SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM

Wilmar Flórez R.
Medellín, Colombia
wilmar.florez@gmail.com

Carlos A. Arboleda S.
Bancolombia
Medellín, Colombia
carlos_suaza@hotmail.com

John F. Cadavid A.
Escuela de Ingeniería de Antioquia
Medellín Colombia
johnfcadavid@gmail.com

(Tipo de Artículo: **Reflexión**. Recibido el 21/11/2011. Aprobado el 12/03/2012)

RESUMEN
Este documento está enfocado a realizar un aporte teórico a la implementación de una solución de seguridad informática modular que permita integrar las funcionalidades requeridas más comunes, como son los firewall, antivirus y control de contenido, denominada como UTM (Gestor Unificado de Amenazas). Esta solución se orienta a contrarrestar los diferentes tipos de ataques y amenazas en seguridad informática, a los que se ven expuestas las medianas y pequeñas empresas (Pymes). Estas amenazas y ataques informáticos están relacionados principalmente con el bajo control de malware, ausencia de protección perimetral (firewall) y falta de control de contenido, permitiendo ser neutralizarlas con la implementación de un gestor unificado de amenazas (UTM), con los módulos básicos de firewall, antivirus y listas de control de acceso.

Palabras clave
Antivirus, corta fuegos, Pequeña y Mediana Empresa (Pyme), riesgos tecnológicos, seguridad informática, Gestor Unificado de Amenazas (UTM).

A COMPREHENSIVE SECURITY SOLUTION FOR SMEs TROUGH AN UTM

ABSTRACT
This document is focused on realizing a theoretical contribution to the implementation of a solution of modular IT security that allows integrating the most common needed functionalities such as firewall, antivirus and control of content, named as UTM (Unified Threat Management). This solution is intended to prevent different types of assaults and threats in IT security for small and medium-sized enterprises (SMEs). These threats and IT assaults are mainly related to the very minimal malware control, lack of perimeter protection (firewall) and lack of content control, but they can be neutralized with the implementation of a Unified Threat Manager (UTM) having the basic modules of firewall, antivirus and access check lists.

Keywords
Antivirus, firewall, Small and Medium-sized Enterprises (SMEs), technology risks, security, Unified Threat Manager (UTM).

SOLUTION INTÉGRAL DE SECURITE POUR LES PETITES ET MOYENNES ENTREPRISES AU MOYEN D'UN UTM

RÉSUMÉ
Cet article se concentre sur des apports théoriques quant à l'implémentation d'une solution de sécurité informatique en modules qui permettent d'intégrer les plus communes fonctionnalités requises, comme les pare-feu, l'antivirus et le contrôle des contenus, appelé UTM (par ses sigles en anglais ou Gestion Unifiée des Menaces). Cette solution est destinée à contrer les différents types d'attaques et menaces en sécurité informatique pour les petites et moyennes entreprises (PME). Ces menaces et attaques informatiques sont liées essentiellement à la précarité du contrôle du malware, l'absence de protection du périmètre (pare-feu) et l'absence de contrôle des contenus, mais elles peuvent être neutralisés au moyen de l'implémentation d'un gestionnaire unifie des menaces (UTM), avec les modules de pare-feu, antivirus et listes de contrôle d'accès.

Mots-clés
Antivirus, pare-feu, Petite et Moyenne Entreprise (PME), risques technologiques, sécurité informatique, Gestion Unifiée des Menaces (UTM).

INTRODUCCIÓN

La globalización de los mercados en el siglo XXI está exigiendo que las Pymes se adapten a modelos de mercados altamente competitivos, en donde deben primar estándares de seguridad que garanticen las transacciones comerciales y la integridad de la información de los clientes.

Con el incremento de los servicios en línea, también se ha incrementado el nivel de riesgos y ataques derivados de las vulnerabilidades que acarrea la implementación de nuevas tecnologías, para el intercambio comercial de información. Las herramientas de los ciber-delincuentes han evolucionado si no más rápido, por lo menos paralelamente al desarrollo tecnológico, como ha venido sucediendo con los virus informáticos [1].

Las Pymes se encuentran en la obligación tecnológica de salvaguardar todas sus bases de datos de conocimiento de una manera ágil, generando a sus clientes la suficiente confianza y credibilidad para poder realizar sus transacciones comerciales de forma segura, rápida y eficiente.

Al implementar modelos de seguridad integral a través de herramientas tecnológicas que brinden una solución completa, las Pymes pueden garantizarles a sus usuarios, que están aplicando estándares de seguridad internacional para los negocios electrónicos. Ejemplos tecnológicos de modelos de seguridad integral son los UTM. Internet es una actividad esencial para cualquier negocio hoy en día. Con el uso generalizado del correo electrónico, y de nuevas tecnologías tales como los "mensajes instantáneos", la conexión a Internet resulta fundamental para mantener el contacto directo con los clientes y estar al día en las tendencias de la industria y al tanto de los desarrollos competitivos [2].

