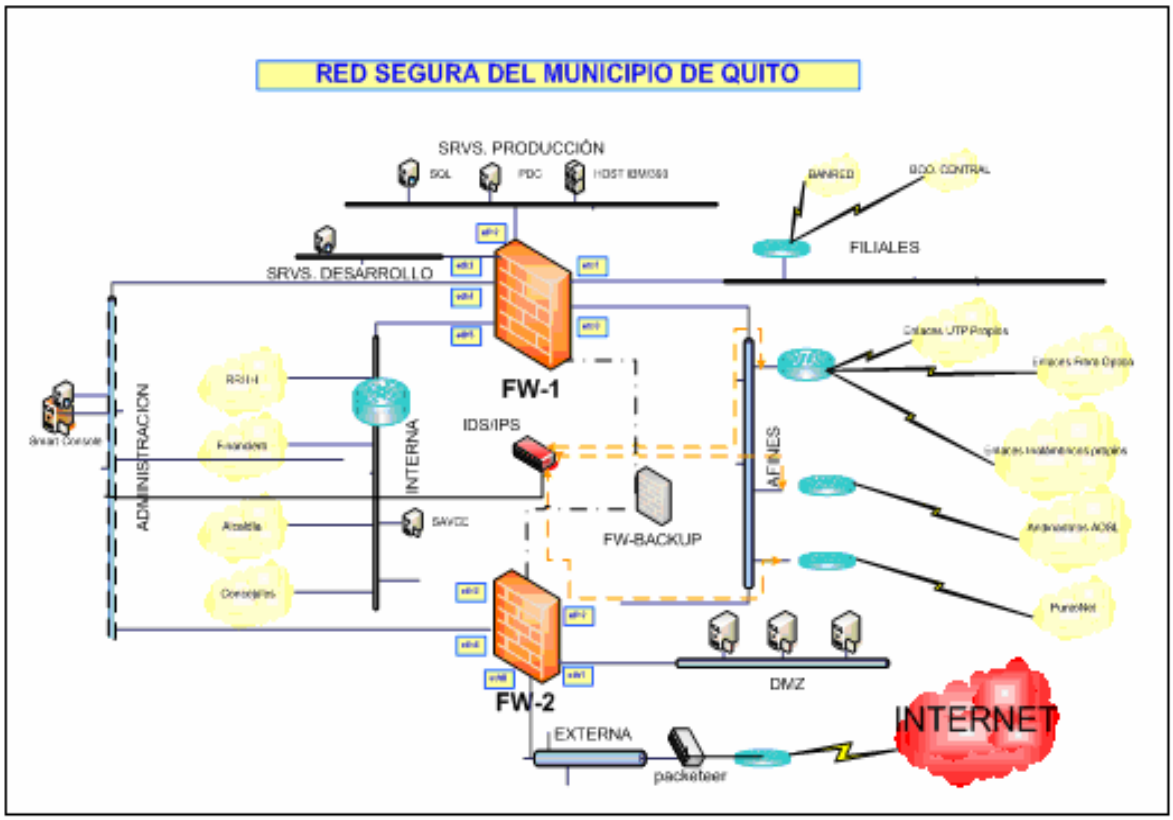

Figura 4.1: Módulo WAN

Este diseño modular provee flexibilidad, cuya implementación puede ser realizada por fases, según las necesidades del Municipio, además permite optimizar la infraestructura de seguridad existente, identificando dónde y por qué los productos de seguridad crítico y las tecnologías (Firewall, IDS, VLANS, etc.) son necesarios.

4.3.5.9. Clasificación de los Segmentos de Red

Red Servidores de Producción.- En esta red se conectarán todos los servidores de bases de datos transaccionales actualmente en producción como Hosts IBM/390, los directorios activos, etc.

Red Servidores de desarrollo.- En esta red se conectarán los servidores que están en fases de pruebas, esto con el fin de que los permisos que se apliquen ha esta red no afecten a los servidores de producción.

Red Interna.- Esta red conectará todas las máquinas que son parte de la red interna del Municipio, y que las conocemos como redes aledañas.

Red Filiales.- En esta red se ubicarán todos los accesos remotos de redes que no son parte de la red del Municipio, empresas externas como es el caso de Banred, Banco Central, pero los usuarios del Municipio necesitan su acceso.

En este segmento también se conectaran todos los accesos remotos que necesiten acceder a los aplicativos a través de enlaces virtuales seguros con VPN, como es el caso de Secure Client.

Red Afines.- En esta red se conectarán todas las redes remotas de empresas que son afines a Municipio como es el caso de las Administraciones Zonales, Direcciones Metropolitanas, Instituciones Educativas que maneja el Municipio, Oficinas Administrativas.

