UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Estudio de soluciones Unified Threat Management (UTM) de libre acceso

Trabajo Fin de Máster

Presentado por: León Casas, Diego

Director/a: Sánchez Rubio, Manuel

Ciudad: Villaviciosa de Odón (Madrid)
Fecha: 29/01/2016

Resumen

En este estudio se analizan las capacidades de protección de las soluciones UTM de libre acceso Endian Firewall Community, Sophos UTM Home Edition, y Untangle NG Firewall. Para ello se han creado diferentes escenarios simulando las amenazas básicas y avanzadas que un usuario doméstico o una pequeña empresa podrían encontrar para comprobar la eficacia de cada solución a la hora de detectar y bloquear los distintos ataques.

Las pruebas revelan que Sophos es la que mejor resultados ha obtenido de las tres soluciones analizadas.

Palabras Clave: Utm, firewall, filtro de contenidos, proxy, antivirus.

Abstract

In this study the protection capabilities of the free UTM solutions Endian Firewall Community, Sophos UTM Home Edition and Untangle NG Firewall are analyzed. To this end, different scenarios have been created simulating basic and advanced threats that a home user or small business could find to check the effectiveness of each solution detecting and blocking the different attacks.

Tests reveal that Sophos has achieved the best results of the three solutions discussed.

Keywords: Utm, firewall, web filter, proxy, antivirus.

Agradecimientos

No me gustaría acabar este trabajo sin agradecer a mi familia y a mi novia el apoyo incondicional que me han ofrecido durante toda mi etapa de estudios de máster.

Contenido

Tabla de Figuras

1. Introducción

1.1 Presentación

Desde 2014 los UTM son una de las primeras soluciones de seguridad en red de las organizaciones [1].

El término Gestión Unificada de Amenazas, del inglés Unified Threat Management (UTM), también conocido como Gestión Unificada de Seguridad o Unified Security Management, fue originalmente acuñado por la firma de investigación de mercado International Data Corporation (IDC). Con él se hace referencia a una solución considerada como la evolución del firewall tradicional en una solución integral de seguridad: un sistema único capaz de realizar distintas funciones tradicionalmente existentes en diferentes dispositivos, como firewall de red, prevención de intrusos, antivirus, antispam, VPN, filtro de contenidos, balanceo de carga, prevención de fuga de datos, panel de informes de seguridad, etc.

La principal ventaja de la seguridad unificada recae en el hecho de que se sustituye la necesidad de administrar múltiples sistemas que de forma individual cubren diferentes necesidades, por la flexibilidad que ofrece implantar una única solución que cubre toda la funcionalidad, ya sea como unidad física alojada en rack o como máquina virtual.

Las soluciones UTM basadas en identidad son más completas, ya que no sólo identifican direcciones IP, puertos o protocolos de la red, sino que además ofrecen información discreta de la identidad de cada usuario para cada una de las funciones de seguridad que se ofrecen. Gracias a esto se permite la creación de políticas de red basadas en la identidad de usuarios y grupos, lo que permite a la organización detectar patrones de comportamiento que puedan evidenciar usos indebidos, intrusiones, o ataques desde el interior de la empresa. Es lo que algunos fabricantes han llamado la capa 8, o capa de usuario [3].

Precisamente las empresas están tomando conciencia de que sus sistemas son tan vulnerables a ataques desde el exterior como desde el interior de la empresa [1]. Estos riesgos internos, provocados tanto por la malicia como por la ignorancia del empleado, pueden llevar a situaciones de accesos no autorizados, a filtraciones de datos confidenciales, al abuso del ancho de banda o a otros riesgos relacionados. Por ejemplo, el phishing utiliza el email y páginas web falsas para engañar al usuario y conseguir datos personales o credenciales de acceso que abren la puerta a ataques internos. En este sentido se está produciendo un cambio desde el método de ataque indiscriminado pero poco

eficiente, hasta otros ataques más sofisticados como son los ataques dirigidos mediante Spear-Phishing. Algunos de los ataques dirigidos más famosos que se han producido, como el ataque a RSA [9], a HBGary [10], la Operación Aurora [12] contra Google, o el ataque a Sony Entertainment en 2014 [11] comenzaron con ataques de tipo Spear-Phishing. Esto se debe a que las defensas tradicionales simplemente no impiden este tipo de ataque [8]. Las políticas basadas en usuarios y grupos podrían ayudar a mitigar este tipo de ataques.

Asimismo, los UTM ofrecen tecnología capaz de manejar el entorno regulatorio que existe a lo largo del mundo. Las normativas como HIPAA, PCI-DSS, SOX, CIPA, NERC o FFIEC requieren controles de acceso y auditorías para el control de fugas de información. Ya que los UTM basados en identidad ofrecen visibilidad de la actividad a nivel de usuario y permiten crear políticas basadas en esta identidad, pueden ofrecer una gran ayuda para el cumplimiento de requisitos normativos. Una funcionalidad habitual es la de creación de informes de auditoría basados en dichas normativas, por lo que se reduce el tiempo a invertir en estas tareas, ayudando en cierta medida a alcanzar el cumplimiento buscado.

1.2 Motivación

El gobierno federal de Estados Unidos comenzó a registrar estadísticas de cibercrimen en 2005. El primer informe realizado por el Departamento de Justicia de EEUU relacionado con el cibercrimen arrojó cifras muy claras: más del 70% de las víctimas de los cibercriminales sufrieron pérdidas iguales o superiores a 10.000 dólares, mientras que estos mismos crímenes provocaron un gasto de más de 867 millones de dólares a las empresas estadounidenses [13]. Para añadir gravedad al asunto, se cree que por aquel entonces sólo se habían registrado una pequeña fracción de los incidentes que realmente se habían producido. Los delitos informáticos tienen a tener una importante cantidad de cifras negras, delitos no denunciados por culpa del desconocimiento de propia víctima, que es inconsciente de haber sido víctima de un ataque, por pérdidas que no motivan el proceso de denuncia, o por miedo a sufrir las consecuencias del impacto en la imagen corporativa.

Gracias a nuevas legislaciones, como la reciente Network and Information Security Directive [45] [46], que obliga a determinadas empresas a publicar cualquier incidente grave de seguridad a los estados, y también a motivos relacionados con la concienciación, o la búsqueda de notoriedad de algunos atacantes que publican libremente los datos robados en la red, cada vez tenemos más información de las brechas de seguridad producidas. Algunas de las más notorias de los últimos tiempos son [13] [14] [15] [16]:

- Sony Pictures Entertainment fue atacada a finales de 2014, cuando unos criminales consiguieron robar más de 100 terabytes de información y posteriormente borrar información de la compañía. Las pérdidas económicas se estiman en 100 millones de dólares.

- Heartland, un famoso procesador de pagos mediante tarjeta de EEUU, fue vulnerado en 2008 y en el incidente perdió más de 130 millones de registros relacionados con tarjetas de crédito, números de cuentas bancarias, e información personal de sus clientes. Las pérdidas económicas derivadas de las multas y sanciones se estiman en 140 millones de dólares.

- Target, un centro comercial de EEUU sufrió una brecha en 2013 y los cibercriminales consiguieron robar más de 110 millones registros de tarjetas de crédito y débito de sus clientes. El coste estimado de las perdidas supera los 162 millones de dólares.

- Epsilon, la mayor firma de marketing por email del mundo fue vulnerada mediante un ataque de Spear-Phising. Esto permitió a sus atacantes robar información de nombres y correos electrónicos de hasta 75 de sus clientes, entre los que se encuentran Best Buy, TiVo, JPMorgan Chase, Capital One, Citi y Target. Los costes estimados de esta filtración se cree que rondan los 225 millones de dólares, pero hay firmas que aseguran que los gastos podrían llegar a subir hasta los 4.000 millones de dólares.

Al margen de estas enormes filtraciones, hay que tener en cuenta que este se trata de un problema que no afecta únicamente a las grandes empresas. Según el informe del Departamento de Justicia de EEUU, durante el año 2013 se produjeron más de 600 brechas de seguridad que impactaron gravemente en la operación de negocios y en la vida cotidiana de los ciudadanos. Los gastos asociados suelen estar relacionados con la necesidad de volver a producir y almacenar la información, con la recuperación de información perdida, y con la identificación y reparación de los canales a través de los cuales se produjeron estas filtraciones.

Los productos de seguridad de red utilizados por grandes empresas tienen necesidades muy altas de escalabilidad y fiabilidad. Por este motivo las corporaciones disponen de un menor abanico de posibilidades entre los que elegir, ya que necesitan soluciones capaces de analizar potentes conexiones de red en búsqueda de ataques y malware sin que ello provoque un impacto en la latencia, algo que es difícil de conseguir [2]. Sirva como ejemplo la plataforma Network Security de McAfee [17], un Sistema de Prevención de Intrusos (IPS)

que es capaz de analizar conexiones superiores a los 40Gbit/s, un tráfico muy superior al esperado en cualquier pequeña o mediana empresa. Además, los productos de seguridad de esta categoría tienen precios muy elevados que impiden su acceso a empresas con insuficiente presupuesto, así como a entusiastas de la seguridad e investigadores independientes que quieran analizar su seguridad.

En este contexto los proveedores UTM han buscado mercado en las pequeñas y medianas empresas, ofreciendo soluciones UTM incluso para pequeñas oficinas [2]. Gracias a ello el mercado mundial de la gestión unificada de seguridad movía aproximadamente 1200 millones de dólares en 2007, con un crecimiento anual compuesto de un 35-40% hasta 2011. Según un estudio de Frost & Sullivan, el mercado de este tipo de productos creció un 20% en 2009, después de haber tenido un incremento del 32% en 2008 [18].

Entre las soluciones para pequeñas empresas existen productos como los mostrados en la siguiente tabla. Como se puede observar, todos requieren de una inversión mínima que puede llegar a superar la capacidad tanto del usuario doméstico o del investigador independiente, como el presupuesto que una nueva empresa pueda invertir en seguridad.

Dispositivo	Precio
Barracuda X100	~1200$
Cisco MX64	~650$
SonicWall NSA 250m TotalSecure	~1900$
FortiGate 60D-3G4G-VZW	~1800$
Juniper Services Gateway (SRX100H)	~500$
Sophos XG 105	~780$
Watchguard XTM 25 Firewall Appliance	~495$

Figura 1: Precios UTM de gama baja extraídos de Amazon.com

1.3 Objetivos

Teniendo en cuenta la situación anteriormente planteada, se propone analizar la seguridad que ofrecen soluciones UTM de libre acceso. Esto nos permitirá evaluar el nivel de protección y características esperables dentro de este tipo de solución de seguridad integral, sirviendo como conocimiento previo a la adquisición de soluciones de pago, y como investigación del nivel de seguridad aproximado que se puede esperar en soluciones del mercado similares.

Las soluciones que se propone analizar son:

- Endian Community Edition
- Sophos UTM Home Edition
- Untangle

La herramienta de Sophos es gratuita, aunque su licenciamiento permite únicamente un uso no comercial [19]. Untangle sí permite el uso en entornos comerciales, pero sin embargo, la versión gratuita tiene versiones limitadas de algunas de las funcionalidades incluidas. Por ejemplo, el filtro de contenidos libre es más limitado que el filtro de contenidos de pago, ya que no puede inspeccionar tráfico HTTPS y tiene una base de datos de aproximadamente un millón de entradas, frente a las más de 450 millones del filtro de contenidos completo. Con el producto de Endian sucede algo similar. Al tratarse de un software libre permite el uso sin cargos de la solución en su versión “Community”, sin más restricción que la ausencia de las versiones completas de los módulos y del soporte al usuario final.

Aunque se propone el estudio de las versiones gratuitas por su fácil acceso, y usando como premisa que es mejor usar una versión gratuita sin soporte que no tener solución de seguridad alguna, es necesario tener en cuenta una serie de recomendaciones a la hora de desplegar estos productos en un entorno de producción:

- Un primer aspecto a tener en cuenta es que las soluciones gratuitas carecen de soporte. No existe garantía de ningún tipo, ni soporte técnico, y la única información disponible es la presente en foros públicos o páginas de preguntas frecuentes. No es recomendable usar un producto de estas características en un entorno comercial de producción, ya que ante cualquier eventualidad no se dispone de una línea directa con el fabricante para la resolución rápida de problemas.
- Las licencias de pago reciben actualizaciones de seguridad de forma muy frecuente, mientras que las licencias gratuitas se actualizan con mucha menor asiduidad, principalmente con la salida de nuevas versiones mayores. Esto incrementa la ventana de tiempo en la que podemos estar expuestos a nuevas amenazas de seguridad que en las versiones comerciales ya han sido parcheadas.
- En ocasiones, las versiones gratuitas se utilizan de laboratorio de pruebas para tecnología experimental que no ha sido suficientemente analizada, antes de

desplegar la tecnología parcheada en la versión comercial. Por este motivo se pueden tener problemas de inestabilidad o fallos no documentados.