Con la masificación de internet las empresas se han visto en la necesidad de interconectar diversos procesos internos y publicar servicios a los clientes externos en la Web, con el fin de mantener un nivel óptimo de competitividad y de rendimiento económico. Como consecuencia de esto se han visto expuestas a una serie de riesgos y amenazas inherentes a la implementación de transacciones comerciales a nivel nacional e internacional. Este problema impacta de manera negativa en las empresas:

- Falta de aseguramiento en la continuidad del negocio.
- Pérdida de capital intelectual.
- Pérdida de información crítica para la empresa.
- Vulnerabilidad en su infraestructura de TI.
- Pérdida de confiabilidad en su imagen corporativa.

1. CONTEXTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁMBITO EMPRESARIAL

Las pequeñas y medianas empresas requieren herramientas que generen en la alta gerencia la suficiente confianza para la toma de decisiones al momento de generarse riesgos de TI. Estas decisiones deben estar respaldadas mediante argumentos físicos e históricos, de manera que le eviten a la empresa incurrir en sobrecostos y en subestimaciones o sobreestimaciones de los riesgos al momento de ser evaluados.

Al inicio de la década de los 90's, varias empresas norteamericanas sufrieron masivos ataques de virus. Aunque en un principio solo afectaban el funcionamiento del sistema operativo, fueron evolucionando en nuevos métodos de infiltración, orientados a la recolección de información y minería de datos, sin ver comprometida la funcionalidad de los sistemas y servidores.

En múltiples investigaciones realizadas se considera el tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de la organización y así contar con estrategias para avanzar ante cualquier eventualidad [3].

Abrir una página Web, usar dispositivos de almacenamiento extraíbles, usar correos electrónicos privados y públicos, entre otros, son algunos de los medios más utilizados hoy en día para ejecutar acciones de hurto de información y minería de datos.

En los últimos años, estos incidentes han tenido su punto más alto, ya que se han hecho a información financiera de clientes de diversas compañías multinacionales como fue el caso de Sony, donde grupos de hackers ingresaron a servidores de compras online y hurtaron cuentas de tarjetas de crédito de los usuarios, afectando esto la imagen de Sony y cuestionando el manejo de seguridad que se le está brindando a los datos.

La aparición de los ataques de tipo distribuido y los efectos drásticos del número creciente de virus que se propagan en la red, presagian la posibilidad de un enorme *black out* informático. Surgen, de este modo, los primeros sistemas que fueron ideados explícitamente para la protección de la infraestructura como los *routers* y otros sistemas de interconexión [4].

Para contrarrestar las amenazas tecnológicas se han desarrollado varias soluciones informáticas de seguridad que operan de manera independiente, como lo son los firewalls, antivirus, anti-*spam*, etc. No obstante el crecimiento de amenazas y diversificación de los modos de ataque, hacen que estas soluciones que operan individualmente tengan un alto costo operativo y administrativo.

Debido a que los resultados entregados por estas soluciones no se encuentran consolidados en un informe único de sistema de gestión de riesgos, tal que permita hacer una evaluación integral del tipo de incidente de seguridad detectado, es difícil realizar la

trazabilidad y el análisis forense requerido para detectar la posible vulnerabilidad informática que está siendo explotada.

Es a raíz de esto donde se requiere diseñar una solución que integre todas las soluciones ofrecidas a nivel de seguridad informática, sin afectar la operatividad de la empresa, manteniendo un equilibrio entre el nivel de seguridad recomendado y el nivel de operatividad exigido. Con esto se busca que las empresas presten sus servicios comerciales con un margen de riesgo controlable y aceptable.

Para lograr este objetivo se demostrarán las ventajas de implementar un sistema integral de seguridad a través de un Gestor Unificado de Amenazas (UTM), haciendo énfasis en los riesgos más comunes a los que las empresas están siendo expuestas, tales como ataques de denegación de servicio, riesgos por control de acceso y ejecución de malware.

1.1 Riesgos de seguridad en el ciclo de vida de la información

Anteriormente, las Pymes manejaban un modelo reactivo al momento de presentarse un incidente que afectara su estabilidad tecnológica lo cual generaba diversos re-procesos, y estos incidentes al no ser medidos, alcanzaban un alto impacto en la continuidad del negocio. El principal problema es que no se manejaba una base de datos de conocimiento que permitiera reconocer patrones de errores en la organización y generar alertas tempranas que permitan identificarlos oportunamente, para así crear indicadores de seguimiento en su resolución.

