ARTÍCULO MONOGRÁFICO

UTM: Administración Unificada de Amenazas*

[UTM:Unified Threat Management]

Yamil Casas-Moreno[1]

***Recibo**: 16.12.2009 - **Ajuste**: 31.01.2010 - **Ajuste**: 02.05.2010*
***Aprobación**: 06.05.2010*

Resumen

UTM es el dispositivo de hardware perimetral que se está imponiendo en la actualidad en las grandes organizaciones ya que controla todo tipo de tráfico entrante, saliente y malintencionado a través de avanzadas técnicas de detección y sincronización de datos.

Según la forma en que este se desempeñará en la red, esta herramienta de seguridad tiene diferentes clasificaciones y la selección de la herramienta adecuada dependerá del criterio del analista de red que determinará la solución más correcta.

El equilibrio de carga es la base del funcionamiento de este hardware ya que él determina la rapidez con que se establecerá el control de flujo de todo el tráfico entrante y saliente a la red en la que se implemente.

Es un esfuerzo de las grandes compañías desarrolladoras por mejorar el rendimiento en diferentes redes y evitar la implementación de un sin número de herramientas para solucionar cada riesgo informático ya que las unifica todas, centralizando así el control de la seguridad.

La presente monografía pretende realizar un recorrido por diferentes conceptos relacionados con esta tecnología y dar un panorama a los interesados sobre su aplicabilidad, funcionalidad y estado del arte en el mundo de la seguridad informática.

* Modelo para citación:
CASAS MORENO, Yamil (2010). UTM: Administración Unificada de Amenazas. En: Ventana Informática. No. 22 (ene-jun., 2010). Manizales (Colombia): Universidad de Manizales. p.173-185. ISSN: 0123-9678

1 Ingeniero de Sistemas y Computación.
Coordinador de Sistemas COODESCA, Manizales, Caldas, Colombia. Correo electrónico: yamil100co@yahoo.com.mx

Palabras Clave: *UTM, seguridad informática, equilibrio de carga, protección en redes.*

Abstract

UTM is the hardware device perimeter that is developing now in the large organizations because controls all kind of traffic inbound, outbound and malicious through advanced detection techniques and data synchronization.

Depending how this will work in the network, this security tool has different classifications and the selecting the right tool will depend on the criterion network analyst that it will determine the correct solution.

Load balancing is the basis of how work this hardware because it determines the speed to be established flow control of all incoming and outgoing traffic to network that is implemented.

It is an effort by the major company provider of improve performance in different networks and avoid implementation of a myriad of tools to solve each computer risk because the unifies all centralizing control and security.

This paper tries to make a tour different concept related to this technology and give picture to stakeholders about its applicability, functionality and state of the art in the world of computing security.

Keywords*: UTM, computing security, load balancing, protection networks*

Introducción

En la actualidad, las amenazas informáticas se han convertido en uno de los temas más apasionantes y a su vez complicados para los encargados de la seguridad y las redes en las diferentes organizaciones, ya que la constante evolución de las herramientas y técnicas de ataques, son proporcionales a los avances de las herramientas y técnicas de contención trayendo como consecuencia que la optimización de recursos y un control más efectivo, sean claves al momento de determinar los dispositivos que se requieren en un área para el control de amenazas.

Es por ello que herramientas como UTM (*Unified Threat Management*) se constituyen en elementos de gran ayuda ya que en una sola herramienta se concentran diferentes agentes de control de amenazas, facilitando así el trabajo de los jefes de seguridad y de los usuarios de la red controlada.

Según Watchguard (2007), UTM es una tendencia emergente en el mercado de seguridad de redes. Los dispositivos UTM son una evolución de los tradicionales *firewalls* y VPN (red privada virtual) y se convirtieron en una solución que tiene muchos elementos adicionales, como filtro de páginas, bloqueo de *spam*, protección contra *spyware*, prevención de intrusos y antivirus de *Gateway*, adicionalmente ofrece la posibilidad de realizar una administración integrada, monitoreo y registro. Todas estas funciones eran anteriormente logradas sólo con la adquisición de distintos sistemas específicos.