Por todo ello, es necesario entender que el uso de licencias de este tipo no está recomendado para ser mantenido en el tiempo en entornos comerciales de producción, sino que es interesante para usuarios domésticos o para acceder a la tecnología y poder probarla antes de tomar una decisión de compra final.

1.4 Organización del presente documento

El presente documento está organizado en capítulos que explican las diferentes partes del trabajo desarrollado. En el capítulo 1 se ha realizado una breve introducción al proyecto. El capítulo 2, *Estado del Arte*, se explican todos los conceptos teóricos en los que se basa el trabajo y que son necesarios para entender el resto de la documentación incluida en este documento. En el capítulo 3, *Desarrollo del Estudio*, se explica el laboratorio virtual utilizado para el análisis de las soluciones, así como la gama de ataques básicos y avanzados que se han utilizado en el trascurso del estudio. El capítulo 4, *Plan de Pruebas y Resultados,* se incluyen los planes de pruebas seguidos y los resultados obtenidos. Finalmente, en el capítulo 5 se comentan las conclusiones y posibles trabajos futuros relacionados con este proyecto. Finalmente se incluyen las referencias utilizadas en el capítulo 6, *Referencias,* y se adjuntan evidencias relevantes en forma de capturas de pantalla o información adicional en los correspondientes anexos del capítulo 7.

2. Estado del Arte

2.1 Historia, teoría y conceptos

2.1.1 Introducción

La seguridad perimetral es la arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a Internet [20]. Algunos dispositivos destinados a la seguridad perimetral son los cortafuegos, los sistemas de detección y prevención de intrusos (IDS/IPS), las pasarelas antivirus y antispam, y los honeypots o honeynets. A continuación se realiza una breve descripción de estos términos que son necesarios para entender el funcionamiento de un UTM.

- **Firewall**

  Un firewall es un elemento de red que monitoriza y controla el tráfico de red entrante y saliente en función de la política de accesos creada. Existen dos políticas, la política restrictiva o de lista blanca, donde se deniega todo el tráfico excepto el que esté aceptado de forma explícita, y la política permisiva o de lista negra, que permite todo el tráfico excepto el que ha sido denegado explícitamente. De estas dos políticas, la política restrictiva o de lista blanca es la más segura pero más tediosa de mantener.

  Los filtros de paquetes, o de capa de red, funcionan comparando el origen, destino, protocolo y número de puerto para tomar una decisión de aceptación o rechazo del paquete. Este tipo de filtrado en principio no tiene en cuenta si el paquete forma parte de una secuencia existente de tráfico (stateless). Sin embargo, existen firewalls con estado (stateful) capaces de distinguir si un paquete forma parte de una comunicación anterior y tomar decisiones teniendo en cuenta esta información.

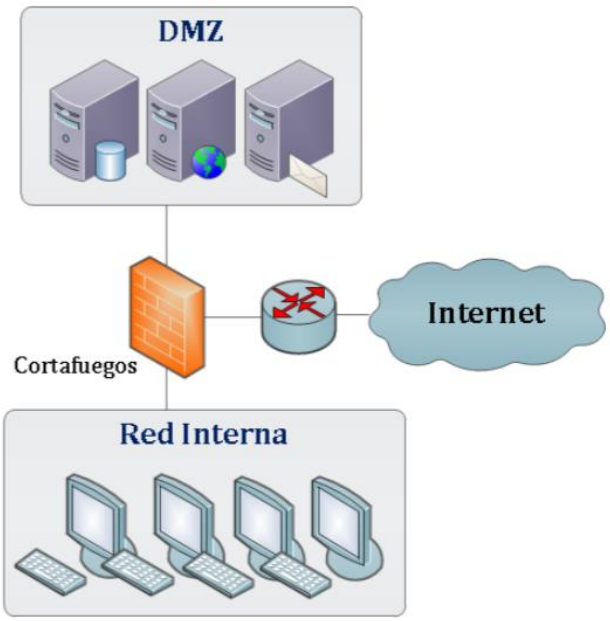


Figura 2: El firewall protege el perímetro de la red [20].

Por otro lado existen los firewalls de aplicación, que como su nombre indica trabajan en la capa de aplicación, por ejemplo, filtrando el tráfico http. Estos firewalls pueden interceptar los paquetes que viajan hacia o desde una aplicación y aplicar restricciones a nivel de proceso. Al analizar los datos a nivel de aplicación y añadir una capa de inteligencia más compleja, y dependiendo de la complejidad de las reglas aplicadas, pueden añadir una latencia mayor que el resto de firewalls mencionados

- **Sistemas de Detección de Intrusos y Prevención de Intrusiones**

Los sistemas de detección de intrusiones monitorizan la red o el sistema en búsqueda de actividades maliciosas o violaciones de políticas de seguridad, ofreciendo informes en una consola de gestión. Principalmente se dividen en dos categorías [21]:

1. Los sistemas de detección de intrusos de red (NIDS) se colocan en puntos estratégicos de la red para analizar todo el tráfico que atraviesa dicho punto y detectar posibles ataques. Una vez que un comportamiento anómalo es detectado, se registra y se informa al administrador.
2. Los sistemas de detección de intrusos de host (HIDS) se instalan en dispositivos concretos, analizando el comportamiento del sistema, y en ocasiones también los paquetes de red que entran y salen, en busca de

actividades maliciosas. También pueden tomar una captura del sistema en un estado conocido y alertar si alguna zona crítica del sistema de archivos es modificada, enviando una alerta al administrador para su posterior análisis.

La detección puede estar basada en firmas de ataques conocidos, o en la detección de anomalías estadísticas. En este último caso, se compara el comportamiento actual con el comportamiento que se considera “normal”, como es el ancho de banda transmitido un día normal, los puertos o protocolos utilizados habitualmente, o los orígenes y destinos de las comunicaciones. Siempre que se detecte un tráfico anómalo o suficientemente distinto a lo habitual, se lanza una alarma para el análisis de los administradores.

Finalmente, la diferencia entre los sistemas de detección y los sistemas de prevención radica en la capacidad de estos últimos de dar respuesta automática a los incidentes. Así, un IDS sólo es capaz de detectar, registrar y alertar al administrador, mientras que un IPS es capaz de frenar el ataque cortando la conexión o creando nuevas reglas en el firewall perimetral.

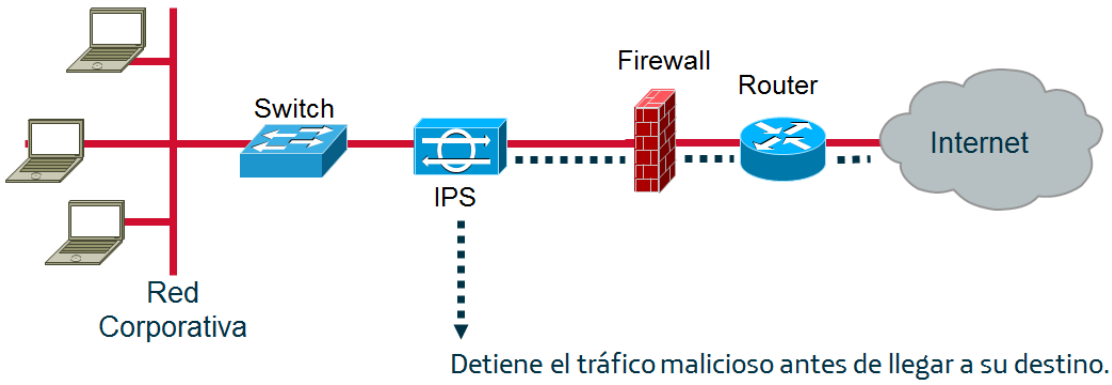


Figura 3: Un IPS tiene capacidad de detener el tráfico.

- **Pasarela Antivirus**

Estos dispositivos ofrecen la posibilidad de analizar el tráfico que entra a la red en búsqueda de malware para poder bloquearlo antes de que pueda llegar a los dispositivos y conseguir la infección. Para ello trabajan en la capa de aplicación, escaneando el tráfico que se transmite por protocolos como HTTP, HTTPS, FTP, SMTP y POP3, pudiendo incluso analizar ficheros comprimidos, con el fin de impedir las propagaciones de virus en el interior de la red corporativa.

- **Pasarela Antispam**

Las pasarelas antispam intentan bloquear la entrada y salida de correo no deseado de la red corporativa. Para proteger de la recepción de correo no deseado se utilizan todo tipo de técnicas de filtrado, desde técnicas básicas como rechazar el correo de fuentes no fiables, hasta técnicas avanzadas basadas en filtros bayesianos. Con esta tecnología los usuarios marcan los correos no deseados para que el software de filtrado aprenda y mejore su eficacia.

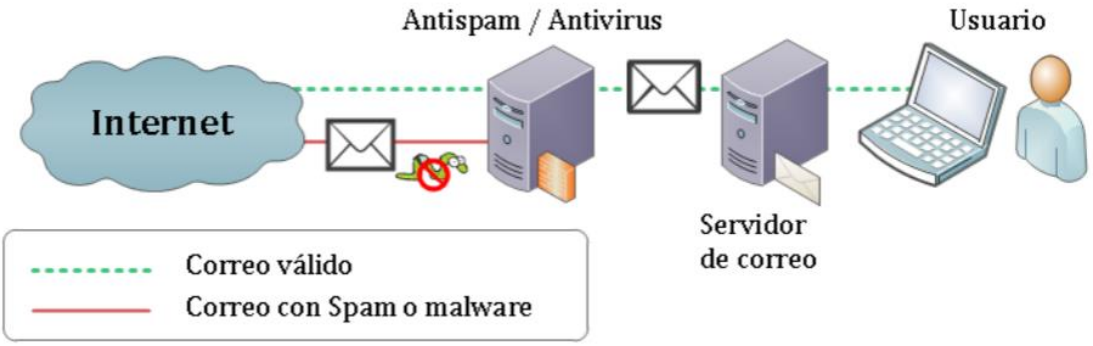


Figura 4: Pasarela de filtrado de spam y antivirus [20].

- **Honeypot y honeynet**

Un honeypot es un sistema trampa de seguridad. Su objetivo es detectar, redirigir y ayudar a reaccionar en intentos de acceso no autorizado a sistemas de información, así como en la investigación de nuevos tipos de ataques. En general se trata de un sistema que parece ser legítimo y contener información valiosa para un atacante, pero que en realidad está aislado y monitorizado para la detección de intrusiones. Por tanto, un usuario malicioso que intente conectar al honeypot y extraer información será detectado en la red y podrá ser bloqueado, permitiendo además a los administradores estudiar su comportamiento.

Dentro de los honeypot existen principalmente dos tipos de sistemas, los de baja y los de alta interacción. Cuanta más alta sea la capacidad de interacción, más servicios ofrecen a un posible atacante para que pierda su tiempo y realice acciones maliciosas sin detectar la trampa, ayudando a los administradores a investigar los métodos de actuación del atacante. Sin embargo, se convierten en sistemas más difíciles de mantener y que consumen más recursos. Por otro lado, los de baja interacción necesitan menos mantenimiento y son menos complejos, pero esto hace

que un atacante los pueda detectar más fácilmente. En cualquiera de los casos, habitualmente se hace uso de máquinas virtuales para poder restaurar al estado inicial de la máquina una vez ha sido comprometida.

Una honeynet no es más que una red en la que se utilizan dos o más honeypots con el objetivo de mejorar el realismo del escenario y tener más sondas de control para mejorar las posibilidades de detectar una intrusión.