1.2 Protección de capas y gestión de riesgos en TI

Las Pymes al verse impactadas de manera económica, optaron por la creación de equipos de trabajo especializados que se encargaran de este tipo de riesgos. Estos equipos de trabajo fueron denominados gerencias de continuidad del negocio o gerencias de manejo de riesgos de TI, en las cuales su principal objetivo es prevenir mediante herramientas que generen datos cuantificables, valores estadísticos y valores históricos, los posibles riesgos tanto a nivel físico o tecnológico inherentes a la propia naturaleza del negocio.

1.3 Modelo relacional probabilístico en la gestión de riesgos de TI

El manejo de seguridad en las Pymes se debe gestionar tanto física como procedimentalmente a un nivel que permita identificar que no hay riesgos aislados y que estos son generados por una cadena de incidentes que desde el punto de vista externo pueden parecer no relacionados, pero analizándolos en detalle se pueden identificar patrones de ataques y dado el caso a que se encuentren asociados a incidentes o riesgos mayores no detectados.

1.4 Método de análisis de riesgos de TI

Las Pymes que no manejen y aprendan de una base de datos de conocimiento de riesgos e incidentes tecnológicos propia y/o ajena, incurre en responsabilidades por omisión, debido a que no está midiendo el riesgo en el impacto tecnológico y económico que implica interactuar en un mercado globalizado en donde cada vez más se exigen estándares de seguridad para poder hacer parte de un sector de mercado específico.

1.5 Gestión de incidentes de seguridad de TI

El ciclo de manejo de los incidentes está basado en el modelo PHVA el cual inicia con una identificación de los incidentes por parte de las Pymes, estos eventos deben ser analizados y documentados a partir de una adecuada detección y control preventivo de las causas que lo han generado, y finaliza con la medición y seguimiento a todo este ciclo del manejo del incidente, enfocándose en los eventos iniciales y en la manera que fueron solucionados.

1.6 Amenazas informáticas

Las Pymes deben contar con la suficiente experiencia para identificar los diferentes tipos de riesgos tecnológicos por los cuales se puede vulnerar su continuidad en el negocio, estos tipos de riesgos pueden ser clasificados como amenazas internas y externas a la empresa.

1.7 Conceptos y retos en la atención de incidentes

Los crímenes y delitos informáticos están teniendo un gran auge debido al incremento exponencial de transacciones en la web, implicando transferencias bancarias y manejo de información de alta criticidad tanto para las empresas como para los usuarios finales.

2. GESTORES UNIFICADOS DE AMENAZAS (UTM)

En el mundo empresarial uno de los bienes más importantes es la información sobre la cual soporta su negocio. Debido a esto, las Pymes requieren implementar una serie de controles que permita evitar de manera proactiva los diferentes ataques a los que su información se ve expuesta.

La información empresarial es un bien intangible de alto valor agregado exclusivamente para sus propietarios, sin embargo, también puede generar interés a individuos dentro y fuera de las Pymes, la cual la pueden considerar de uso vital para cumplir sus propósitos de carácter ilícito.

La alta gerencia de las Pymes, debe estar en la obligación de implementar controles con el fin de garantizarles a los clientes internos y externos el buen manejo y distribución de la información, en este punto están en la necesidad de implementar dispositivos que ofrezcan las características requeridas para este propósito.

Toda empresa y en especial las Pymes que manejen información crítica, deben implementar un área de administración de seguridad informática que les permita contrarrestar los diferentes tipos de ataques y amenazas a los que se ven expuestas como:

- *Bugs***.** Problemas de calidad de sus aplicativos generados de manera malintencionada o por omisión por parte de los proveedores de software.

- *Malware.* Programas enviados a través de otros sistemas ya sean internos o externos de la empresa.

- *Spyware***.** Programas espías dedicados a la recopilación y robo de información.

- *Botnet***.** Ataques generados por fuera de la empresa con el fin de tomar control de los equipos.

- *Spam***.** Correo basura enviado con el objetivo de saturar el servidor de correo.

- *DOS***.** Ataques de denegación de servicio para inhabilitación de los servicios, mediante múltiples peticiones de acceso.

- *Cross-Site Scripting***.** Forzar a un sitio Web para replicar programas ejecutables orientados a los clientes del navegador.

- *Suplantación de Contenido***.** Técnica para engañar a los usuarios presentando información falsa en sitios Web auténticos.

- *Fuga de Información***.** Revelación y robo de información privada y sensible de la empresa por parte de empleados o terceros usando métodos de transferencia electrónica.

- *Intrusión remota***.** Ingreso externo no autorizado a un equipo de cómputo usando la infraestructura de conectividad de la empresa.

- *Fuerza Bruta***.** Proceso de ingreso de credenciales de autenticación de forma masiva para violar sistemas de seguridad.

