

Appliance UTM U450 de Netasq

En el presente laboratorio se identifica, examina, analiza, valora y evalúa UTM U450 de Netasq, una herramienta de seguridad de red, en principio para medianas empresas, escalable, robusta y de buen rendimiento, de naturaleza hardware-software, del tipo UTM que opera sobre interfaces Ethernet 10/100/1000 bajo la pila de protocolos TCP/IP. Integra un amplio conjunto de funcionalidades como *firewall-stateful*, *proxy*, IPS/IDS en tiempo real basado en el motor ASQ, opera a nivel L2 y L3, combina protección con firmas contextuales, análisis estadístico de comportamiento y protocolos, antivirus/anti-spyware, filtrado URL web, anti-spam, gestión de vulnerabilidades y análisis de riesgos (tecnología SEISMO Netasq), servidor-cliente DHCP y cliente NTP. Soporta gestión VLAN y clientes PPTP, VPN-SSL/VPN-IPSec. Incorpora funcionalidades de alta disponibilidad y proporciona funciones de red, QoS y *routing* (*routing* estático basado en políticas y dinámico con RIP-BGP-OSPF), limitación-garantía de ancho banda, gestión de ancho de banda basada en prioridad, DiffServ filtering/marking, y NAT/PAT. Igualmente, incluye autenticación de usuarios, PKI con LDAP, BD interna, autoridad de certificación, autenticación transparente, certificados SSL y SPNEGO de Microsoft. Al tiempo, incorpora una GUI muy bien dimensionada y rica en ayudas para facilitar la gestión centralizada (local o remota) de todas las funcionalidades del *appliance* UTM U450, pudiendo generar informes personalizados a medida.

IDENTIFICACIÓN DE LA HERRAMIENTA. PRINCIPALES FUNCIONALIDADES

La herramienta de seguridad hardware-software Netasq con *Appliance U450*, de la compañía Netasq, puede ser catalogada como un sistema multi-funcional basado en una o varias

UTM U450



unidades hardware desplegadas tipo *appliance* UTM, administradas desde un potente sistema de gestión centralizado basado en GUI que incluye un cuadro de mando. Se han podido constatar en esta evaluación, entre otras, las siguientes

funcionalidades más relevantes:

(1) **Filtrado URL Web.** Permite controlar la navegación web de los empleados por Internet; asimismo protege de ciertos ataques como *phishing* y *malware-virus*, prohibiendo el acceso de los usuarios a sitios potencialmente peligrosos. Se combina con filtrado *Optenet*, que soporta un motor de actualización automática robusto y profesional.

(2) **Motor antispam bimodal.** Combina dos grupos de tecnologías en paralelo de análisis, una basada en listas negras DNS y otra basada en análisis heurístico (en cabeceras de mensajes y contenidos mediante reglas empíricas, análisis semántico, contra-reacciones y detección de código HTML embebido).

(3) **Encaminamiento dinámico.** Permite gestionar diferentes protocolos de encaminamiento dinámico L3 (nivel 3) como RIP v1/2, OSPF v2 y BGP v4. Esta funcionalidad permite la modificación automática del encaminamiento de tráfico en el caso en que un dispositivo de red, que normalmente transmite tráfico, deje de estar disponible. Esta característica, presente en plata-

formas dedicadas, permite al *appliance* de seguridad unificado aquí evaluado operar con diversas opciones, como *firewall*, IPS, VPN, QoS, filtrado de contenido URL, etc.