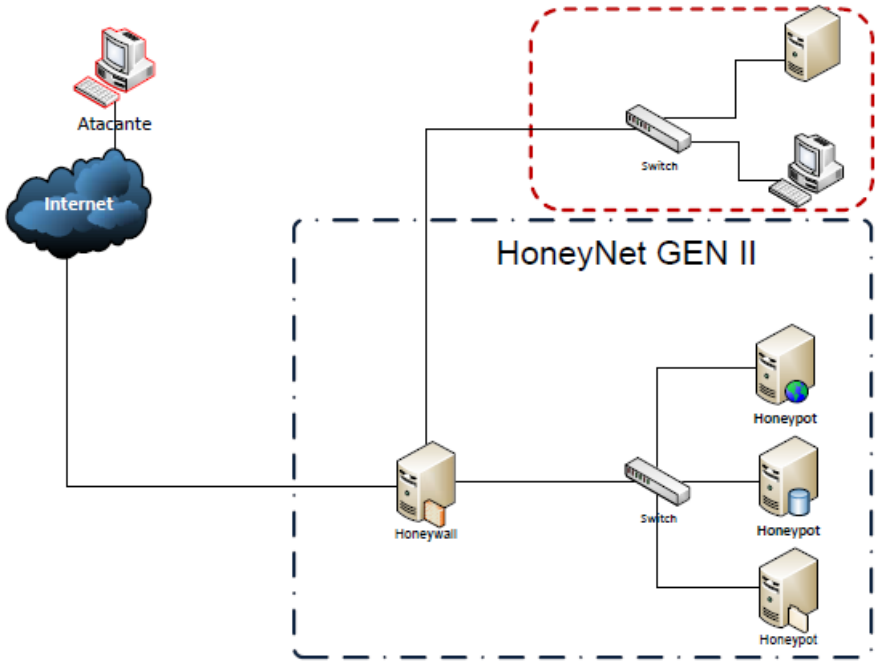


Figura 5: Arquitectura de una Honeynet [22]

- **VPN**

Una VPN, o Red Privada Virtual, es un tipo de red que utiliza una infraestructura pública (considerada no segura) para acceder a una red privada de forma confiable. Habitualmente se utiliza para conectar usuarios remotos, sucursales u oficinas con su intranet. Una VPN tiene las siguientes características:

1. Servicios de autenticación y autorización, mediante la gestión de usuarios, roles y permisos.
2. Protección de integridad, mediante el uso de funciones hash.
3. Servicio de confidencialidad, protegiendo la información mediante el cifrado de los datos en tránsito.
4. No repudio, mediante el uso de firma digital.

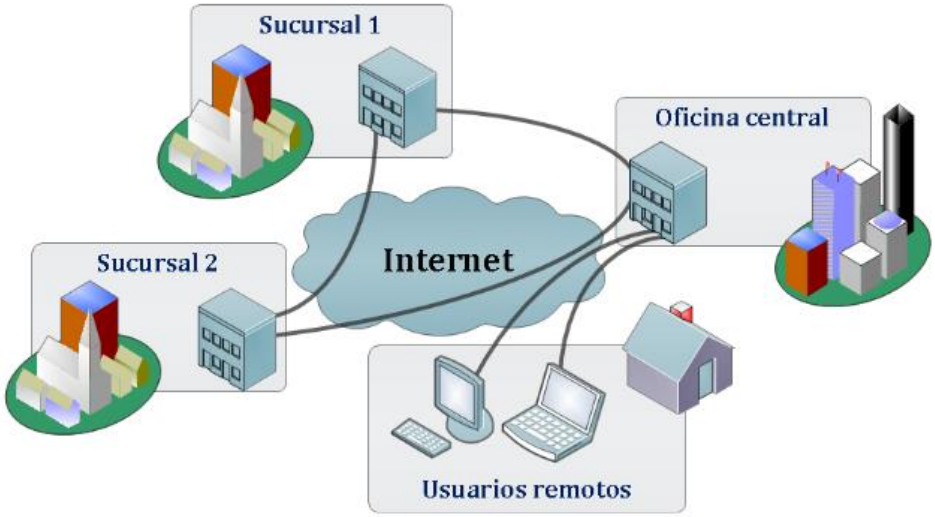


Figura 6: Las VPN permiten conectar usuarios y oficinas remotas con la intranet central [20]

2.1.2 Historia

Como se ha comprobado existen todo tipo de soluciones que ofrecen distintas características de seguridad. Sin embargo esto genera dos problemas. Primero, la dificultad de mantener una red con tantos tipos de dispositivos diferentes, cada uno de distintos fabricantes, con sus propias versiones, actualizaciones y requisitos de mantenimiento. Y segundo, la necesidad de cubrir unos gastos elevados al tener que adquirir equipamiento y licencias de soporte separadas para cada dispositivo.

En este contexto nacen los Unified Threat Management (UTM), productos con los que como ya se ha mencionado se hace referencia a soluciones integrales de seguridad con funciones como firewall de red, sistema de prevención de intrusos, antivirus, antispam, VPN, filtro de contenidos, balanceo de carga, prevención de fuga de datos, paneles de informes de seguridad, etc.

Las soluciones unificadas nacen en un contexto en el que es necesario detener un número creciente de ataques sobre los sistemas de información corporativos a través de malware y de combinaciones de amenazas externas e internas. Habitualmente los atacantes intentan atacar el eslabón más débil de la organización, el usuario, y en ocasiones las repercusiones pueden ser tan serias como la pérdida total de acceso a la información, como es el caso de los ataques por Ransomware en los que la información del dispositivo es secuestrada mediante el cifrado de los datos.

La seguridad de los datos y el acceso no autorizado de empleados se ha convertido en una de las mayores preocupaciones actuales de las empresas. Como se ha mencionado anteriormente, la filtración malintencionada y la pérdida de datos confidenciales resultante puede provocar enormes pérdidas económicas, tanto por la pérdida de propiedad intelectual, como por la responsabilidad legal resultante. En este sentido las empresas han comenzado a entender que la ignorancia del usuario puede provocar que la seguridad de las redes internas se vea comprometida [3].

En este contexto, una de las ventajas que ha promovido el auge de las soluciones UTM es la simplicidad de la solución, de la instalación y de su uso, y la capacidad de actualizar todas las características de seguridad de forma paralela. El objetivo de los UTM es proveer de múltiples características de seguridad en un único producto gestionado a través de una única consola. Estas soluciones integrales evolucionan de una forma lógica para aplacar la cantidad creciente de amenazas complejas que impactan a las organizaciones [5].

2.1.3 Transición a soluciones integradas: ventajas y desventajas.

Las soluciones tradicionales, capaces de abordar una única característica de seguridad, y que eran instaladas para resolver amenazas generales de seguridad son complejas de desplegar, administrar y actualizar, lo que incrementa la complejidad y el coste de operación [6]. Es más difícil mantener actualizadas múltiples soluciones diferenciadas de seguridad, cada una con sus propios fallos, vulnerabilidades y ciclos de parches, que una solución única integrada. Por este motivo, algunas empresas buscan actualmente una aproximación integral a la seguridad de red.

En estos escenarios existe la posibilidad de utilización de dispositivos UTM, que además facilitan el despliegue de un nivel de seguridad estándar en cualquier punto de la organización, evitando puntos débiles en lugares como oficinas remotas. Un único dispositivo simplifica la gestión de la estrategia de seguridad de la compañía, con un único aparato sustituyendo a múltiples capas de hardware y software. Además, a través de una única consola central web es posible configurar y monitorizar todas las funciones de seguridad, lo que puede mejorar la integración, productividad y facilidad de uso frente a la estrategia de múltiples dispositivos. Esto mismo también puede derivar en una mayor facilidad para entrenar al personal en el uso, ya que se trata de un único dispositivo.

Hay que tener en cuenta que al tratarse de dispositivos individuales es posible reducir la complejidad del soporte, gracias a que se simplifica la instalación y mantenimiento, con una

gestión única de actualizaciones, y con un único punto de contacto del mismo fabricante. Toda esta simplificación puede ayudar en el cumplimiento de la normativa interna de la organización.

A pesar de todas estas ventajas existen una serie de inconvenientes que deben ser tenidos en cuenta a la hora de desplegar soluciones de este tipo. Al tratarse de un único dispositivo de seguridad que analiza el tráfico de toda la red, existe un punto único de fallo que puede provocar la caída del servicio. Para evitar esta situación es necesario hacer uso de configuraciones en alta disponibilidad [7], garantizando que no haya impacto en la latencia ni el ancho de banda de la organización por falta de rendimiento o por fallo en la comunicación. Por el mismo motivo, existe un único punto de compromiso en caso de que un atacante encuentre fallos de seguridad en el dispositivo, pudiendo invalidar todas las funciones de seguridad desde un mismo punto comprometido. Esta aproximación choca con el concepto de seguridad en profundidad, en el que se introducen múltiples capas de seguridad diferentes con la esperanza de que en caso de compromiso de una de ellas el atacante se encuentre de nuevo con otras capas adicionales.

2.1.4 Capa de usuarios

Como ya adelantábamos existen soluciones UTM basadas en identidad, capaces de ofrecer protección con granularidad a nivel usuario, en lo que algunos fabricantes han llamado capa 8. Este sería el siguiente paso a la capa 7, la capa de aplicación.

Mientras que un UTM tradicional identifica únicamente direcciones IP de la red, aquellos basados en identidad ofrecen en sus registros información nominal de la identidad de cada usuario en la red. Gracias a estos datos es posible crear políticas de red basadas en usuarios y grupos, lo que ayuda a la gestión de seguridad basada en funciones y roles.

Como esta información es accesible por todas las funciones de seguridad, es posible detectar patrones de comportamiento realizados por determinados usuarios o grupos que pueda evidenciar desde simples usos indebidos, hasta intrusiones o ataques maliciosos del interior o exterior de la empresa [3]. Más aún, al no depender de direcciones IP concretas pueden ofrecer protección incluso en entornos con IP dinámica, como DHCP o WIFI, y especialmente en entornos donde múltiples usuarios comparten un mismo ordenador, siempre y cuando usen cuentas diferenciadas.

2.2 Antecedentes y estado actual

Antes de proponer las soluciones de libre acceso que serán objeto de estudio, se ha realizado un breve análisis de soluciones integrales ofrecidas por grandes empresas de seguridad. En concreto, se han analizado las funciones de seguridad ofrecidas por Bluecoat y McAfee en algunos de sus productos.

- Gestión Centralizada. Los dispositivos destinados a entornos corporativos disponen de consolas de gestión centralizada, como McAfee ePO (ePolicy Orchestrator) o Bluecoat Director, que permiten la distribución de políticas a todos los dispositivos de la red.

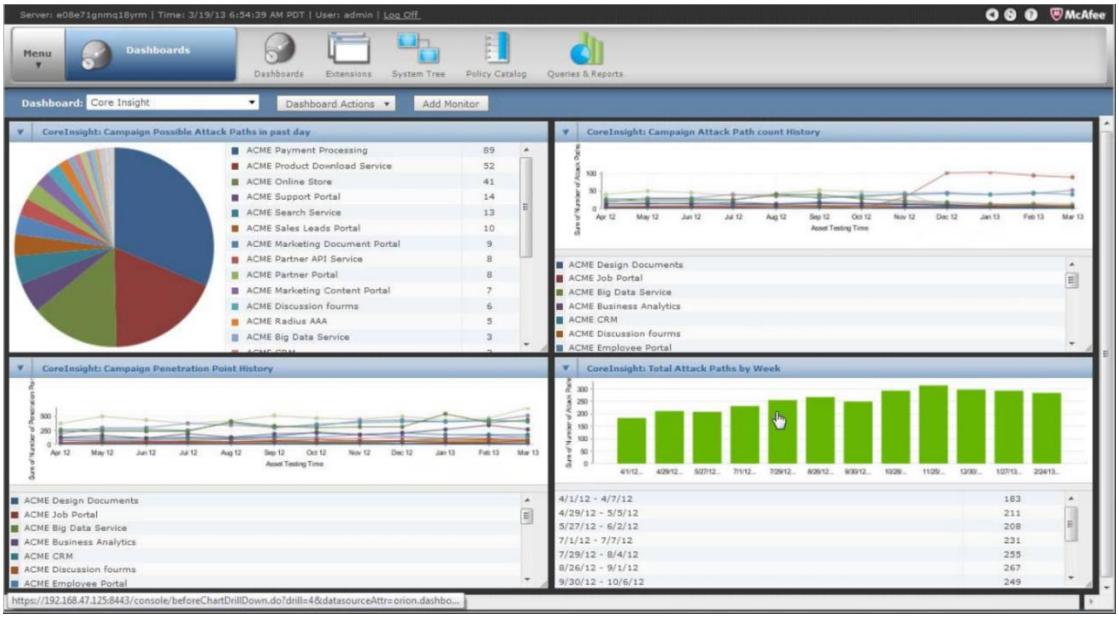


Figura 7: Consola de Gestión ePO de McAfee

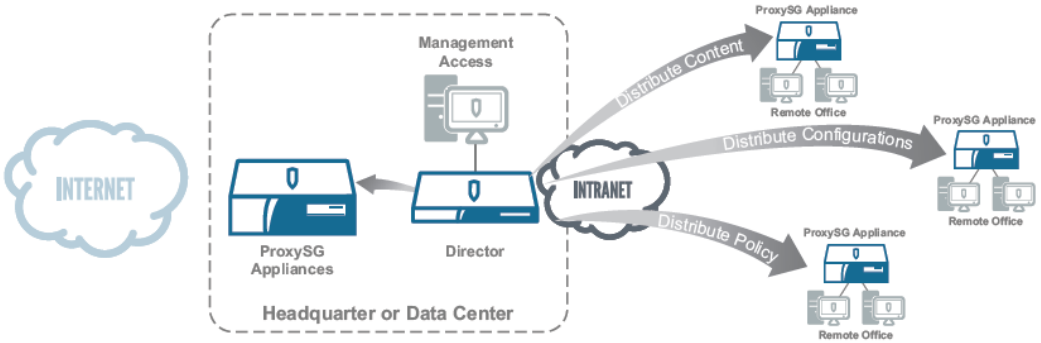


Figura 8: Gestión centralizada en dispositivos Bluecoat SG a través de la plataforma Director [32].