- *Desbordamiento de Buffer***.** Alteración del normal funcionamiento de un sistema o programa mediante la sobre escritura de espacios de memoria.

- *Inyección LDAP***.** Violentar el acceso a sitios que implementan autenticación vía LDAP mediante enviando credenciales de autenticación falsas del directorio.

- *Inyección de Comandos***.** Envío de comandos dirigidos al sistema operativo y a través de los componentes de ingreso de información a la aplicación.

- *Inyección de SQL***.** Envío de sentencias de SQL a través de los componentes de ingreso de información a la aplicación, para ser ejecutados en la base de datos.

Las Pymes pueden tomar diversas alternativas con el fin de contrarrestar los ataques y amenazas a lo que se pueden ver expuestas, una de estas opciones es adquirir productos especializados en contrarrestar cada uno de estos eventos de manera individual, pero la opción más recomendable, debido a su presupuesto reducido y a que sus prioridad está enfocada en la sostenibilidad de su negocio, es adquirir un producto que se encargue de centralizar la detección y gestión de los diferentes ataques y amenazas, a un costo que se adecue a su presupuesto, este tipo de soluciones son los UTM.

Las características básicas ofrecidas por estos gestores se encuentran en la lista superior de criterios de selección. La idea es simple: si se requiere un antivirus, este debe comportarse como un antivirus. El funcionamiento de los que son configurados como firewall no es tan simple como los que se configuran como antivirus. La mayoría de *firewall* no está en capacidad de examinar el gran número de protocolos que se encuentran en las firmas de los virus, incluso aquellos antivirus que realizan análisis de protocolos a muy alto nivel [5].

Los UTM brindan en un mismo dispositivo, ya sea de hardware o software, una serie de funcionalidades que ayudan a cumplir los requerimientos básicos en seguridad informática y permiten contrarrestar debilidades como:

- Fallos por desconocimiento u omisión en los controles de seguridad en el manejo de la información.

- Ataques informáticos generados por personal interno y externo a la empresa.

- Violación a las políticas de control de acceso y administración de los recursos.

- Mal manejo de los sistemas de información y de las bases de datos de conocimiento empresarial.

Un UTM es una plataforma que brinda conjuntamente múltiples funciones de seguridad en un solo dispositivo de hardware. Pero esto no es siempre la solución más indicada. La Tabla I resume las ventajas y desventajas de la implementación de un UTM [6].

Los UTM son sistemas compactos de hardware o de software los cuales se encargan de agrupar todas las funcionalidades de seguridad requeridas para proteger las Pymes, incorporando entre ellas las características más relevantes de seguridad: Firewall, Filtrado de contenido en la red, Antivirus, Anti-Spyware y Anti-*spam*.

La funcionalidad más importante de un UTM es el Firewall. Su importancia se debe, a que permite realizar una detección temprana de los ataques generados desde el exterior hacia el interior de la empresa, mitigando los riesgos inherentes de la principal necesidad de las Pymes, que es el acceso a contenidos e información en la Web.

TABLA I
Ventajas y desventajas de un UTM

Ventajas	Desventajas
Un único dispositivo para simplificar la arquitectura de red.	Las aplicaciones individuales pueden no tener todas las características de los dispositivos independientes.
Funciones integradas de seguridad para una administración más simple.	Implementación de dispositivos redundantes son requeridos para evitar puntos únicos de falla.
Reportes unificados para dar una imagen completa de la red y su estado de seguridad.	Procesadores compartidos pueden requerir grandes actualizaciones para todo el dispositivo, o descargas de aplicaciones por separado, para evitar problemas de rendimiento.
El personal de Tecnologías de la Información tendrá menos dispositivos sobre los cuales requerirá capacitación.	Las plataformas pueden no soportar todos los tipos de aplicaciones requeridos.

Aunque existen diferencias entre los dispositivos, los principios generales para configurar un UTM son: Ser restrictivo, Obtener granularidad, Estar al tanto de las cosas, Estar alerta, Actualizar regularmente, Mantener contratos de soporte, Considerar, monitorear los servicios de acceso disponibles, Tener cuidado con las VPN, Balancear productividad y protección [7].

3. FUNCIONAMIENTO BÁSICO DE UN UTM PARA LAS PYMES

La principal característica de seguridad en la que se deben de enfocar las Pymes, es asegurar su infraestructura informática al conectarla a la Web para evitar posibles filtraciones y daños a su información de negocio, para esto la opción más recomendable es implementar un UTM de tres niveles en donde se garantice la seguridad las terminales de trabajo, los servidores de procesamiento y almacenamiento de datos y el acceso a Internet.