(4) **Funcionalidades Firewall-IPS/IDS.** ASQ es el motor de prevención de intrusiones de los *apliances* Netasq. El motor IDS/IPS se encuentra embebido en el núcleo del sistema operativo (en el nivel de *driver* de red), tiene capacidad para acceder a todos los recursos (CPU y memorias) del *appliance*. Intercepta el tráfico en tiempo real sobre el flujo de red original en el nivel *driver* del hardware. Combina las siguientes tecnologías: i) *Análisis de protocolos.* Seguimiento de protocolos, comprobaciones de seguridad y normalización de flujo. ii) *Análisis de comportamiento.* Detección de comportamientos anómalos, como escaneos, inundación, canales encubiertos, etc. iii) *Firmas contextuales de protección de día cero.* Utiliza más de una treintena de bases de datos de firmas; cada base está relacionada con un contexto de protocolo específico. iv) *Firmas de contexto de vulnerabilidades y ataques.* Estas firmas se basan en observación de seguridad en tiempo real. La funcionalidad IPS se ha constatado que protege eficazmente contra ataques como: robos de sesión, DoS/DDoS (con gestión de conexiones, limpieza de sesiones configurable que se adapta automáticamente a la carga de tráfico), ataques *rose* de reensamblado de segmentos, inundación ICMP/UDP/TCP SYN, ataques utilizando fragmentos IP enanos, ataques utilizando MTU, al tiempo que detecta y bloquea canales encubiertos ICMP y tráfico multimedia, previene inyección SQL y XSS (*Cross Site Scripting*), protege VoIP, detecta caballos de Troya, y análisis de aplicaciones dedicadas: H323, IMAP4, NNTP, Edonkey, MGCP, SIP, RTP/RTCP, FTP, DNS, etc. El motor IPS proporciona protección

de nivel 7 dentro del sistema operativo; esto ahorra recursos como no contexto de conmutación sistema operativo-sistema, no duplica datos ya que la memoria del sistema operativo es la memoria del sistema, analiza el flujo y no se requiere ningún *proxy*, lo que ahorra recursos.

(5) **Seguridad en el nivel de correo electrónico.** Opera con protocolos como SMTP, POP3, IMAP4, y actúa sobre el *spam*, *phishing*, *spyware* y *malware*.

(6) **Administración centralizada.** Permite configurar, desplegar y monitorizar la política desplegada. Combina vistas topológicas

UTM U450 de Netasq es una herramienta hardware-software multifuncional de seguridad de red de elevado rendimiento e instalación y configuración rápida y sencilla, basada en el despliegue de uno o varios *apliances* UTM. Permite una protección proactiva escalable, integrando bajo una gestión centralizada un extenso y rico conjunto de funcionalidades -VPN (SSL y basada en IPSec), IPS/IDS- cortafuegos, antivirus, anti-spam, filtrado URL, funciones de encaminamiento, red y QoS. Al tiempo, combina con gran sinergia la prevención de intrusiones-*firewall* con el análisis en tiempo real de la red y la gestión de sus vulnerabilidades, y presenta una excelente adaptación entre las arquitecturas hardware y software, operando a nivel de kernel de sistema operativo.

PPP, PPOE a un proveedor de acceso o para acceder a túneles L2TP.

Cabe recordar que una VPN permite la transmisión segura de datos sensibles a través de un medio inseguro (por ejemplo Internet). Los mecanismos de cifrado y autenticación posibilitan esta transmisión segura a través de la red entre las entidades correspondientes que se comunican. Se ha constatado que la presente herramienta evaluada utiliza tres tecnologías para proporcionar sus capacidades VPN:

(1) **Túneles IPSec.** IPSec (protocolo estándar L3 del IETF) permite la creación de túneles VPN entre dos *firewall* o entre un *firewall* y estaciones móviles en las que deben instalarse *clientes VPN*.

(2) **PPTP** (protocolo propietario de Microsoft). Permite la creación de túneles VPN entre el cortafuegos y estaciones móviles en las que existe un *cliente PPTP integrado*.

(3) **VPN-SSL.** Permite crear túneles VPN entre el *firewall* y estaciones internas (por ejemplo servidores web seguros o comunicaciones de correo-e Webmail). A diferencia de las dos tecnologías anteriores, VPN-SSL permite crear túneles VPN sin necesidad de instalar cliente VPN alguno en las estaciones móviles; tan sólo se precisa de un *navegador Web*.