Red Administración.- Esta red se ubicarán todos los servidores de administración y monitoreo como es el caso de la consola de Administración de los Firewall y de los equipos de red administrables, interfase de acceso a los IDS/IPS, sistemas de monitoreo, etc. En esta red van a circular datos referentes a nombres de usuarios y contraseñas de administración, por lo que

esta red debe trabajar de manera separada (red fuera de banda) de la red de datos del Municipio.

Red Desmilitarizada o DMZ.- Esta red se conectarán todos los servidores que van a dar la cara al Internet como es el caso del Servidor de Correo, Servidor WEB, Servidor Proxy.

Red Externa.- en esta red se conectará el router de salida a Internet, el optimizador de ancho de banda Packeteer, este equipo permite adicionalmente restringir la navegación en el Internet de sitios prohibidos.

4.4. ARQUITECTURA DE FIREWALLS

Tomando en cuenta la realidad de la red del Municipio de Quito y basándonos en la cantidad de segmentos de red que dispondría, se recomienda que los Firewalls para esta arquitectura, sean de tipo software que se implemente en hardware especializado para servidores, con lo que se obtendría una gran variedad de ventajas, como:

- Independencia de la arquitectura de hardware y software.- es decir se pude instalar sobre cualquier tipo hardware sea este HP, DELL, etc. Y sobre distintos sistemas operativos como son Linux, Windows, etc.
- Administración Centralizada.- A través de una sola consola se puede administrar varios sitios remotos.
- Configuración totalmente gráfica.- Permite configurar y compilar las políticas de una forma gráfica y sencilla para el administrador.

- Revisión de tráfico en línea o por históricos.- Permite revisar el tráfico que atraviesa entre las redes al instante y de forma gráfica, y filtrar las consultas, permitiendo al administrador encontrar errores o ataques al instante.
- Sistema de detección y prevención de intrusos
- Recuperación de fallas de forma inmediata sin depender del hardware.

Para completar con la arquitectura de red segura, se describen las funciones que deben cumplir cada uno de los elementos, a fin de que puedan ser considerados como bases para que la Dirección Metropolitana de Informática pueda contratar o adquirir estos sistemas.

Firewall-1 (FW-1).- Este Motor de firewall, tendrá 6 interfases de red Ethernet que permitirá proteger los servidores de datos y transaccionales de los diferentes ataques o intrusiones que se produzcan desde la red interna, redes afines, redes externas.

Firewall-2 (FW-2).- Este Motor de Firewall contará con 5 interfases de red Ethernet que permitirá proteger las redes internas, y la red de servidores de los intrusos que deseen ingresar desde el Internet, se convierte en nuestra primera protección contra ataques provenientes del exterior.

Consola de Administración.- Esta consola permitirá administrar a los diferentes módulos de firewall de una forma centralizada, su función principal es permitir que el administrador configure políticas, sin interrumpir el normal

funcionamiento del los motores de firewall, y los aplique. Adicionalmente nos permite tener toda la configuración guardada que será independiente del contenido de los motores de firewall, esto nos permite tener un grado de disponibilidad mejorada.

Secure Client.- Este es un software que permite realizar una VPN a través del estandar IPSEC, y con autenticación, teniendo como autenticación métodos que usan certificados digitales. Esto es para acceso desde redes externas de forma segura a los aplicativos y datos de la red de servidores.

4.5. ARQUITECTURA DEL SISTEMA DE ANTISPAM, ANTIVIRUS Y NAVEGACIÓN

Debido a que en los actuales momentos el Municipio y las empresas afines, utilizan como sistema de antivirus el producto distribuido por la casa SYMANTEC (software sin licenciamiento), cuya versión es la COORPORATE EDITION, se recomienda que el sistema de antivirus sea el mismo, con la diferencia que cuando se compre la actualización del antivirus se la haga hacia la versión ENTERPRISE EDITION, esto permitirá adquirir dos productos más que ayudarán a mejorar la seguridad de la red.

Con esta finalidad recomendamos la siguiente arquitectura de red distribuida para los productos de SYMANTEC:

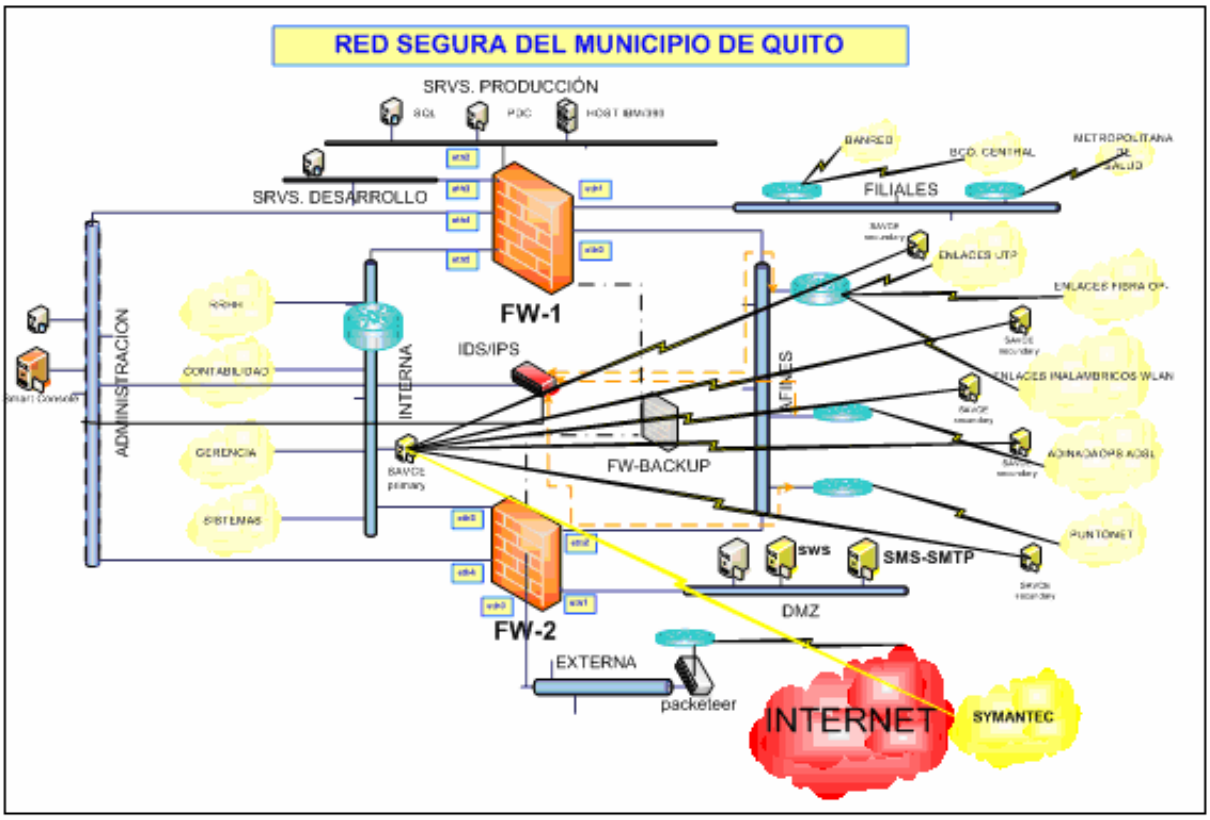

Figura 4.2: Arquitectura del Sistema de Antispam, Antivirus y Navegación

Symantec AntiVirus Coorporate Edition (SAVCE).- Este sistema permite proteger las computadoras personales ante la presencia de amenazas como son: Gusanos, Virus Informáticos, Caballos de Troya, Spyware, este software es simplemente un agente interactivo que va chequeando los software maliciosos que están trabajando dentro del PC, su administración se la realiza centralizadamente a través de la consola administrativa (Console Management).

En el caso de la red de datos del Municipio de Quito se puede configurar el Symantec Antivirus Coorporate Edition de manera distribuida, para esto se crea una consola primaria y varias consolas secundarias de acuerdo a la cantidad de empresas afines que se tenga, con esta configuración se pueden

definir las políticas más rápidamente y en una sola consola; las definiciones de virus se actualizan hacia la consola principal y de allí es distribuida hacia cada Symantec AntiVirus Coorporate Edition secundario, de esta manera se optimiza el ancho de banda utilizado por este tipo de tráfico, como se muestra en la figura 4.2.

La versión Enterprise de Symantec, consta de aplicativos adicionales para un manejo adecuado del sistema de correo electrónico, así como del sistema de navegación en el Internet, estos aplicativos son:

Symantec Mail Security for SMTP (SMS-SMTP).- Este aplicativo se instala sobre un servidor Windows que actúa como pasarela de correo, la función principal de este software es filtrar el correo que ingresa y sale de la red de datos del Municipio de Quito, este filtro es programable y permite verificar si el correo es un Spam, si tiene virus, gusanos, Caballos de Troya, Spyware, Fishing, etc, con esta consola además se puede definir políticas de uso de correo electrónico, como por ejemplo limitar el tamaño del mensaje, adicionar mensajes al pie de los correos, políticas que se pueden definir por grupos o de manera universal a todos los usuarios.