La evolución de las tecnologías informáticas y el descenso del precio del hardware han hecho que las soluciones perimetrales sean cada vez más asequibles en el mundo empresarial. Sin embargo, para las empresas pequeñas supone un coste importante añadido, la inversión en administración de las protecciones, por lo que demandan una solución integrada de protección contra todo tipo de amenazas [8]. Para cada uno de estos niveles se debe implementar una funcionalidad específica del UTM.

Para proteger la información y las redes de los cada vez más sofisticados retos y amenazas de seguridad, muchas empresas están siguiendo enfoques de aseguramiento en capas. Y son también muchas las que se están dando cuenta de que una manera eficaz de hacerlo es instalar dispositivos UTM [9]. Las principales funcionalidades asociadas al UTM son:

- Bloqueo y filtrado de contenido Web. Acceso a sitios Web que contengan software y/o contenido malicioso tales como sitios de pornografía, juegos en línea, redes sociales, sitios para compras, subastas en línea, descarga de programas, almacenamiento en línea, sitios de farándula, apuestas en línea, videos en línea, etc.

- Bloqueo de puertos de sistema. Controlar el acceso a software de mensajería instantánea tales como MSN Messenger, GTalk, Yahoo Messenger, ICQ, AOL, Skype entre otros y software de intercambio de archivos punto a punto como Emule, Ares, Torrent, etc.

- Bloqueo de archivos específicos. Torrentes, ejecutables, archivos de script como JAR, VBS, JS, archivos multimedia, archivos comprimidos, entre otros.

- Bloqueo de dispositivos extraíbles de almacenamiento. USB, discos duros extraíbles, quemadores de DVD y otros sistemas de almacenamiento.

- Prevención de fuga de información. Monitoreo masivo de datos adjuntos que se envían por correo electrónico, páginas Web de almacenamiento en línea, discos duros virtuales, sistemas de mensajería instantánea.

- Protección de Malware y Spyware. Disminuye en un alto porcentaje el riesgo de infección y propagación de archivos de contenido malicioso que provengan en su mayoría tanto de la red externa, como también de la interna.

- Protección de ataques informáticos. Permite minimizar los impactos producidos por un ataque de denegación de servicio, y un escaneo remoto no autorizado de puertos y servicios.

- Protección frente al correo no deseado. Regula mediante la aplicación de reglas, la recepción y envío de correo masivo y mensajes de contenido restringido como sexo, comercio, racismo etc. y correos que no estén relacionados con las actividades de la empresa.

- Control de ancho de banda y tráfico de la red. Regula la carga y descarga de archivos que sobrepasen el límite permitido por las políticas de control definidas en la empresa, la tasa de transferencia por equipo al acceder a la Web, mediante la implementación de políticas de control del ancho de banda demandada por sitio, contenido y protocolo.

- Creación de redes como DMZ y MZ. Define la segmentación de redes a proteger permitiendo la configuración de zonas seguras y zonas menos seguras.

- Enrutamiento. Posee características de enrutador de red para enlazar las redes y aplicar las políticas que estén definidas en su configuración.

- Proxy. Implementa funcionalidad básica de navegación Web anónima y optimización del ancho de banda por guardar una cache de contenido.

- Firewall para el control de acceso remoto a la Red. Limita y protege del acceso no autorizado a las redes, recursos y servicios de la empresa.

- Redes virtuales privadas VPN (Tunneling). Facilita el acceso remoto a los recursos de sistemas empresariales mediante la creación de redes virtuales seguras.

- Generación de reportes centralizados de la red. Consolida en reportes detallados de eventos como es el uso de ancho de banda, ataques, Spam y Malware detectados, graficas de rendimiento, estadísticas de uso de servicios como lo es la Web y el correo interno.

- Autenticación Single Sign-On. Permite la integración de seguridad con aplicativos que tengan implementadas características de autenticación con LDAP, directorio activo (AD) o RADIUS.

4. ASEGURAMIENTO DE LAS PYMES MEDIANTE UTM

La viabilidad funcional y sostenibilidad financiera de las Pymes está basada en cuatro pilares fundamentales que son Administrativo, Financiero, Tecnológico y Ambiental. Estos deben ser considerados por la alta gerencia, para apoyar al cumplimento de la misión y visión empresarial.

Debido a que una solución global de seguridad requiere de un gran potencial de procesamiento para examinar el tráfico de la red en tiempo real, las soluciones actuales de seguridad todo en uno para Pymes, a menudo utilizan tecnología rudimentaria de seguridad que confunde globalidad con velocidad. Una seguridad completa debe cumplir con ambos requisitos velocidad y cobertura [10].

Al implementar un UTM el impacto en los cuatro pilares administrativos sería el siguiente:

- Administrativo. Desde el punto de vista administrativo, la empresa podrá enfocar todos sus esfuerzos y su operatividad en la viabilidad del negocio, ya que las Pymes al implementar un UTM, pueden delegar el esfuerzo que implica salvaguardar su información administrativa y operacional, a una configuración predeterminada según sus necesidades.