Las *políticas de túneles VPN* se soportan en arquitecturas *hub&spoke*. Una arquitectura de este tipo utiliza un sitio central con dos enlaces a sitios satélites, el sitio central representa el *hub* y los sitios satélites permiten acceder a redes remotas. Los sitios satélites no se dan cuenta de que participan en una política VPN *hub&spoke*, desde su punto de vista acceden a un sitio remoto, identificado o no, sin conocimiento de la arquitectura general de red ni de su paso a través del sitio central. De forma similar, con los túneles VPN clásicos existen dos modos de utilizar una arquitectura *hub&spoke*: 1) **Modo pasarela a pasarela**, donde se conocen las direcciones IP de los puntos finales del túnel. 2) **Modo anónimo**, donde no se conoce la dirección IP de uno de los extremos VPN. En cada caso, las posibles comunicaciones son:

- Comunicación entre dos satélites usando un sitio central.
- Comunicación entre un satélite y cualquier sitio remoto (Internet, otro satélite, el sitio central, etc.).

Una característica de esta arquitectura es considerar el correspondiente IPSec como interno.

SEISMO: GESTIÓN DE VULNERABILIDADES Y ANÁLISIS DE RIESGOS.

La funcionalidad SEISMO de gestión de vulnerabilidades estática permite generar en tiempo real un inventario de equipos con sus sistemas operativos, servicios y vulnerabilidades sin necesidad de ningún hardware

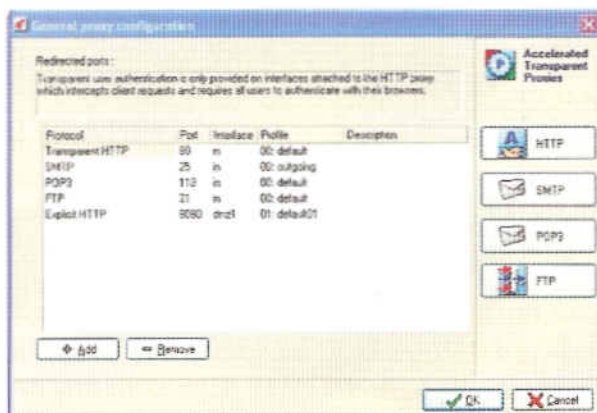


Fig. 3.- Pantalla para configuración proxy general con el *appliance* UTM U450 de Netasq.

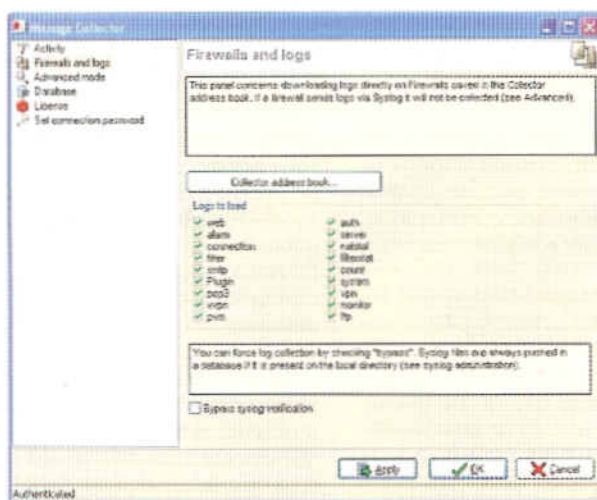


Fig. 4.- Detalle pantalla *logs* del cortafuegos.

amenazas descubiertas o informadas. Los dos tipos de información amenazas y vulnerabilidades se correlacionan para calcular el riesgo, y el resultado es la generación de informes de riesgo sobre el inventario de equipos y sistemas de la red. La información de riesgo se actualiza en tiempo real a medida que se van detectando nuevas aplicaciones y servicios vulnerables, en base al tráfico generado en la red, asimismo se actualiza cuando se publican nuevas alertas y amenazas que afectan a dichos equipos. El administrador de seguridad puede determinar el impacto real de las nuevas amenazas sobre su inventario de activos conociendo cuáles son vulnerables, lo que permite generar en tiempo real alertas de variación del riesgo, con independencia de que se esté produciendo el ataque o del tráfico que en ese momento circule por la red.