- Red de Inteligencia. Las grandes empresas ofrecen suscripciones a su propia red global de inteligencia relacionada con cualquier tipo de amenaza en Internet. Estas redes reciben retroalimentación de los ataques producidos, y por tanto, tras la detección e identificación de un ataque en cualquier punto de su red, todos los clientes quedan inmunizados frente a ese mismo ataque. En este sentido, cuanto mayor sea la cantidad de clientes conectados a la red de inteligencia, mayor será el número de sensores, y por tanto mayor es la efectividad real del servicio. McAfee ofrece la red GTI (Global Threat Intelligence) mientras que Bluecoat ofrece la Global Intelligence Network.

  Estas redes también permiten mejorar la capacidad de análisis de malware, al ayudar en la detección de ficheros conocidos buenos y malos, un paso previo a la necesidad de analizar ficheros mediante el envío a entornos de sandboxing.

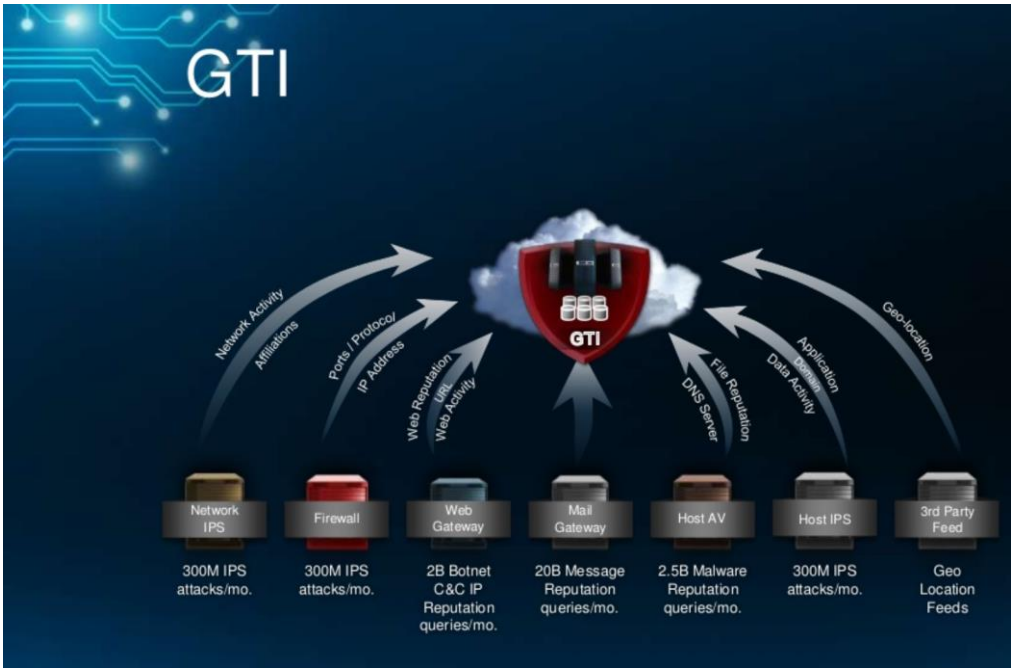


Figura 9: McAfee GTI extrae información de los sensores para conseguir Inteligencia de Amenazas [42].

- Prevención contra DDoS. Se usan técnicas como los topes de conexiones activas, o un límite al número de conexiones abiertas en determinado tiempo. También, es posible configurar reglas en las que se tiene en cuenta el origen geográfico de las conexiones, pudiendo restringir el tráfico general o a determinados países en concreto [42].

- Aislado automático de Hosts: cuando un host ha sido infectado, automáticamente es aislado de la red para evitar la propagación de malware o el desplazamiento lateral por parte de un posible atacante.

- Sandboxing y análisis avanzado de malware. Aquellos ficheros que no han sido identificados en anteriores etapas ni como legítimos ni como maliciosos pasan a ser analizados en entornos virtualizados o emulados que permiten el análisis del comportamiento del fichero sin riesgo de infección en un entorno seguro. Este estudio permite comprobar si un fichero realiza actividades sospechosas o directamente maliciosas, y por tanto, si debe ser puesto en cuarentena para su estudio o bloqueo.

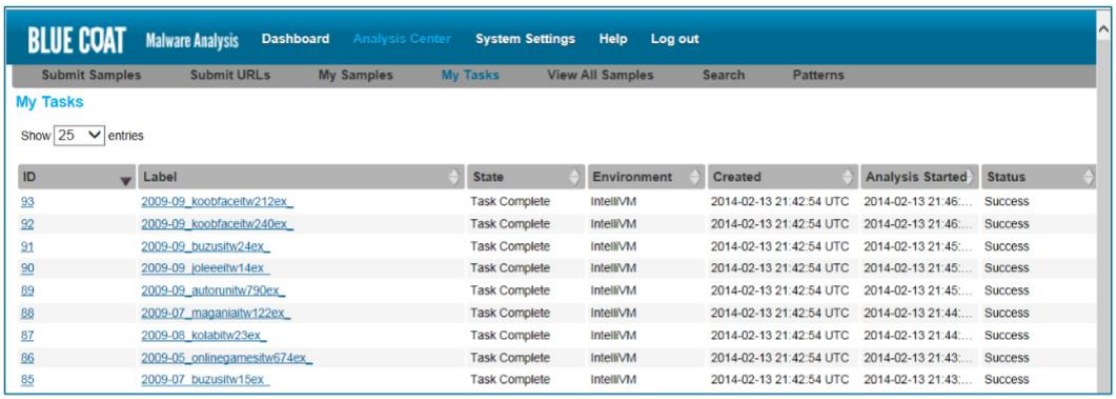


Figura 10: Bluecoat Malware Analysis Appliance, la solución de Sandboxing de Bluecoat [43].

Las muestras de malware avanzado intentan evitar este tipo soluciones con tecnologías anti-sandboxing. Algunas de las técnicas utilizadas son [23]:

- Búsqueda de parámetros conocidos relacionados con máquinas virtuales, como puedan ser claves de registro concretas, nombres y direcciones MAC de tarjetas de red, o el string del fabricante de la CPU.
- Comprobación de tamaños de disco duro poco probables en entornos de usuario, por ejemplo, menores de 50GB.
- Ejecución de la carga maliciosa sólo en días determinados del mes.
- Esperar a que el usuario realice una acción concreta, como iniciar sesión en Facebook, Gmail, o incluso mostrar un captcha por pantalla.
- Comprobar la conectividad a Internet, el historial de navegación, o la existencia de aplicaciones habituales en ejecución.
- Comprobar la existencia de hooks de nivel de kernel y usuario.

Para probar las capacidades de detección de máquinas virtuales existe una herramienta llamada Pafish (Paranoid Fish) [24] que ejecuta diversas técnicas de detección de entornos virtualizados. Esta herramienta puede ser útil para comprobar la capacidad de análisis de los entornos de sandboxing incluidos en estas soluciones.

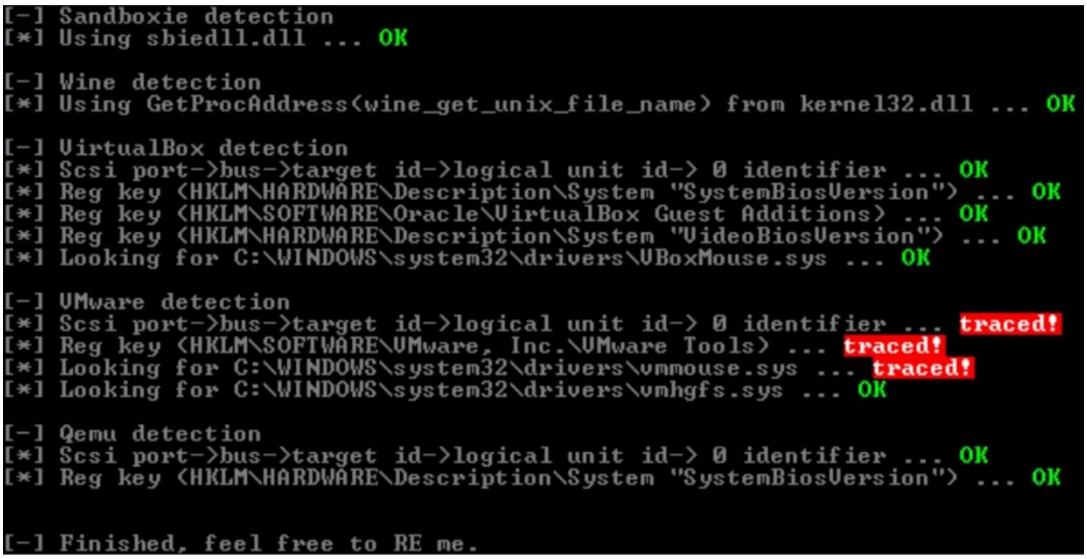


Figura 11: Pafish detectando la presencia de un entorno virtualizado VMWare [23].

2.3 Contexto del trabajo

2.3.1 Sophos UTM Home Edition

Sophos UTM Home Edition incluye todas las funciones existentes en la versión comercial [25]. Esta versión está enfocada al usuario doméstico, y por tanto sus únicas limitaciones son la prohibición de usar el software en entornos comerciales y la protección máxima de 50 direcciones IP.

La interfaz principal de Sophos ofrece un cuadro de mandos con información del producto, las actualizaciones disponibles, los recursos utilizados, y qué módulos e interfaces están activas, así como los mensajes de alerta del módulo de amenazas avanzadas, donde se notifica si algún malware ha intentado conectar con su servidor C&C.