La posibilidad de unificar perimetralmente la administración de los diferentes dispositivos de seguridad en la red se ve soportado en sus resultados gracias al equilibrio de carga, aunque trae consigo un debate muy interesante en el que se debe decidir si se logra esta solución, trayendo como consecuencia la pérdida de rendimiento o mantener los sistemas tradicionales administrados de manera singular y aumentando la complejidad de la administración aunque con una mayor eficiencia en cuanto a resultados.

1. Generalidades de UTM

Las amenazas a la seguridad de las redes y los sistemas informáticos se han convertido en una interminable lucha dada por personas que tratan de vulnerarlos y otros que intentan detenerlos.

Las técnicas, metodologías y herramientas para contener los agentes agresores, han evolucionado y la complejidad a la que se ha llegado hace que sean necesarios métodos más ágiles y flexibles para su administración además de ser efectivos.

Año a año se presentan, en altos porcentajes, todo tipo de ataques y amenazas informáticas que hace poco tiempo atrás no eran muy comunes, por lo que no es de extrañar que las empresas sigan considerando la seguridad TI como una de las máximas prioridades durante los próximos años.

Dado que no hay muchos profesionales en seguridad informática, las empresas han optado por buscar soluciones informáticas que sean fáciles de configurar, manejar y al mismo tiempo de gestionar hasta por usuarios de más bajo perfil en cuanto a conocimientos informáticos.

«Las amenazas a las redes son cada vez más sofisticadas, debido a que los agresores lanzan ataques dirigidos utilizando formas combinadas. En la actualidad, las redes de las empresas se ven amenazadas por

una combinación de amenazas externas tales como virus, gusanos, programas espía, troyanos, *phishing, pharming y cross-site scripting*.

El enfoque tradicional consistente en implementar únicamente firewalls y soluciones antivirus que ya no son suficientes y las empresas necesitan soluciones de seguridad múltiples para enfrentarse a las amenazas combinadas contra las redes» (Infosecurity Bureau, 2007). En cuanto a los datos informáticos, los usuarios de las empresas representan la mayor amenaza a la seguridad, ya que tienen fácil acceso a información corporativa sensible, aplicaciones y recursos de la red, y pueden poner en peligro la seguridad debido a su desconocimiento o malas intenciones.

Por este motivo, los dispositivos UTM, están tomando mucha fuerza y aceptación en los encargados de la seguridad de las redes de las diferentes organizaciones, ya que cambian el concepto tradicional de seguridad perimetral a una solución integrada de protección unificada contra todas las amenazas, facilitando la gestión desde una sola interfaz de administración de un modo muy simple e indiferente del usuario que lo manipule.

Los dispositivos de gestión unificada de amenazas se están convirtiendo en una solución bastante aceptada en las arquitecturas de seguridad en el mundo. Según Infosecurity Bureau (2007), une capacidades de seguridad muy ampliamente utilizadas como antivirus, *antispam*, detección de intrusos, *firewall* entre otros que normalmente se encuentran en el mercado como soluciones independientes de software y que aquí se reemplaza en una sola herramienta *hardware* y de un mismo fabricante evitando así a los administradores conocer configuraciones de distintas fuentes y además centralizar el control, liberando la carga de actualizaciones a los computadores de los usuarios y diferentes servidores.

«Desde que, hace muy pocos años, Charles Kolodgy, analista de seguridad de IDC, bautizara con las siglas UTM a los dispositivos de seguridad multipropósito que comenzaban a comercializarse en ese momento, este nuevo mercado no ha dejado de crecer, generando ya en 2006 un volumen de ventas de 850 millones de dólares. Se trata de un negocio en el que participa todo tipo de agentes, desde los centrados en la gama alta, como Fortinet, a los dirigidos especialmente a las pymes, como SonicWall, sin olvidar a Cisco» (Network World, 2010).

A pesar de que es una herramienta muy poderosa y ofrece tantas ventajas, se debe tener en cuenta de que hay ciertos escenarios y

situaciones donde no es viable su implementación. Para Network World (2010), uno de los principales problemas es que se apoyan en complejos requerimientos de procesamiento de paquetes que acaban por impactar el rendimiento.