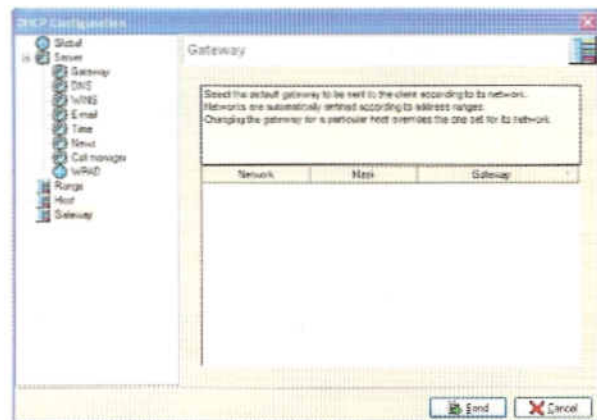


Fig. 5.- Interfaz para configurar DHCP con el *appliance* UTM U450 de Netasq.

adicional; también permite crear informes relativos a la evolución del nivel de riesgo y a las acciones necesarias para reducirlo. Podría permitir la asignación de permisos de acceso a los usuarios en función del nivel de riesgo *on-line* de los equipos desde los que se accede. La gestión de vulnerabilidades tradicional o activa se basa en lanzar una batería de tests contra los equipos de la red para obtener un informe de los sistemas operativos, servicios, aplicaciones y vulnerabilidades detectadas. A diferencia de la gestión de vulnerabilidades tradicional, SEISMO (que se encuentra embebido en el sistema operativo del *appliance*) permite obtener los mismos resultados pero con información actualizada en tiempo real y sin generar tráfico adicional por la red. La información obtenida proviene de dos focos:

- Se obtiene un inventario de equipos con información sobre el sistema operativo, los servicios y las aplicaciones detectadas en la red. Esta información se actualiza en tiempo real a medida que los equipos de la red generan tráfico que atraviesa el *appliance*.

- Se obtiene información sobre *exploits* y vulnerabilidades que afectan a los distintos sistemas, aplicaciones y servicios detectados en la red. Esta información se obtiene de forma automática a medida que se hacen públicos los informes de nuevas alertas y amenazas descubiertas o informadas. Los dos tipos de información amenazas y vulnerabilidades se correlacionan para calcular el riesgo, y el resultado es la generación de informes de riesgo sobre el inventario de equipos y sistemas de la red. La información de riesgo se actualiza en tiempo real a medida que se van detectando nuevas aplicaciones y servicios vulnerables, en base al tráfico generado en la red, asimismo se actualiza cuando se publican nuevas alertas y amenazas que afectan a dichos equipos. El administrador de seguridad puede determinar el impacto real de las nuevas amenazas sobre su inventario de activos conociendo cuáles son vulnerables, lo que permite generar en tiempo real alertas de variación del riesgo, con independencia de que se esté produciendo el ataque o del tráfico que en ese momento circule por la red.

Se ha podido constatar que la tecnología SEISMO permite hacer un seguimiento y monitorización de la variación del riesgo de la organización a lo largo del tiempo de forma muy eficaz sin impactar en el tráfico de red. SEISMO gestiona riesgos en base al análisis estático en tiempo real, se encuentra embebido en el motor ASQ en el sistema operativo, y proporciona al administrador información relevante acerca del nivel de riesgo de toda la infraestructura. Se basa en el análisis de los protocolos del motor de prevención de

intrusiones, por tanto recoge sólo la información relevante de modo que el rendimiento es muy satisfactorio. Descarga de forma automática las actualizaciones de las bases de datos de vulnerabilidades y avisa al administrador sobre dónde encontrar los parches a posibles *bugs*-vulnerabilidades encontradas.