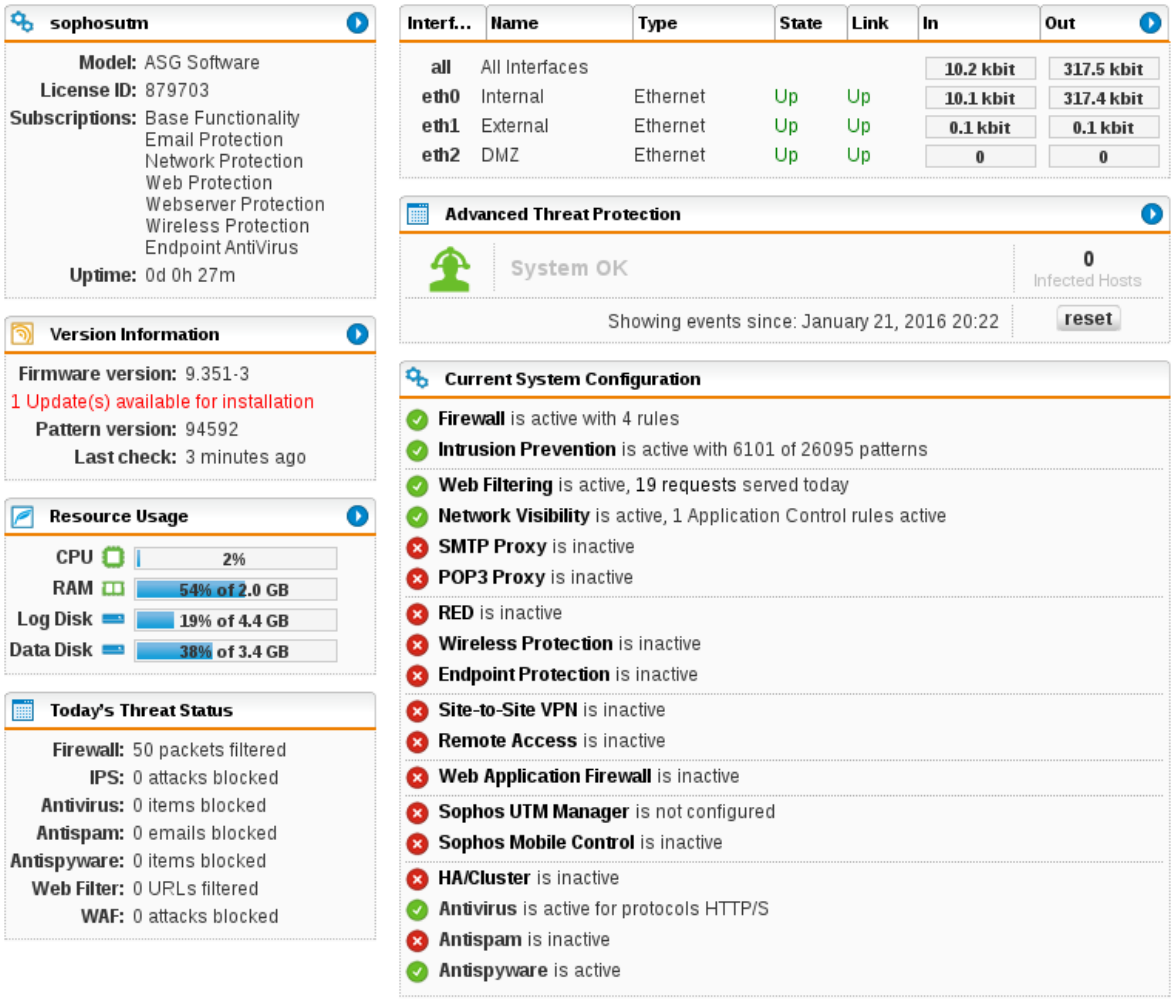


Figura 12: Cuadro de mandos principal

En la interfaz de gestión se pueden configurar los paneles de mandos, centralizar la gestión de múltiples dispositivos, comprobar licencias y actualizaciones, configurar las copias de seguridad automáticas y manuales, configurar el portal de usuarios, así como las notificaciones vía email y SNMP traps. También es posible configurar la administración basada en roles de usuario: sólo lectura, de administración y de auditoría, para garantizar la separación de funciones. Desde esta interfaz es posible activar el servicio de alta disponibilidad en modo activo-pasivo, o crear clústeres activo-activo con hasta 10 dispositivos.

Para la autenticación es posible gestionar accesos transparentes, proxy (NTLM y Kerberos) y autenticación de cliente en portal captivo, existiendo soporte para Directorio Activo (AD), eDirectory, Radius, LDAP y TACACS+. Además, existe la posibilidad de forzar políticas de contraseñas seguras.

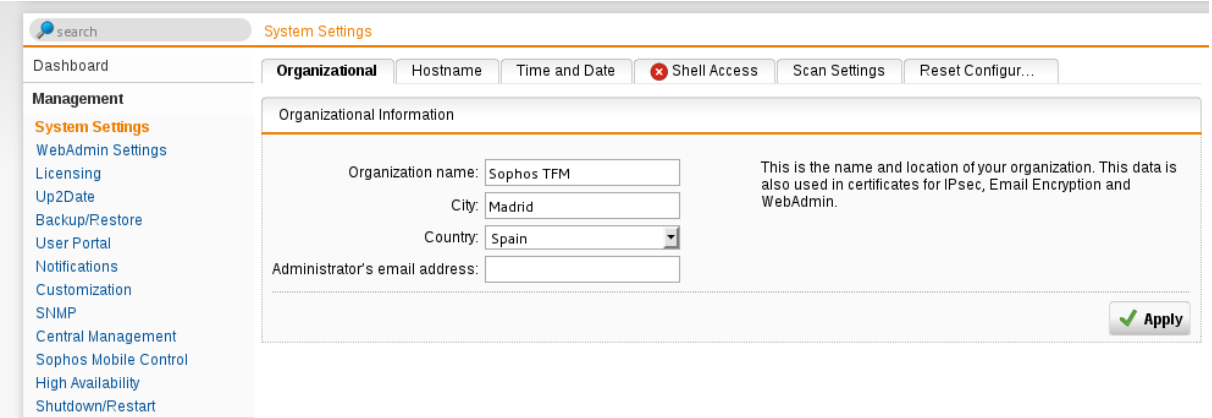


Figura 13: Gestión y configuración

Dentro de definiciones y usuarios se pueden crear objetos de red (hosts, direcciones ip, redes, etc.) y servicios como SSH, HTTPs, y otros. También es posible definir periodos de tiempo, usuarios y grupos, y configurar mecanismos de autenticación como el Single Sign On (SSO) o los One Time Passwords (OTP) para el portal de usuario, de administración, y para conexiones SSH o VPN

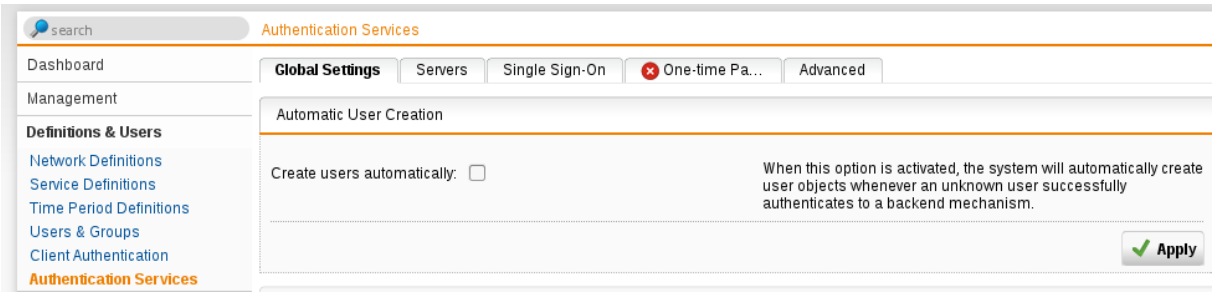


Figura 14: Definiciones, usuarios y autenticación

La configuración de interfaces y rutas ofrece soporte para enrutamiento estático, multicast (PIM-SM), y dinámico (BGB y OSPF). También permite configurar NAT estático y dinámico, calidad de servicio y el soporte para IPv6. El dispositivo permite activar agregado de enlaces con hasta 32 conexiones, failover automático, y balanceo de carga.

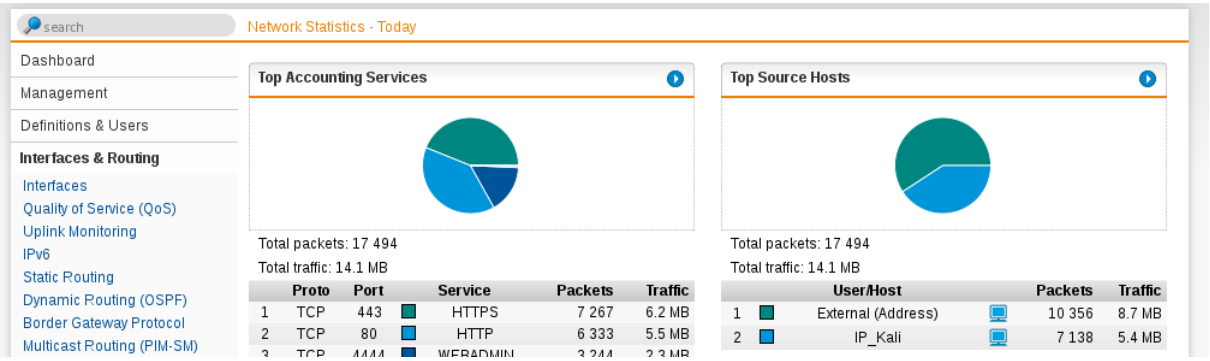


Figura 15: Interfaces y rutas

Dentro de los servicios de red se pueden configurar los servidores DNS, DHCP y NTP.

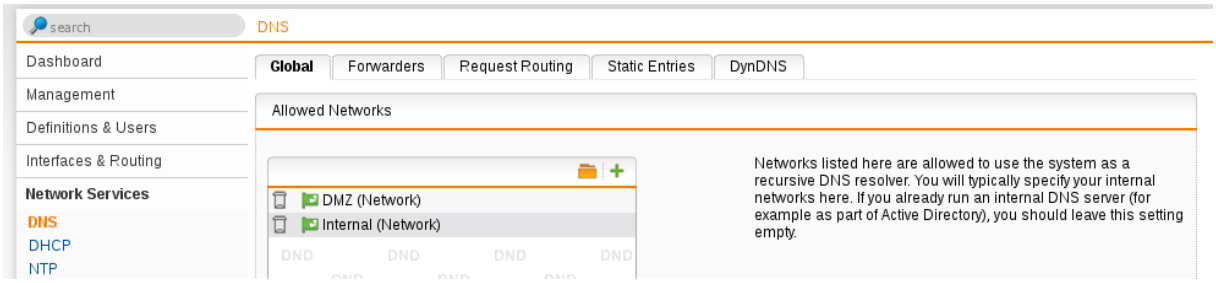


Figura 16: Servicios de red

En la capa de protección de red se pueden configurar el firewall de estado con soporte DPI (Deep Packet Inspection), el IPS, la protección contra escaneos de red, contra ataques DoS/DDoS, y los bloqueos por regiones o países individuales con reglas de entrada y salida independientemente configurables. Adicionalmente, se pueden crear reglas basadas en identidad de usuarios. La protección avanzada permite la detección y bloqueo de tráfico de contacto con servidores C&C, la identificación y aislamiento automático de hosts de la red, y dispone de una funcionalidad de sandboxing remota de muestras sospechosas en los servidores de Sophos.