No es infrecuente que tal impacto reduzca el rendimiento hasta en un 50% (aunque algunos suministradores no reconocen una pérdida superior al 10%) cuando se activan todas las funciones; un inconveniente común tanto a los dispositivos UTM de baja gama y a los preparados para soportar velocidades de varios *gigabits* por segundo.

«El problema, obviamente, no pasa desapercibido a los fabricantes, que algunas veces aconsejan a sus clientes compensarlo con más ancho de banda o el despliegue de tecnologías de aceleración de hardware para mejorar la capacidad de proceso y reducir la latencia.

Sus ventajas pueden compensar fácilmente sus inconvenientes, pero según los expertos, no es recomendable contar con un único punto de mitigación de riesgos a través del cual fluya todo el tráfico cuando la red cuenta con docenas, cientos o miles de localizaciones; y por varias razones. Hay responsables de TI que son reacios a poner todas sus herramientas de seguridad en un mismo punto, por cuanto tales despliegues suponen un único punto de fallo. No obstante, se puede soslayar este inconveniente instalando UTM en forma redundante con propósitos de *failover*, lo que ofrece mayores niveles de disponibilidad. Además, como en las redes de gran tamaño la capacidad de proceso real es una cuestión crítica, los responsables de TI a menudo prefieren distribuir la protección contra retos en vez de centralizarla, simplemente para reducir la probabilidad de que se produzca un cuello de botella del rendimiento» (Network World, 2010).

1.1 Características

Estos dispositivos reúnen en un solo *hardware* diferentes servicios de seguridad (conocidas como esenciales) y que se implementa en el punto perimetral del área de red, pero a pesar de estar en auge en la actualidad, no es un tema nuevo en el ámbito de la informática ya que marcas como *Fortinet* y *Check Point* desde hace mucho tiempo no han ahorrado esfuerzos en desarrollar y mejorar este tipo de dispositivos y darlos a conocer en el mercado.

Según Requejo e Hijas (2007), en seguridad es ampliamente conocido el hecho que entre más servicios en un dispositivo se encuentren activados, más posibilidades de ataques se pueden presentar ya que es a partir de los puertos que se encuentran habilitados que la mayoría

de amenazas se aprovechan para explotar las vulnerabilidades de los equipos y hacer daño.

Teniendo en cuenta lo anterior, es muy común ver un servidor destinado a realizar un control de un área determinada y con un servicio especial dejando los demás controles a otros servidores, cada uno con su servicio específico. La modalidad mencionada no sólo concentra una gran cantidad de gastos en recursos tecnológicos, *hardware-software*, sino también recursos humanos para garantizar el buen funcionamiento de toda esa arquitectura.

La modalidad UTM, libra todo esto, llegando a concentrar, no sólo un solo dispositivo sino también un administrador, su control. Ello no asegura que en todos los casos vaya a satisfacer todas las necesidades de la organización al nivel de las herramientas de control esencial que se encuentran ahí, ni tampoco garantiza que la gestión se va a facilitar, para ello se requiere de un análisis detallado de necesidades y de recursos para evaluar su viabilidad.

Hay escenarios en las organizaciones en las que cada elemento de seguridad es gestionado por una parte diferente de la estructura interna; unificar la gestión en este caso puede complicar el planteamiento anterior por los diferentes equipos que han de convivir en el mismo entorno.

La facilidad en el uso y la gestión tiene su contrapeso con la pérdida de calidad y de la arquitectura de seguridad, y a esto se le debe sumar el hecho de que el sistema va a bajar su rendimiento notablemente ya que, a pesar de ofrecer servicios de seguridad básicos, requieren de mucho procesamiento de máquina, lo cual implica que el sistema pueda tornarse algo lento.

Para Requejo e Hijas (2007), esta problemática hace que los diferentes proveedores de sistemas UTM avancen en sus soluciones y actualmente se tenga un gran abanico de posibilidades, aunque las diferencias entre proveedores se presentan sólo en puntos como: Ancho de banda soportado, Número de interfaces y Servicios ofrecidos.