Es de destacar que SEISMO permite detectar aplicaciones desplegadas a lo largo de la organización. Existen dos tipos de aplicaciones: i) **Productos**. Aplicaciones cliente instaladas en estaciones de trabajo, como *FireFox 1.5*. ii) **Servicios**. Son aplicaciones servidor asociadas a un puerto, por ejemplo *OpenSSH 3.5*. Utilizando los datos detectados por el motor ASQ, SEISMO genera información referente a las aplicaciones detectadas. La adición de esta característica hace posible agrupar las aplicaciones por familias.

SUITE DE ADMINISTRACIÓN CENTRALIZADA

El software de la *Suite de Administración* Netasq puede utilizarse para facilitar la supervisión y monitorización de todo el conjunto de *appliances* desplegado. Las principales funcionalidades constatadas en la *Suite de Administración* son:

Gestor unificado

Permite la administración y definición de políticas de seguridad de forma segura, tanto de forma local como remota. En el contexto del correo electrónico permite gestionar de forma centralizada diferentes aplicaciones de correo. Desde su ventana se puede: (i) Configurar acceso al servidor de correo electrónico. (ii) Definir grupos de receptores (se pueden crear hasta cincuenta). (iii) Definir el grupo de receptores para alarmas ASQ de prevención de intrusiones y para eventos del sistema. (iv) Modificar modelos de correo pre-configurados.

El gestor unificado puede operar en dos modos diferentes: a) *Modo administración global*. Es la solución software para gestionar ciertas acciones de administración sobre todo el conjunto y desde una localización central. b) *Modo gestor de cortafuegos*. Permite configurar la unidad. La *base de datos de objetos* se utiliza en la mayor parte de los módulos de configuración del gestor unificado. Los *objetos* pueden ser: i) Usuarios (con *logins* y contraseñas para autenticación). ii) Computadores (existiendo una relación entre objeto y una dirección IP). iii) Intervalos de direcciones. iv) Redes (direcciones de red y máscaras de subred). v) Protocolos (existiendo una relación entre nombre de protocolo y su número). vi) Servicios (nombre del servicio, puerto y protocolo). vii) Grupos (computadores y/o redes, intervalos de dirección, grupos de usuarios, grupos de servicios).

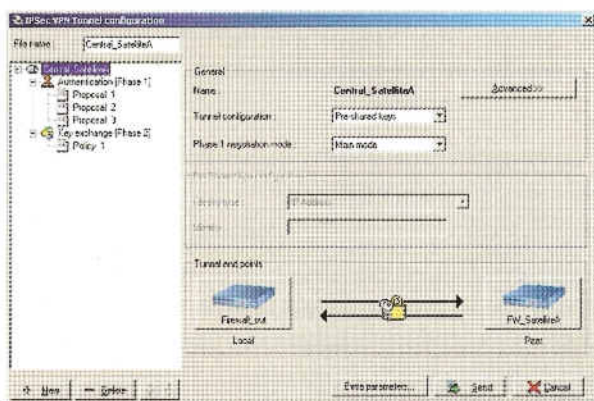


Fig. 6.- Configuración de túneles VPN IPsec con el *appliance* de Netasq.

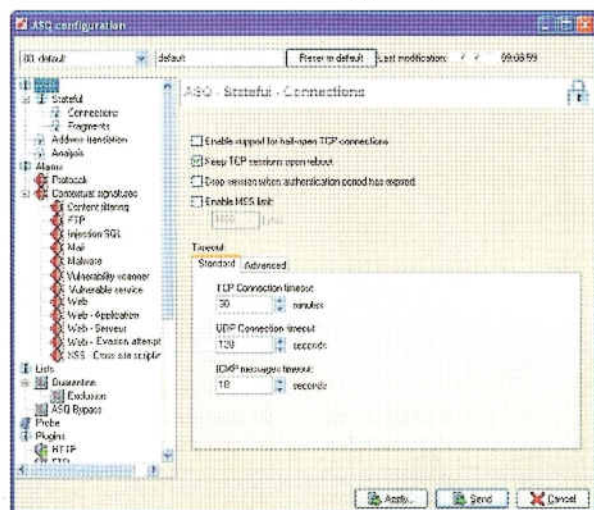


Fig. 7.- Configuración del ASQ-IPS del *appliance* UTM U450 de Netasq.

principales para caudal entrante, xv) Los cinco interfaces principales para caudal saliente, xvi) Los cinco computadores principales para el caudal entrante, xvii) Los cinco computadores principales para el caudal saliente.