- Financiero. Las Pymes deben alcanzar su sostenibilidad económica durante los primeros años de vida. Para lograr este objetivo, deben centralizar la responsabilidad de seguridad en un solo dispositivo como lo es un UTM, ya que no se verán en la necesidad de adquirir dispositivos adicionales con su correspondiente costo de soporte y administración. Adicionalmente este se encargará de asegurar sus activos de información y con esto podrán ver minimizados los impactos económicos derivados de un posible incidente informático.

- Tecnológico**.** Al no contar con un área de infraestructura muy robusta que amerite una gestión de TI especializada, las Pymes puede destinar los recursos que implicarían gestionar distintos dispositivos de seguridad especializados y centralizar su capacidad en un único UTM.

- Ambiental**.** La legislación internacional exige que las empresas cumplan con unos estándares mínimos de protección ambiental, tecnologías verdes o amigables con el medio ambiente. Con la implementación de un UTM, las Pymes podrán disminuir el consumo de energía eléctrica, minimizar sus emisiones de CO2 y reducir el impacto generado por los excedentes de basura electrónica derivados de la adquisición de otros productos de seguridad no consolidados.

Tareas tales como la operación y la gestión del firewall dedicado, detección de intrusos y sistemas de prevención de intrusiones (IDS/IPS), filtrado de contenidos, encriptación y otros sistemas de seguridad pueden requerir habilidades especiales de los equipos de seguridad de las grandes empresas. Para las pequeñas empresas o sucursales, estas labores son tan abrumadoras que simplemente no se hacen [11].

5. IMPLEMENTACIÓN DEL UTM pfSense

pfSense es una distribución libre de código abierto personalizado basado en el sistema operativo FreeBSD, adaptado para su uso como *firewall* y *router*. Además de ser una plataforma potente, flexible incluye una larga lista de características y un sistema de paquetes que le permite expandir sus funcionalidades sin desbordar su potencial de seguridad [12]. Ofrece bondades de seguridad informática básicas, usando recursos de fácil adquisición por las Pymes, sumado al hecho de una instalación rápida y sencilla, adicionalmente posee los principales módulos de seguridad requeridos.

5.1 Instalación de pfSense

Para la instalación se utilizó un computador con las siguientes especificaciones: procesador de 1 GHz, 512 MB RAM, disco duro de 10 GB y 2 tarjetas de red. Con estas especificaciones el UTM tendrá un rendimiento de 51 a 200 Mbps. La instalación se realiza a través del asistente de configuración, como se ilustra en la Figura 1. Se recomienda implementar la instalación predeterminada ya que ésta se ajusta a la mayoría de las necesidades de las Pymes.

Finalizada la etapa de instalación, se habilitan los módulos de seguridad básicos requeridos como puede verse en la Figura 2. Para este caso se habilitan a través del menú de configuración inicial mediante el gestor de paquetes, los cuales son: Antivirus, proxy y filtrado de contenido.

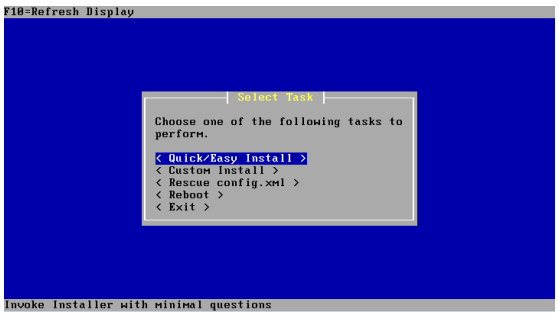

Fig. 1: Asistente de instalación del UTM pfSense

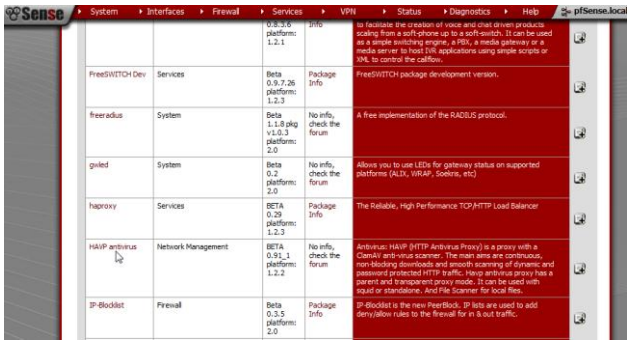

Fig. 2: Módulos que se pueden instalar en el UTM

5.2 Funcionamiento del servidor proxy

El servidor proxy es una aplicación que soporta peticiones HTTP, HTTPS y FTP, entre otras, a equipos que necesitan acceder a Internet y a su vez, provee la funcionalidad de caché especializado que almacena de forma local las páginas consultadas recientemente por los usuarios. De esta manera, incrementa la rapidez de acceso a los servidores de información Web. También puede operar de forma transparente ya que las conexiones son direccionadas dentro del mismo servidor proxy sin configuración adicional por parte del cliente para su navegación en internet, visto de otra forma, el navegador Web no necesita ser configurado para que aproveche las características del servidor proxy. La Figura 3, muestra la activación del servidor proxy transparente en el UTM pfSense.