1.2 Clasificación

Dentro de las diferentes gamas conocidas, se pueden clasificar las soluciones UTM, partiendo de lo propuesto por Requejo e Hijas (2007), como:

- Soluciones que en una sola plataforma *hardware* disponen de un motor multifunción propio que realiza todo el procesamiento del tráfico.
- Soluciones que integran una base de tecnología propia y que acompañan con algún producto complementario de otras compañías.

- Soluciones que virtualizan la ejecución de varios motores en una única plataforma hardware, consiguiendo la simplificación de la arquitectura resultante.
- Soluciones que han convertido su mensaje de plataforma *best of breed* (por ser gama alta de hardware, capaz de ejecutar múltiples aplicaciones) a UTM (por ser gama alta de hardware, capaz de ejecutar múltiples aplicaciones simultáneamente).
- Productos y/o plataformas que ampliando su funcionalidad básica (que sigue siendo el *core* de la solución) incorporan características UTM y que se presentan como soluciones globales.

Para Fortinet (2009), independiente de la clasificación anterior, la tecnología UTM busca:

- Minimizar los riesgos de seguridad en los negocios.
- Reducir la sobrecarga de trabajo en la administración de la seguridad de las organizaciones y dar un uso más eficiente al personal interno.
- Mejorar la infraestructura de seguridad existente.
- Aumentar los niveles de cobertura en la gestión y administración de la seguridad.
- Minimizar los gastos de múltiples dispositivos y a la vez maximizar la protección.
- Acelerar la resolución de incidentes sin la necesidad de contar con personal experto en el área.
- Centralizar la administración.
- Facilidad de mantener una política global y coherente a los dispositivos de apoyo en seguridad.
- Monitoreo y registró en tiempo real de todo lo ocurrido.

El diferenciador clave para determinar que un dispositivo realiza UTM es tener la capacidad de inspeccionar y determinar si los paquetes de datos que analiza, individuales o múltiples, son una amenaza, en otras palabras, debe proporcionar una inspección profunda de paquetes a través de escaneos internos.

«Seleccionar cortafuegos UTM para un entorno corporativo es más complicado que elegir un firewall estándar, porque en general no se dispone de mucha información sobre lo que realmente hacen. A la hora de evaluar productos de este tipo, hay cuatro cuestiones clave a considerar: rendimiento, prestaciones, integración de red y gestión.

Puede que se den muchos solapamientos en todas ellas en relación con los requerimientos de los cortafuegos convencionales, pero deben

ser considerados a la luz de las necesidades específicas de la gran empresa en cuanto a rendimiento y fiabilidad» (Network World, 2010).

Aunque los *firewalls* tradicionales sólo miran el paquete de datos de donde viene y su destino, más el número de puerto que está usando y que es conocido como un escaneo de capa cuatro, la exploración a través de un dispositivo UTM también debe ser capaz de realizar un análisis de los contenidos de cada paquete que se envía o se reciben. Esto se conoce como escaneo de capa siete.

2. Equilibrio de carga

Los productos UTM de alta gama permiten a los administradores de seguridad en las redes de las organizaciones, utilizar todos los servicios ofrecidos con un gran rendimiento ya que utilizan lo que se conoce como *equilibrio de cargas UTM*.

Según SonicWall (2009), el equilibrio de carga como se puede apreciar en su estructura en la figura 1, cuenta con un motor de inspección de paquetes y de clasificación de datos que a una alta velocidad y a través de distintos núcleos de seguridad permite inspeccionar en tiempo real aplicaciones, archivos y tráfico sin que esto repercuta en el rendimiento.