Reportador de eventos

Permite crear informes y registrar los *logs* obtenidos de los *appliances* desplegados; asimismo, con su GUI permite entender los eventos registrados y tomar las acciones adecuadas. Posibilita ver los *logs* generados por los *appliances* y realizar el análisis sobre dichos registros (análisis gráfico, edición de filtros, agrupaciones jerárquicas, etc.).

Proporciona funcionalidades de monitorización y supervisión para los *appliances* desplegados, permitiendo una visión global del estado de todo el equipamiento instalado. Para monitorizar y supervisar se utiliza la visión topológica (permite comprobar el estado operativo de todos los equipos de la zona de visión) y su zona de visualización de topología. El monitor en tiempo real y el reportador de eventos son indispensables para la supervisión y monitorización del conjunto de *appliances* desplegado.

CONSIDERACIONES FINALES

El *appliance* UTM U450 de Netasq fue sometido durante veinte días a

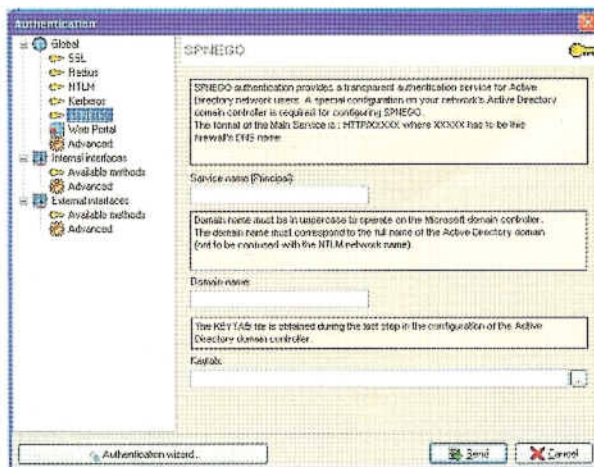


Fig. 8.- Interfaz para autenticación con el *appliance* de Netasq.

un continuado y exhaustivo conjunto de baterías de test y pruebas de carga, realizándose igualmente ataques al hardware y al software con resultados globales de protección en el peor de los casos superiores al 92,8%.

La valoración de los mecanismos de alta disponibilidad fue del 94,3%, y los resultados de las medidas relativas al caudal de las funcionalidades cortafuegos e IPS fueron de 1.000 Mbps. Se pudo constatar latencia del IPS menor de treinta microsegundos, con tramas Ethernet completas. La valoración relacionada con el número de conexiones concurrentes fue de 600.000. Los resultados de la valoración del sistema de gestión centralizada alcanzaron el 96,8%, las medidas de valoración de la funcionalidad VPN con IPSec, el 97,2% y las relativas a VPN con SSL, el 96,8%.

Las pruebas de saturación identificaron como número de nuevas sesiones por segundo 10.500. La efectividad VPN AES medida fue de 225 Mbps. Los test cuantitativos referentes a túneles VPN han conducido a medir como número de túneles VPN máximo 1.000. En cuanto al número de clientes VPN SSL simultáneos fue de 512.

La valoración de los mecanismos de anti-spam condujeron a una tasa de detección de spam del 98% bajo nivel de tráfico superior al 89%. La valoración cuantitativa de límites identificado como número máximo de reglas de filtrado 8.000. Por su parte, las pruebas sobre monitorización e informes destacan el logging a servidores Syslog con un máximo de tres, las alertas de correo electrónico sin

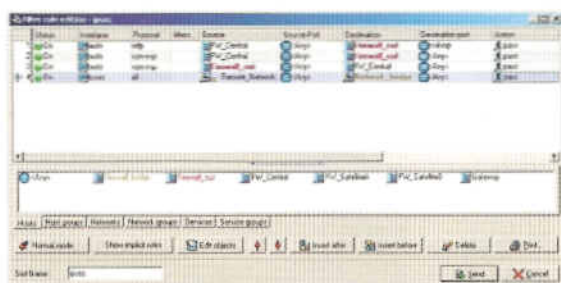


Fig. 9.- Pantalla de edición de reglas de filtrado con UTM U450.