Figura 17: Bloqueo de regiones y países

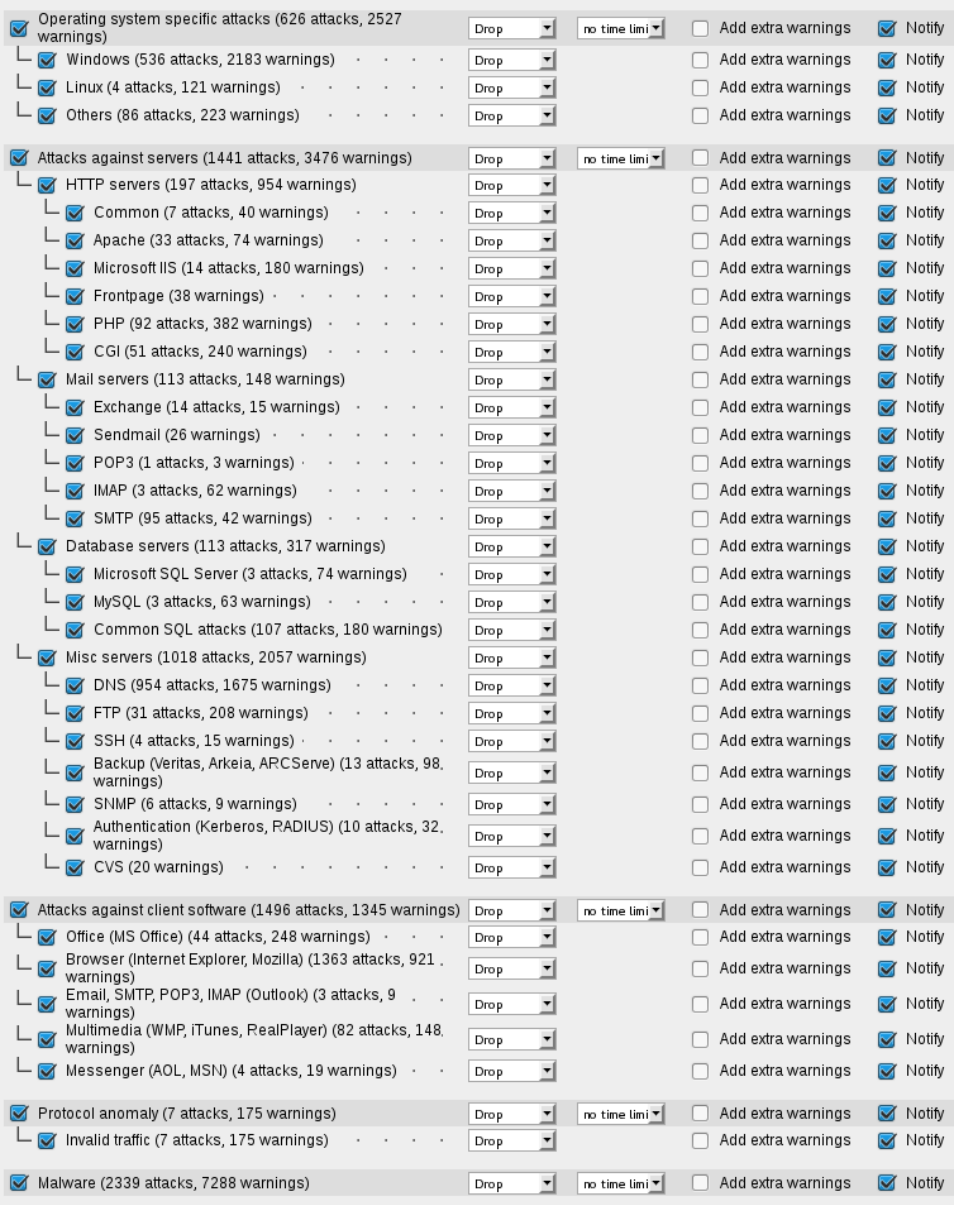


Figura 18: Reglas del IPS

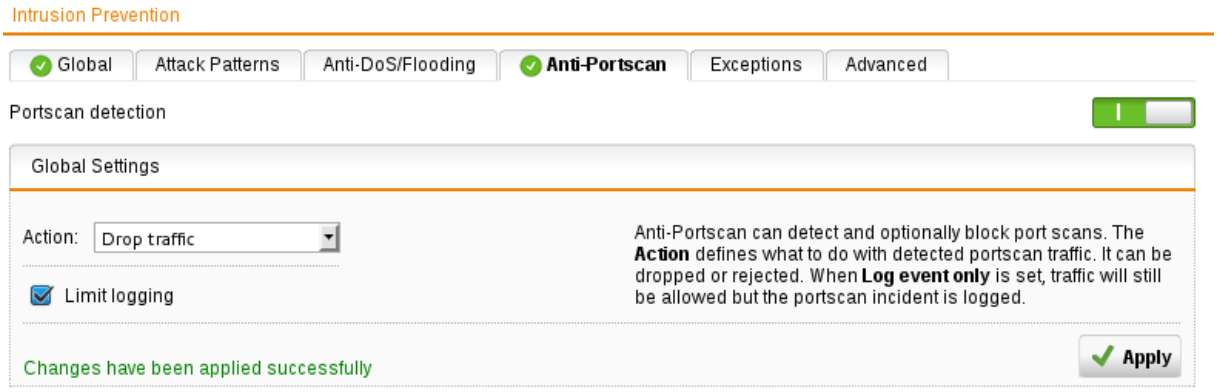


Figura 19: Protección de escaneos de puertos, DoS, excepciones, etc.

Para la protección web se pueden configurar el filtro de contenidos, con 35 millones de direcciones en 96 categorías y más de 65 idiomas, la inspección de tráfico HTTPs con posibilidad de analizar el tráfico en función de categorías, y configurar los filtros de capa 7 con firmas para miles de aplicaciones distintas. Tanto para HTTP como para HTTPs se pueden utilizar los dos motores antivirus incluidos, pudiendo usarse la red de inteligencia vía Cloud para la búsqueda de amenazas recientes.

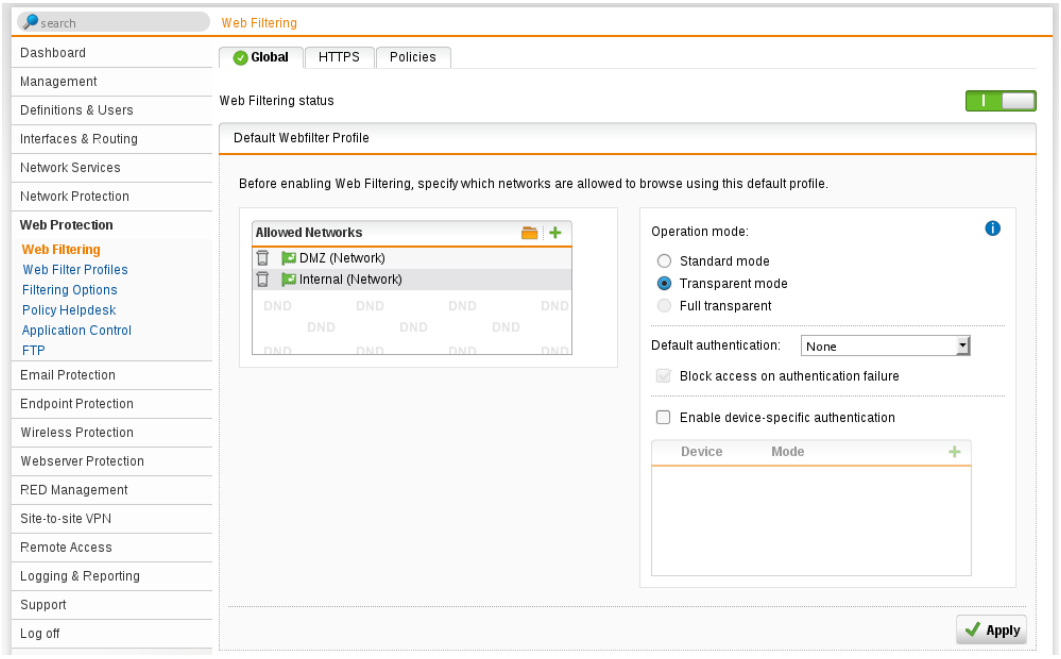


Figura 20: Filtrado web y control de capa 7.

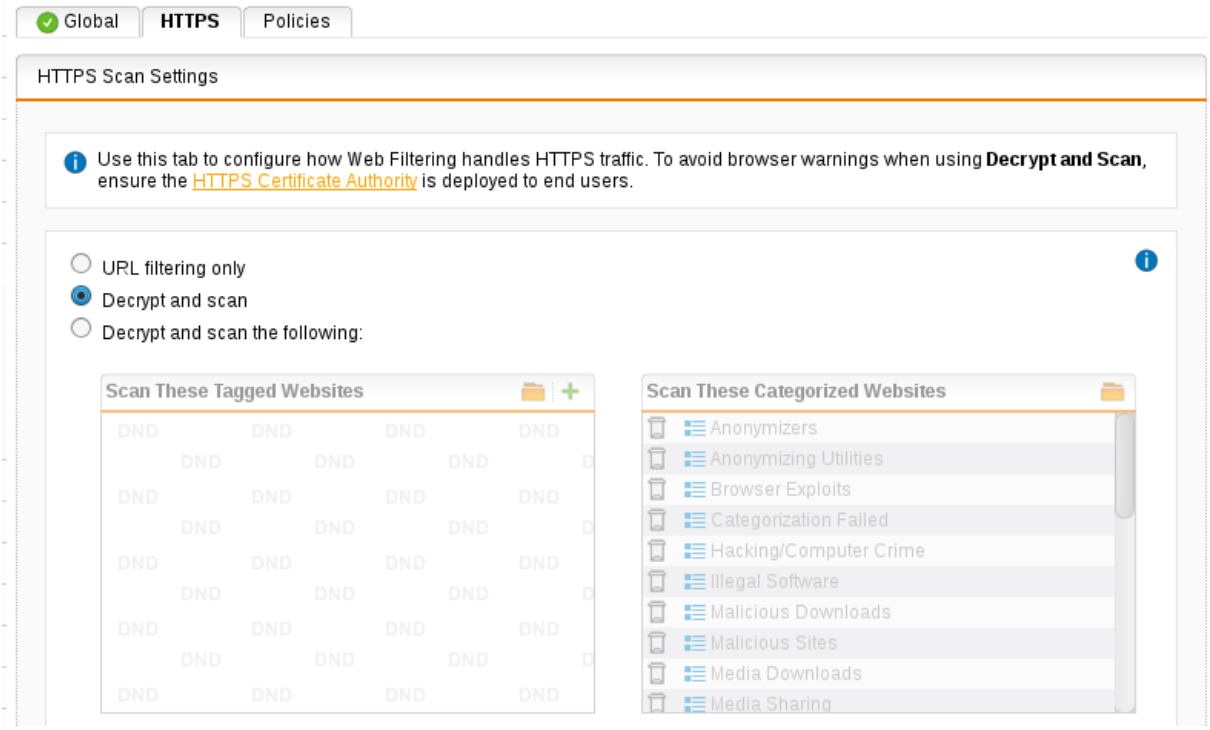


Figura 21: Inspección HTTPs

La configuración de políticas web es muy personalizable y se ofrece una herramienta para verificación de políticas. Los proxies pueden ser transparentes y autenticados, con posibilidad de usar SSO y directorio activo (AD). Hay que tener en cuenta que se pueden configurar distintos proxies de filtrado en distintos modos. Existen políticas basadas en tiempo, en usuarios y grupos, así como la posibilidad de imponer cuotas basadas en tiempo y ancho de banda. También es posible filtrar y autenticar en función del tipo de dispositivo, como puedan ser dispositivos iOS, Android, Mac, Windows u otros. Finalmente, el dispositivo permite activar una función que a través de una contraseña permite saltarse temporalmente los filtros definidos.

En la protección de correo se usan filtros anti spam, con servicio de reputación, motor heurístico, escaneo de URLs, filtro de palabras y expresiones, etc. También es posible activar la detección de direcciones relacionadas con phishing en el interior de los correos. Asimismo, se pueden configurar listas blancas y negras globales o por usuario. Existe soporte para SMTP, POP3 y verificación de receptores en el directorio activo. Para el análisis de malware se pueden usar ambos motores antivirus, y es capaz de analizar los formatos de email embebidos. Las características criptográficas soportadas son el cifrado y descifrado transparente de correos SMTP, el soporte de S/MIME, OpenPGP, TLS, y de servidor PGP, así como el escaneo antivirus de correo cifrado. Igualmente, existe un motor DLP (Data Loss Prevention) que escanea automáticamente los emails y adjuntos para buscar datos sensibles, que permite el uso de filtros personalizados o la utilización de listas de control incluidas que son acordes a PII, PCI, HIPAA y otras normativas internacionales. También es posible configurar los pies y avisos legales de correo, así como manipular las cabeceras del correo.

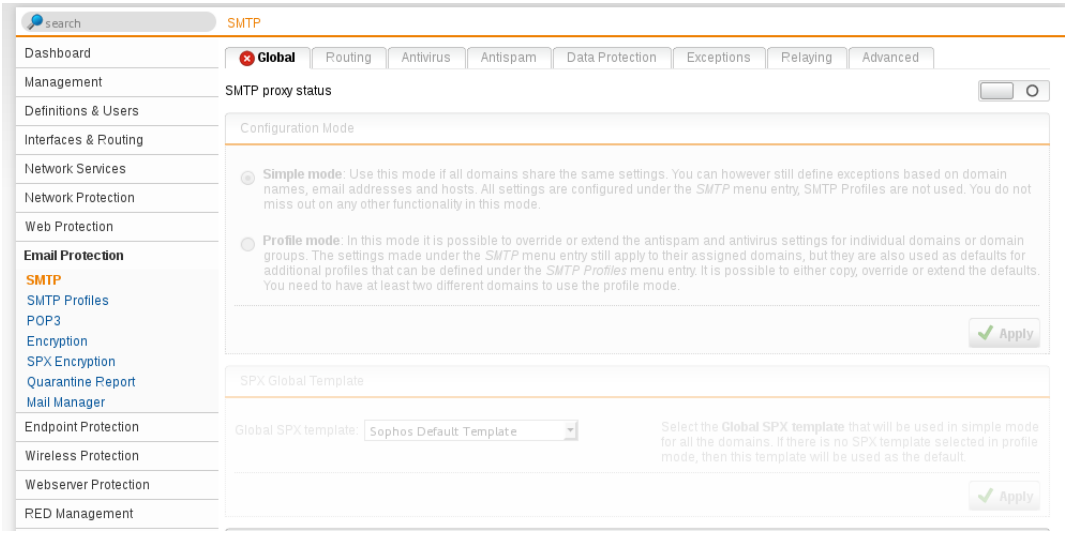


Figura 22: Características de seguridad de correo

Es posible proteger endpoints con clientes descargables para Windows, que permiten la gestión centralizada y alertar de dispositivos afectados.