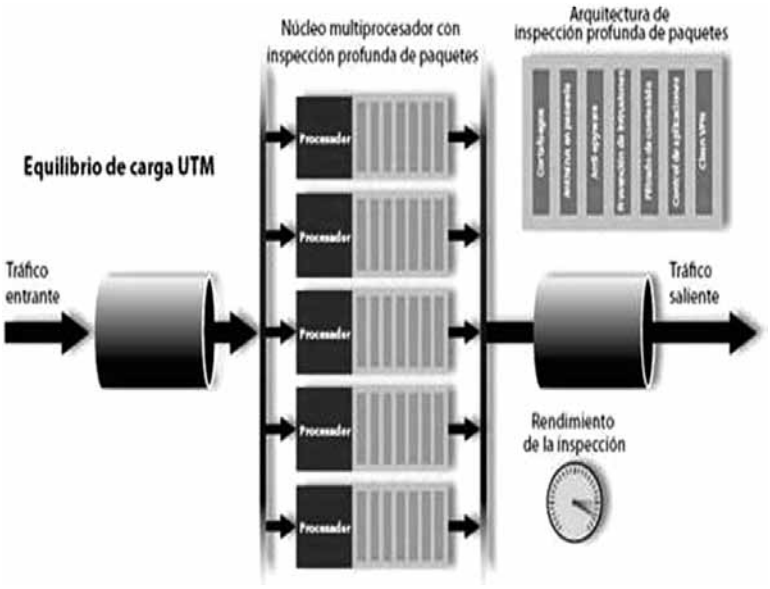

Figura 1. UTM – estructura interna en el equilibrio de carga (Sonicwall, 2009)

El mecanismo, es la base para que esta herramienta pueda soportar todo el tráfico entrante y saliente, además de eso determinar a través de las distintas aplicaciones, cual es el tratamiento que se le debe dar a los datos y los recursos que requiere para que sea conducido por el canal correcto sin pérdida de información y con la rapidez suficiente.

«Los cortafuegos UTM son especialmente atractivos cuando el rendimiento es un factor clave, ya que permiten escalar mediante actualizaciones sencillas, añadiendo mejoras en el chasis o sistemas en una configuración de balanceo de cargas activo/activo. Pero es mejor comenzar con un sistema que corra tan rápido como precise nuestra red y darse un tiempo hasta la próxima actualización» (Network World, 2010).

3. Protección

Visto de manera global en que consiste la solución UTM en seguridad informática, a continuación se presenta un conjunto de amenazas informáticas, a partir de Check Point (2009) (y resumidas en la figura 2), para las cuales servirán las soluciones UTM:

- Virus, Gusanos, Troyanos: *software* que ocultan código malicioso y que pueden, de diferentes maneras, afectar el buen funcionamiento de un sistema de información, destruir información o reportar datos confidenciales a usuarios no autorizados dentro y por fuera de la red.
- *Spyware*: *software* encargado de espiar la actividad de los usuarios que lo contienen.
- *Adware*: *software* con anuncios publicitarios que se almacenan en los equipos de cómputo y que resultan ser muy molestos para los usuarios.
- Acceso no autorizado a la red u a otros dispositivos en el área.
- Ataques de denegación de servicio (*DoS*), obstruyendo los canales de comunicación y dejando fuera de servicio el recurso afectado.
- *Spam*: o correo basura el cual inunda de correos no deseados los servidores de correo de las organizaciones que cuentan con este servicio.
- Acceso no autorizado a sitios por fuera de la red o páginas no autorizadas por los usuarios internos de una organización.
- NAT: traducción de direcciones de red privada con la que se pueden proteger las direcciones IP que hacen parte de la red interna.
- Filtrado de paquetes a través la *QoS* (calidad de servicio) para gestionar el tráfico en una red.

- Protección contra el día *Zero*: Es bien conocido que las nuevas amenazas informáticas tradicionalmente deben pasar primero por un proceso de reconocimiento para encontrar su solución y anexarlo a la base de datos de firmas. UTM cuenta con módulos que pueden anticiparse a esto y detectar posibles nuevas amenazas.