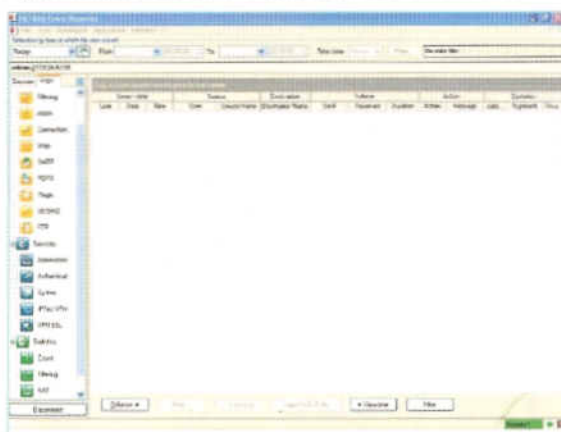


Fig. 10.- Interfaz del reportador de eventos de la herramienta.

limitación, la generación automática de informes muy bien dimensionada, soporta agentes SNMP v1/v2/v3 (con DES/AES).

El comportamiento de la herramienta ante cortes de fluido eléctrico y re-arranques fue satisfactorio. Los resultados obtenidos a las pruebas de ataques *side channels* efectuadas también fueron satisfactorios; así, para análisis de *timing*, del 92,1%; para análisis de potencia y DPA (*Differential Power Analysis*), del 93%; para análisis de fallos, del 93,5%, y para los basados en radiación EM, del 89%. Cabe reseñar que no observaron inestabilidades significativas ante pruebas de estrés y fatiga prolongada. Las pruebas de eficiencia relacionadas con *malware* fueron del 96,3%.

Los resultados cuantitativos relacionados con el número de VLANs con IEEE.1Q fueron de 128. La valoración IPS/IDS se calificó como notable, destacando una tasa de falsos positivos en IPS en el peor de los casos menor del 0,00001. Los test de las pruebas de *routing* y QoS fueron muy satisfactorios. Respecto al encaminamiento basado en política y el *routing* dinámico se constó que flexibilizan en gran medida los despliegues. Es de destacar la operatividad en modo puente L2 y *router* L3 hasta la capa de aplicación.

Finalmente, los resultados en cuanto a límites identificaron como número de clientes PPTP simultáneos 96, la redundancia de enlace WAN fue de 8 y se observó sin degradación, un soporte de hasta 8 conmutaciones PPPoE, PPTP, L2TP, PPP. ■