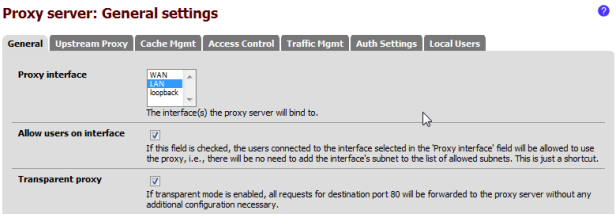

Fig. 3: Proxy transparente en pfSense

5.3 Funcionamiento del antivirus con HAVP

HAVP es un módulo integrado de proxy y antivirus para el contenido Web como se observa en la Figura 4, éste módulo nos brinda un nivel de seguridad alto, garantizando que la plataforma esté protegida de ataques generados por Malware o programas espías, además controla la navegación Web, así como recursos usados. Las actualizaciones periódicas automáticas ayudan para que se mantenga los niveles de protección en las Pymes.

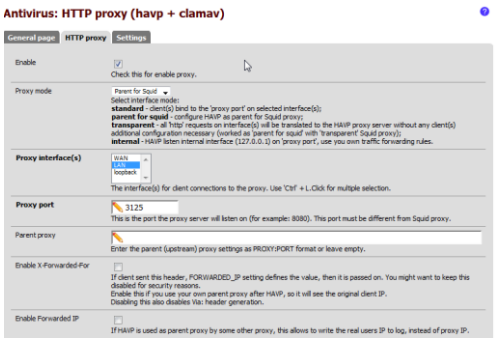

Fig. 4: Integración de Proxy + Antivirus

5.4 Creación de reglas en el Firewall

Para la implementación del Firewall se crean reglas, las cuales se implementan de manera que garanticen la mayor protección posible sin afectar el rendimiento del sistema. pfSense está dividido por etapas y protocolos. El usuario configura estos parámetros dependiendo de las necesidades de su empresa, la Figura 5 indica que solo se permite el acceso web a la Internet por los protocolos comunes DNS, HTTP y HTTPS.

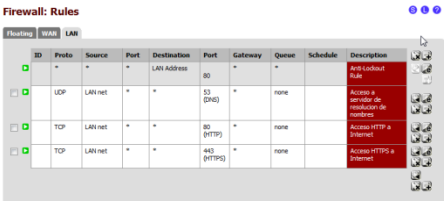

Fig. 5: Firewall aplicado a la red WAN y LAN

5.5 Listas de Control de Acceso

Uno de los módulos más destacados en el UTM pfSense, es el de las listas de control de acceso de direcciones web y/o expresiones no permitidas como sexo, racismo, entre otras, las cuales permiten gestionar, bloquear y usar de modo seguro, la navegación en internet, con lo que se garantiza a las Pymes que sus empleados hagan correcto uso de los recursos informáticos, la Figura 6 ilustra el gestor de las listas de control de acceso.

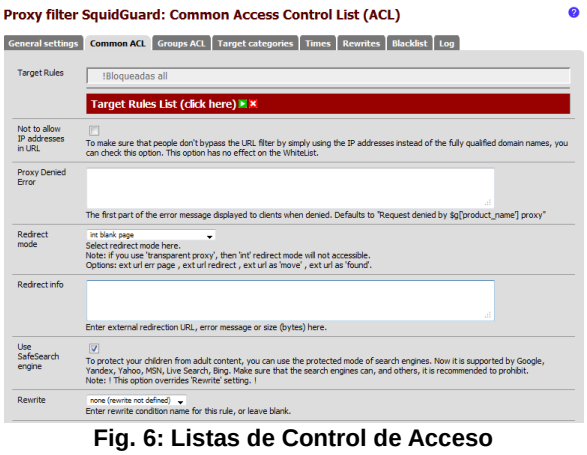

Fig. 6: Listas de Control de Acceso

5.6 Bloqueo de páginas con virus

Una vez configurado el UTM pfSense con el módulo integrado de proxy y antivirus, bloqueará las páginas

que contengan malware, mostrando un mensaje de alerta como lo indica la Figura 7.