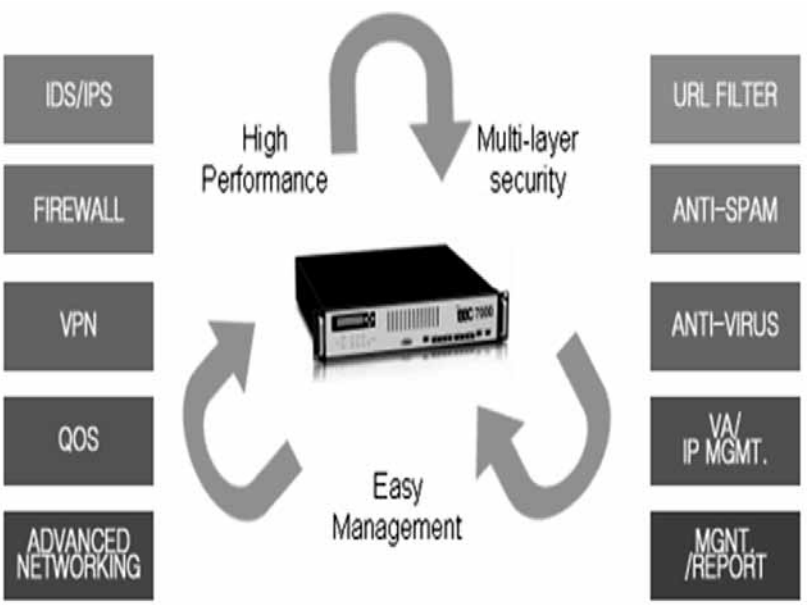

Figura 2. Amenazas controladas con UTM (Infosecurity Bureau, 2007)

La protección contra las anteriores amenazas se logra tanto para tráfico entrante como saliente. De acuerdo con Network World (2010), su funcionamiento consta de:

- El tráfico entrante se desencripta, si es necesario, en el módulo correspondiente antes de que se inicie la inspección en el módulo de cortafuegos.
- El dispositivo de análisis de datos relaciona las inspecciones realizadas por los distintos módulos y dispositivos UTM, descartando cualquier tráfico que suponga una amenaza.
- El dispositivo de análisis vuelve a unirlas cargas útiles de los paquetes para que el dispositivo antivirus y los módulos de filtrado y antispam analicen el contenido. Cualquier tráfico sospechoso se descarta.
- El módulo de encriptación reencripta el tráfico *VPN* y otros del mismo tipo que vayan cifrados.

- Todos los retos se reportan al módulo de *logging* e informes, dedicados a activar alertas en condiciones determinadas y para realizar un análisis forense.

4. Actualidad

Vincular la identidad del usuario a la seguridad es uno de los retos que han llevado a otro nivel los conceptos en la seguridad informática y con esta técnica, se puede realizar un control detallado a los diferentes usuarios en una red y con alcances que no son posibles a través de la seguridad basada en direcciones IP. Esto ayuda a una empresa a cambiar fácilmente su política de seguridad desde el punto de vista de los usuarios y sin presentar traumas en el proceso de cambio.

Según Infosecurity Bureau (2007), Independiente de la ubicación en la red y de los cambios de posición que este pueda tener, a través de la seguridad basada en identidad se puede controlar el cambio de derechos y privilegios que los usuarios puedan tener.

UTM basado en identidad es la técnica que está en auge actualmente ya que vincula los aspectos citados a todos los privilegios ya conocidos de la tecnología tratada. Dentro de las ventajas que esta técnica puede tener en UTM están:

- «Identifica y controla a los usuarios en cualquier lugar de la red mediante la identificación y reporte del nombre de usuario, permitiendo el ajuste de la política por nombre de usuario.
- Ofrece elevados niveles de seguridad incluso en entornos de IP dinámica, gracias a la identificación del usuario incluso en entornos DHCP (*Dynamic Host Configuration Protocol*) y Wi-Fi (*Wireless Fidelity*).
- Permite el control de amenazas en tiempo real mediante el reporte basado en la identidad del usuario con una clara visualización del uso y los patrones de amenaza de cada usuario. Facilita la gestión de la conformidad con las regulaciones, informando de “quién está accediendo a qué”.
- Agiliza los ciclos de auditoría e información, además de controlar fuga de datos.Sus plantillas de conformidad incorporadas ofrecen informes críticos acerca de los usuarios y las actividades, con el fin de satisfacer requisito» (Infosecurity Bureau, 2007).