CONCLUSIONES

- ▶ **OBJETIVO:** herramienta de seguridad de red de naturaleza hardware-software catalogada como sistema multi-funcional UTM basado en *appliance* con un amplio abanico de funcionalidades de detección, prevención y reacción como IPS/IDS, *firewall-proxy*, filtrado URL, antivirus-anti-*spyware*, anti-*spam*, anti-*phishing*, VPN-IPSec-SSL, etc. Se gestiona de forma centralizada sobre un GUI intuitivo, soporta cuadro de mando. Opera sobre redes TCP/IP con interfaz LAN Ethernet 10/100/1000 Mbps en modo puente L2 y *router* L3. Incluye un sistema de generación de informes bien dimensionado y funciones de gestión de riesgos muy útiles.
- ▶ **PUNTAJIZACIONES / LIMITACIONES:** si no se ha alcanzado el número máximo de interfaces configurados, el administrador puede crear tantas VLANs como desee sin tener que re-arrancar el *appliance*. Syslog y el reportador de eventos deben instalarse en la misma estación de trabajo. Durante las tareas administrativas, se debe desactivar la monitorización en el modo de administración global. Para poder utilizar el modo de administración global, hay que asegurarse de que ningún equipo filtre peticiones ICMP que procedan de la estación de trabajo de administración y que los equipos respondan a peticiones ICMP. Si el camino al reportador de eventos no se ha definido para la versión del software del *appliance* o si la versión del software no se reconoce, un asistente ayuda a elegir el reportador adecuado. Las alertas de correo-e que se envían para cada alarma pueden configurarse alarma por alarma.
- ▶ **IMPACTO DE SU UTILIZACIÓN:** fácil despliegue, no se requieren equipos adicionales. Enfoque modular y escalable. Instalación y configuración rápida y sencilla. Elevado rendimiento. Soporta diversos mecanismos de autenticación (Radius, Windows, LDAP, soporta SSO, integra PKI con Autoridad de Certificación y Lista de Revocación de Certificados, compatibilidad con PKI externas, etc.).
- ▶ **PRESTACIONES / VENTAJAS ESPECÍFICAS:** utiliza ASIC-VPN. Puede operar en nivel L2 (*bridge*). El motor IDS/IPS se encuentra embebido en el núcleo del sistema operativo, lo cual permite un rendimiento muy satisfactorio. El sistema operativo se encuentra extra-recortado sólo con los servicios estrictamente necesarios para minimizar vulnerabilidades. Proporciona una protección unificada que facilita la gestión y la administración. El costo de administración se minimiza. Gestión centralizada, de granularidad muy fina y de gran eficiencia. Los mecanismos de actualización son automáticos y de eficiencia satisfactoria. Permite aislar servidores sensibles en una DMZ dedicada, sin necesidad de cargar la infraestructura gracias a la característica de puente transparente. Incluye PKI, VPN-IPSec y SSL-VPN. Las funcionalidades de cortafuegos-IPS-VPN y protocolo de administración han obtenido la certificación Common Criteria EAL2+ del ISO15408/18045.
- ▶ **DOCUMENTACIÓN:** correcta. Utiliza ficheros .pdf.
- ▶ **ESTRUCTURACIÓN DE COMPONENTES:** 1) Hardware. Conjunto de *Appliances* UTM U450 basados en procesador ASIC (en la presente evaluación sólo se ha utilizado una unidad hardware U450). 2) Sistema de gestión de todas las unidades hardware desplegadas. Incluye el gestor unificado, el monitor en tiempo real y el reportador de eventos. Trabaja con SSH v2.
- ▶ **CALIFICACIÓN FINAL:** herramienta de seguridad de red del tipo sistema multi-funcional de protección basado en el despliegue de uno o varios *appliances* UTM. Permite una protección proactiva escalable integrando bajo una gestión centralizada un extenso y rico conjunto de funcionalidades como VPN (SSL y basada en IPSec), IPS/IDS-*firewall*, antivirus, anti-*spam*, filtrado URL, funciones de encaminamiento, red y QoS; permite VLANs y modo transparente L2. Combina con gran sinergia la prevención de intrusiones-*firewall* con el análisis en tiempo real de la red y la gestión de sus vulnerabilidades. Presenta una excelente adaptación entre las arquitecturas hardware y software, operando a nivel de kernel de sistema operativo. Permite un cuidado sistema de generación de informes personalizados a medida. Incorpora tecnologías propietarias muy relevantes como ASQ y SEISMO y establece una excelente simbiosis con otras tecnologías como Kaspersky y Optenet. Incluye una gestión cuidada de vulnerabilidades y análisis de riesgos utilizando la tecnología SEISMO. Posibilita realizar tareas de cumplimiento.

EQUIPO DE EVALUACIÓN

DIRECTOR:
Prof. Dr. Javier Areitio Bertolin
 Catedrático de la Facultad de Ingeniería. ESIDE.
 Director del Grupo de Investigación Redes y Sistemas.
 UNIVERSIDAD DE DEUSTO