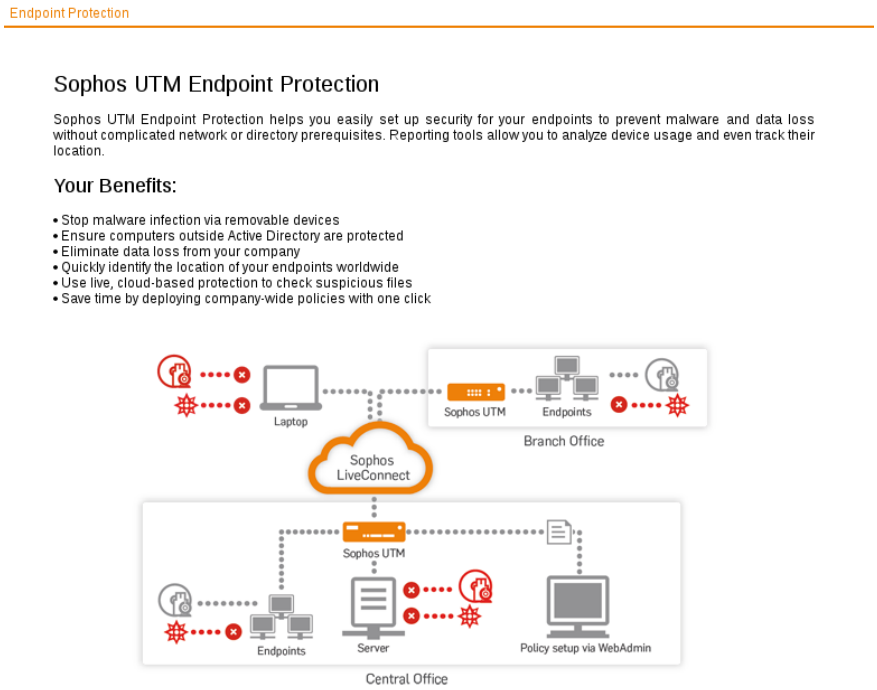


Figura 23: Protección de Endpoints

En cuanto a la seguridad WIFI es posible gestionar de forma centralizada los distintos puntos de acceso, redirigiendo todo el tráfico de forma automática a través del UTM. El producto permite gestionar hasta 8 SSIDs simultáneos, utilizar cifrado WPA2 Enterprise, y activar autenticación RADIUS. También se pueden crear accesos de invitado para el portal captivo, tanto sin restricción como basados en códigos temporales (diarios o semanales) o franjas horarias.

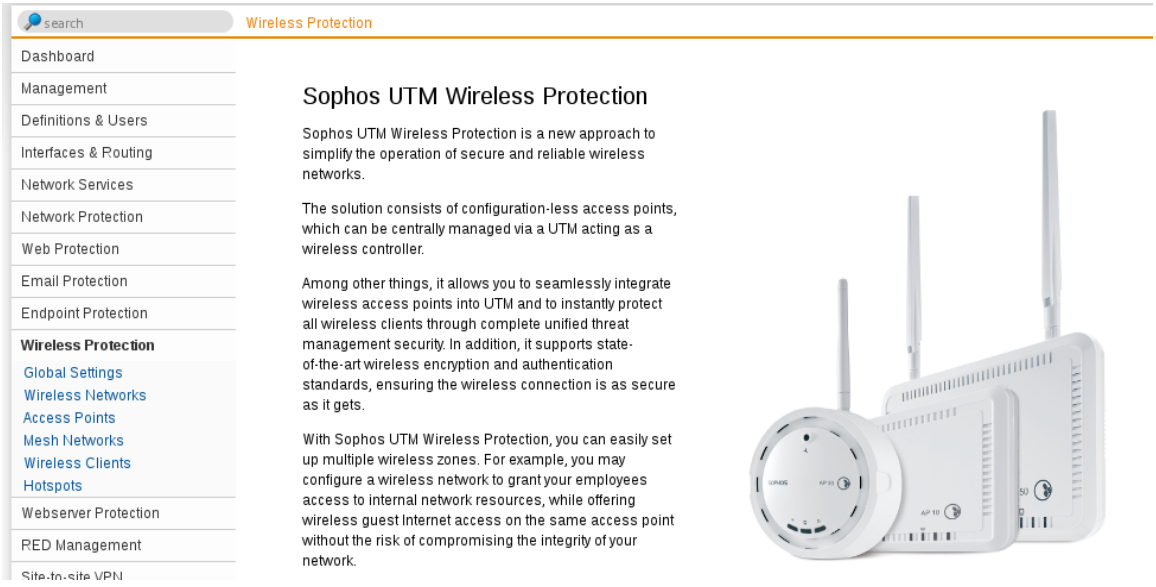


Figura 24: Protección Wireless

El firewall de aplicaciones tiene diversas funciones. Permite proxy inverso, hardening de URLs, formularios y firmado de cookies con certificados. Aparte de hacer uso del doble motor antivirus, tiene reglas para prevención de escalada de directorios, inyecciones SQL, ataques de tipo Cross-Site-Scripting (XSS) y otros ataques web. Las reglas pueden ser editadas, añadidas y configuradas de forma manual. Además, permite hacer HTTPs offloading, balanceo de carga y dispone de perfiles predefinidos para Microsoft Outlook Web Access (OWA)

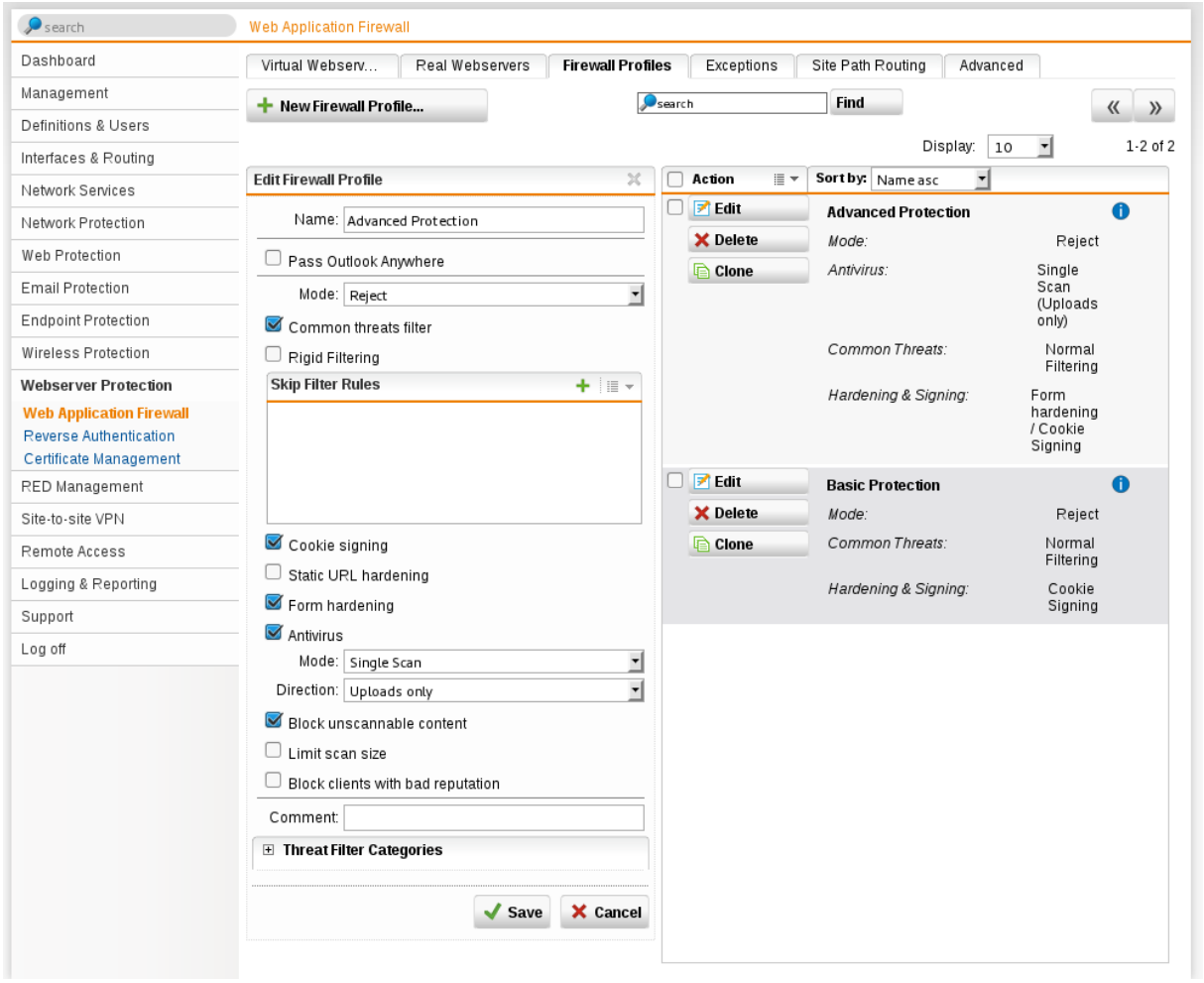


Figura 25: El potente WAF de Sophos

Para el acceso remoto y creación de VPNs también se permiten diversos tipos de configuraciones. Es posible crear VPN site-to-site mediante SSL e IPSEC, con cifrado AES256/3DES, PDFS, RSA, certificados X.509 y claves previamente compartidas. Para las VPN de acceso remoto también se puede usar PPTP, L2TP, SSL, IPSec y existe soporte para iPhone, iPad y el cliente de Cisco, así como una interfaz HTML5.

La autenticación se puede realizar a través de PSK, PKI, Smartcads, Tokens y XAuth. El cifrado soporta AES (128/192/256), DES, 3DES, Blowfish, RSA (2048), DH grupos 1/2/5/14,

MD5 y SHA-256/385/512. De cara a una fácil configuración se puede descargar un software cliente, con configuración y claves/certificados personalizados para la instalación automatizada. Como en el resto de políticas, es posible gestionar reglas basadas en identidad.