5. Conclusiones

- En la actualidad las tecnologías tienden a ser más sencillas, compactas, ágiles además de funcionales como lo demuestra UTM, pero es una alternativa que no va a sustituir completamente la seguridad perimetral tradicional ya que dependiendo de las necesidades de cada organización se puede determinar su uso.
- Es un paso adelante en la simplificación de las operaciones de seguridad en las organizaciones pero no necesariamente la mejor solución en cualquier situación por lo que es conveniente hacer un análisis del área en que se implementará para determinar su viabilidad.
- La cantidad y diversidad de software malicioso y de ataques informáticos hace que el trabajo de un administrador de seguridad en la red se haga muy complejo y es allí donde la determinación de la viabilidad de un dispositivo como UTM puede ser considerado.
- La base del buen funcionamiento de esta tecnología es el equilibrio de carga y es a partir de este que se puede inspeccionar todo tipo de tráfico entrante y saliente a una gran velocidad sin afectar el rendimiento.
- El reto actual en los desarrollos de tecnologías basados en el concepto de UTM es la vinculación de la identidad del usuario en la red con lo que se pretende mantener las políticas de seguridad independiente de los cambios que se den en la red.

Bibliografía

CHECK POINT. (2009). Seguridad para todas las empresas. [en línea]. Barcelona (España): MC Ediciones <http://www.revistatcn.com/wp-content/uploads/diptico-check-point-2.pdf> [Consulta:20/08/2009]

FORTINET. (2009). FortiMail, Seguridad Integral en Tiempo Real. [en línea]. Sunnyvale (CA, USA): Fortinet Inc. <http://www.mambonet.com/fabricantes/fortinet/Fortinet_Seguridad_Integral_en_Tiempo_Real.pdf> [Consulta: 12/11/2009]

INFOSECURITY BUREAU (2007). Unified Threat Management: Experience the all in one. [en línea].En: InfoSecurity, Vol. 1, No. 5 (mar, 2007). Nueva Delhi (India): Fanatic Media. p. 14-19. <www.cyberoam.com/images/news/InfosecurityUTM.pdf> [Consulta: 12/09/2009]

INTECO. (2009). Gestión unificada de amenazas (UTM). [en línea]. León (España): Instituto Nacional de Tecnologías de la Comunicación, INTECO. <www.inteco.es/extfrontinteco/icd/pdf/18_20071003_01_Gestion_unificada_amenazas.pdf> [Consulta: 01/08/2009]

JUNIPER NETWORK. (2008). Branch Office UTM Implementation Guide. [en línea]. Sunnyvale (CA, USA): Juniper. <www.pmi.it/file/whitepaper/000351.pdf> 22 p. [Consulta: 02/08/2009]

NETWORK WORLD. (2010). UTM también para la gran empresa. [en línea]. Madrid: IDG COMMUNICATIONS, S. A. U. <http://www.networkworld.es/UTM_Tambien-para-la-gran-empresa/seccion-/articulo-185976> [Consulta: 04/27/2010]

REQUEJO, Antonio e HIJAS, Javier (2007). UTM: ¿Cuestión de valores?. [en línea]. En: Experienci@s. Madrid: Grupo Gesfor. <http://www.germinus.com/htm/02/CasosExito/seguridad/UTMCuestiondevalores.pdf> [Consulta: 19/09/2009]

SONICWALL. (2009). Protección UTM de próxima generación. [en línea]. Madrid: Sonicwall Iberia. <www.sonicwall.com/downloads/DS_ES_NSA_Series_A4.pdf> [Consulta: 28/08/2009]

WATCHGUARD. (2007). El Activo más Poderoso en su Sistema de Defensa de la Red. [en línea]. Seattle (WA, USA): Watchguard. <http://www.watchguard.com/docs/brochure/wg_utm_zeroday_es.pdf> [Consulta: 13/09/2009]

ZYXEL. (2007). UTM how unified threat management (UTM) can help businesses win the security battle. [en línea]. Wokingham (UK): ZYXEL. <http://www.zyxel.co.uk/upload/doc/ZyXEL_WHITE_PAPER_UTM_0107.pdf> [Consulta:29/09/2009]