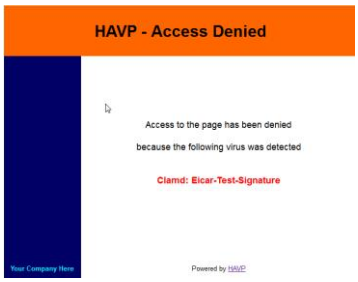

Fig. 7: Bloqueo de Páginas con Virus

5.7 Reportes y estadísticas

Los informes de estadísticas de uso como los que se muestran en las Figuras 8 y 9, son generados con el fin de que las Pymes puedan evaluar el uso dado de los recursos de Internet, permitiendo ver reportes de consumo de ancho de banda, páginas visitadas y número de ingresos, entre otros, con el fin de tomar decisiones como: la limitación selectiva a internet para ciertos empleados, verificar la calidad del servicio de internet y apoyo a los procesos de auditoría.

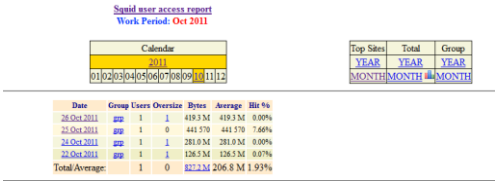

Fig. 8: Consumo de ancho de banda

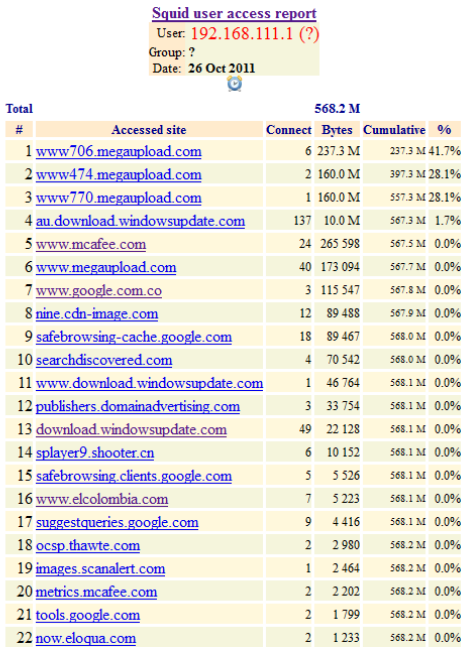

Fig. 9: Páginas visitadas y número de

6. CONCLUSIONES

Las Pymes deben considerar adaptarse a los requerimientos de seguridad informática actualmente exigidos por las entidades de regulación de comercio electrónico internacional, para poder asegurar una continua expansión de su mercado tanto a nivel nacional como internacional.

Dentro de los gastos presupuestados para las Pymes, se debe considerar un rubro dedicado exclusivamente al mantenimiento y soporte de su plataforma tecnológica, en especial el relacionado con el aseguramiento de su base de datos de conocimiento e información relacionada con sus clientes.

Desde el punto de vista funcional, la implementación por parte de las Pymes de un UTM como dispositivo de aseguramiento para su plataforma tecnológica es la mejor alternativa, debido a que podrán encaminar sus esfuerzos en alcanzar su punto de equilibrio económico y operativo.

7. REFERENCIAS

[1] J. E: Ojeda-Pérez et at. “Delitos informáticos y entorno jurídico vigente en Colombia”. *Cuadernos de Contabilidad*, Vol. 11, No. 28, pp. 41-66, 2010.

[2] K. J. Molina et al. Firewall - Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas). *UIS Ingenierías*, Vol. 8, No. 2, 2009, pp. 155-165, 2009.

[3] J. J. Cano. “Inseguridad Informática: Un Concepto Dual en Seguridad Informática”. *Revista de Ingeniería*, No. 19, mayo, pp. 40-44, 2004.

[4] S. Brusotti; G. Lamastra & M. Leone. "e-commerce security issues". *Notiziario Tecnico Telecom Italia*, Vol. 11, No.3, pp.37-56, 2003.

[5] J. Snyder. “How to select enterprise UTM firewalls”. *Network World*, Vol. 24, No. 34, pp. 38-40, 2007.

[6] D. J. Engebretson. “UTMs are not for everybody”. *Security Distributing & Marketing*, Vol. 37, Supplement, pp. 7, 2007.

[7] M. Sarrel. “Unified Threat Management”. *PC Magazine*, Vol. 27, No. 3, pp. 102-102, 2008.

[8] J. M. Crespo. “El valor añadido de los appliance UTM para la Pyme”. Online [Mar. 2011].

[9] A fondo. “UTM: seguridad “todo en uno””. Network World, No. 10, pp. 24-28.

[10] NETGEAR. “Dispositivo ProSecure Para la gestión Unificada de las amenazas”. Online [Mar. 2011].

[11] G. Hulme. “Unified Threat Management for SMBs”. *Channel Advisor*, pp.15-16, spring, 2008.

[12] http://www.pfsense.org/