Symantec Web Security (SWS).- Este aplicativo permite trabajar como un servidor Proxy de tal forma que los usuarios que naveguen hacia cualquier página WEB, ésta sea analiza, si el código que esta bajándose es malicioso como virus, gusanos, spywares, troyanos, los bloquea; adicionalmente nos permite navegar a sitios WEB categorizados o personalizados por el

administrador. Esta aplicación puede trabajar de manera sincronizada con el servidor Proxy existente en la red de datos del Municipio de Quito.

4.6. ARQUITECTURA DE IDS/IPS

Tomando como filosofía que los IDS/IPS, en un inicio permiten el paso de todo el tráfico y después en base a políticas definidas, se bloquea el tráfico innecesario en la red, y además que será el encargado de auditar todo el tráfico que circula por la red de datos del Municipio, se propone la instalación de un sistema IDS/IPS entre las redes externas y Afines que sirven de acceso a las redes remotas del Municipio con el fin de poder bloquear cualquier tipo de ataques entre estas redes, ya que el firewall no ve este tráfico, esto como se muestra en la siguiente figura.

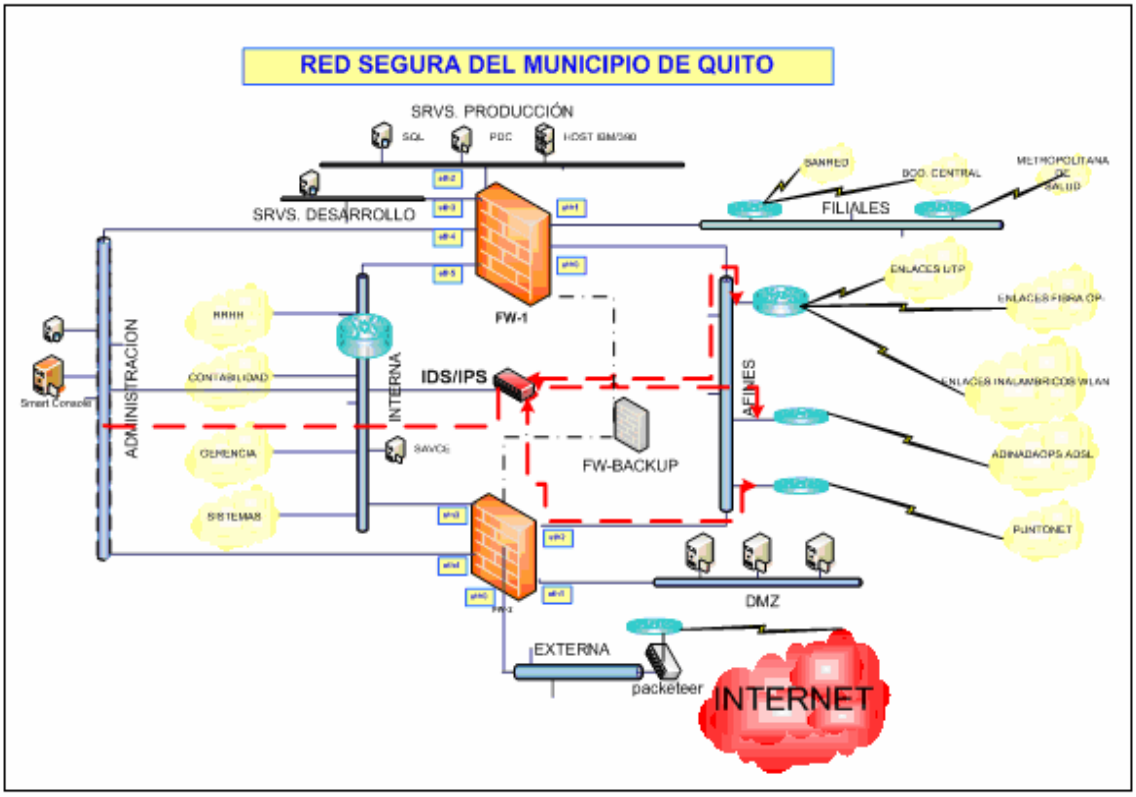

Figura 4.3: Arquitectura de IDS/IPS

La administración de este dispositivo, se lo realiza a través de una interfase que está conectada a la red de administración.

4.7. SISTEMA DE ADMINISTRACIÓN

Existen varios paquetes que sirven para monitorear y administrar los diferentes servidores, ruteadores y elementos activos dentro de toda la arquitectura de red, este software debe tener la capacidad de enviar mensajes al correo o al celular de la persona que administra la red de datos, indicando la caída o subida de un dispositivo, adicionalmente permite tener registro de cualquier apagado anómalo de los dispositivos administrados, y con ello se pueden llevar reportes de malfuncionamiento de dichos equipos y de la red en general.