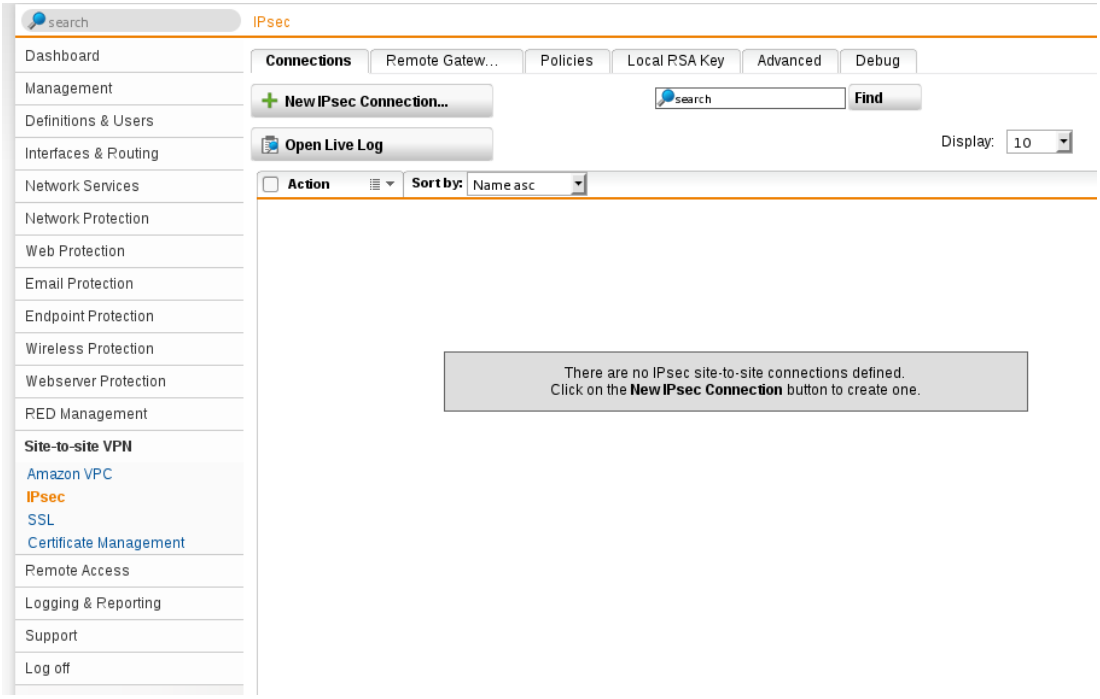


Figura 26: Configuración Site-to-Site VPN

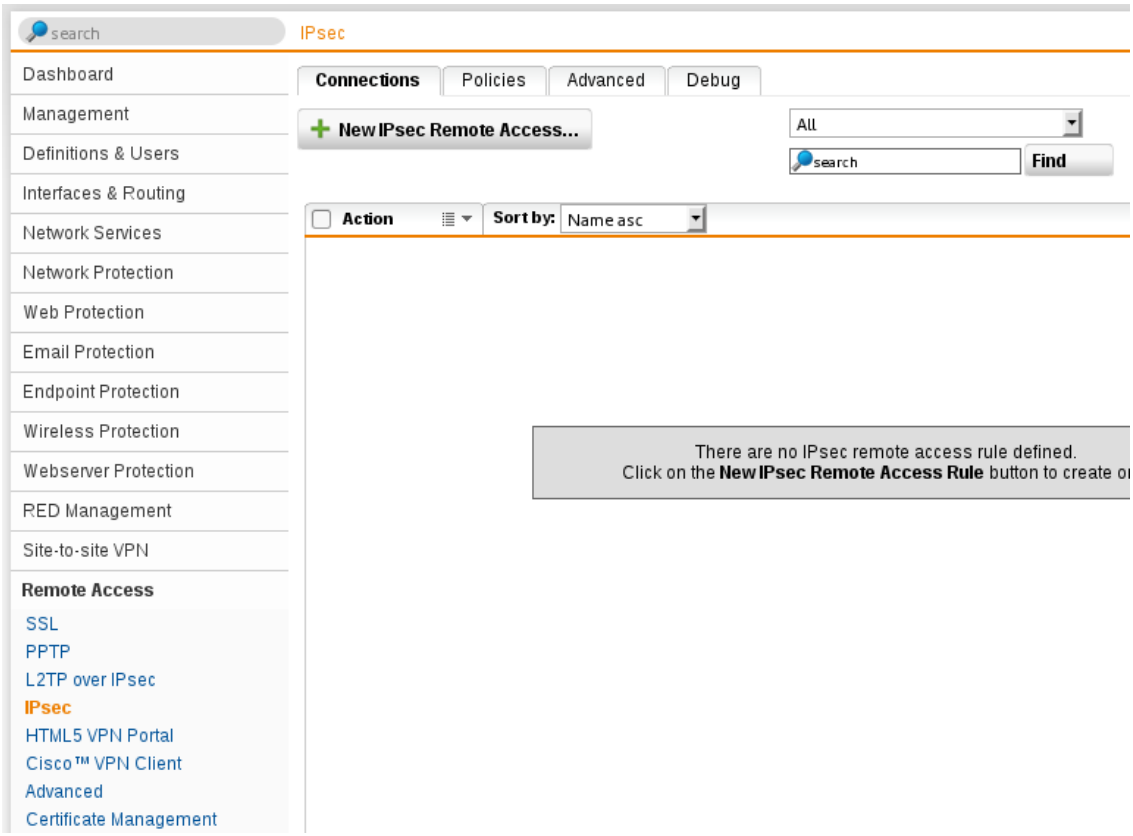


Figura 27: Configuración de Acceso Remoto

Finalmente para los registros es posible configurar syslogs remotos, rotaciones nocturnas, envío por email, FTP, SMB y SSH. Se pueden hacer informes diarios, crear informes ejecutivos, informes basados en identidad, y consultarlos vía web o exportarlos como PDF y CSV. También es posible configurar las políticas de archivado y configurar la protección de campos de datos para el cumplimiento normativo.

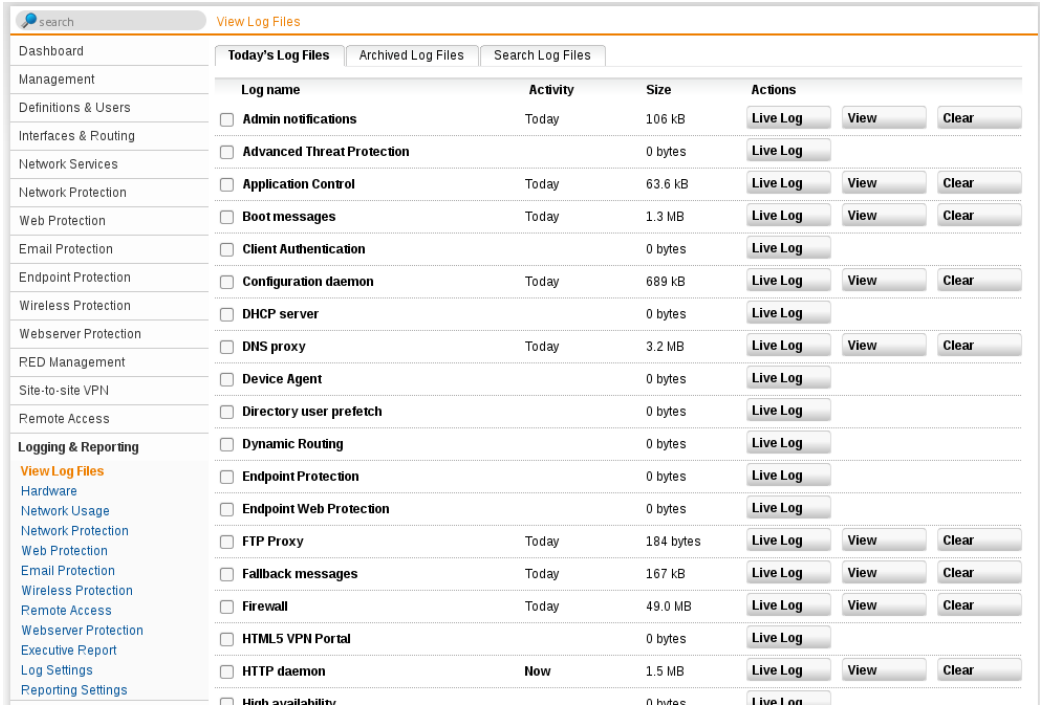


Figura 28: Configuración de logs e informes

2.3.2 Untangle

Untangle es un UTM que ofrece modalidades sin coste y de pago, y que en cualquiera de los casos puede ser utilizado en entornos comerciales. Sin embargo, las versiones gratuitas de cada módulo están limitadas, teniendo acceso a menos recursos y a un conjunto de funcionalidades más pequeño que la versión de pago, y algunos módulos sólo están disponibles en la versión de pago. Cada funcionalidad se ofrece en módulos separados, por lo que es posible adquirir cada módulo de forma independiente para personalizar el tipo de seguridad que necesitamos, o adquirir el pack completo de seguridad [26].

El panel de control permite ver todos los módulos instalados y activarlos o desactivarlos uno por uno, comprobar estadísticas de funcionamiento, o comprobar datos como el número de sesiones abiertas, el tráfico o los recursos utilizados por el UTM.

Figura 29: Cuadro de mandos principal de Untange

Desde la pestaña de aplicaciones se pueden ver los módulos disponibles e instalarlos uno por uno, permitiendo la configuración a nivel de aplicación del UTM.

Figura 30: Instalación individual de módulos

El filtro de contenidos tiene numerosas categorías, permitiendo políticas de paso, bloqueo o registro. También se pueden bloquear categorías enteras, sitios individuales, tipos de fichero por extensión y tipos MIME. La versión gratuita no permite inspeccionar el tráfico cifrado, por lo que este filtro tiene una importante limitación en este sentido.

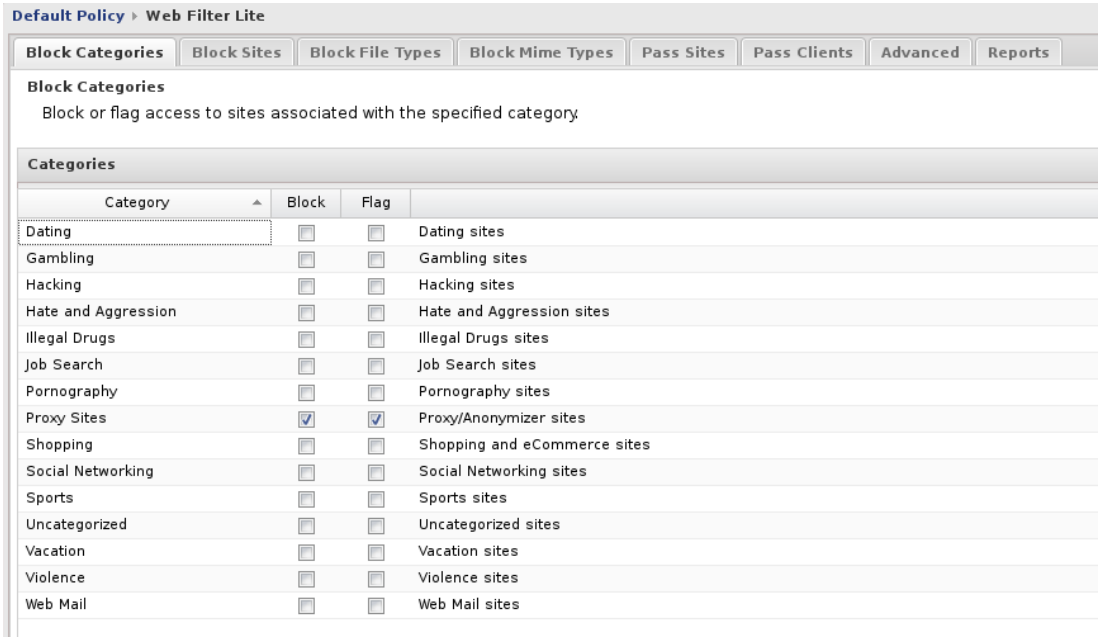


Figura 31: Filtro de Contenidos

El sistema de análisis antivirus usa un único motor antivirus (ClamAV), y puede acceder al tráfico HTTP, a los emails SMTP, y al protocolo FTP. Este motor sólo permite la detección de malware, por lo que no es posible desinfectar ficheros.

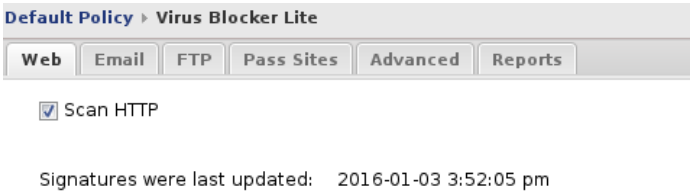


Figura 32: Virus Blocker Lite

Para la seguridad mail existen los módulos de SPAM y Phishing, con interfaces muy sencillas y que trabajan con el protocolo SMTP. Además, dispone de un filtro basado en imágenes para evitar técnicas de spam no textuales. Además, los usuarios pueden gestionar sus propias carpetas de cuarentena.

Figura 33: Bloqueo Phising

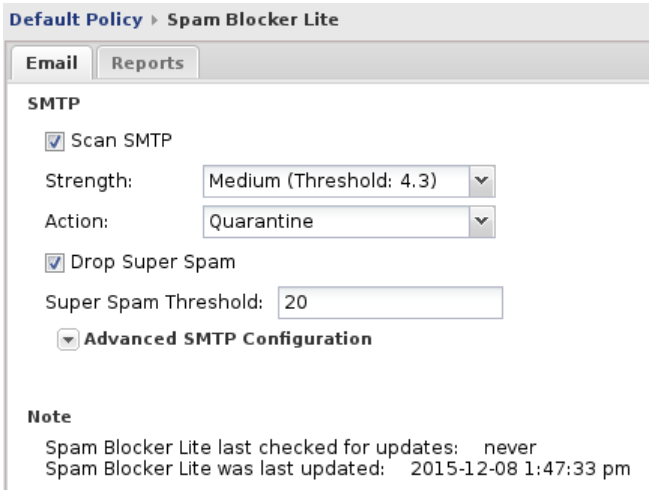


Figura 34: Bloqueo de SPAM

En la capa de nivel de aplicación existe un módulo de control de aplicaciones. En su versión comercial existen miles de firmas para identificar aplicaciones, sin embargo, en su versión gratuita estos patrones no están incluidos y deben ser creados manualmente, necesitándose un conocimiento de protocolos muy alto para poder crear firmas con los que registrarlos o bloquearlos.

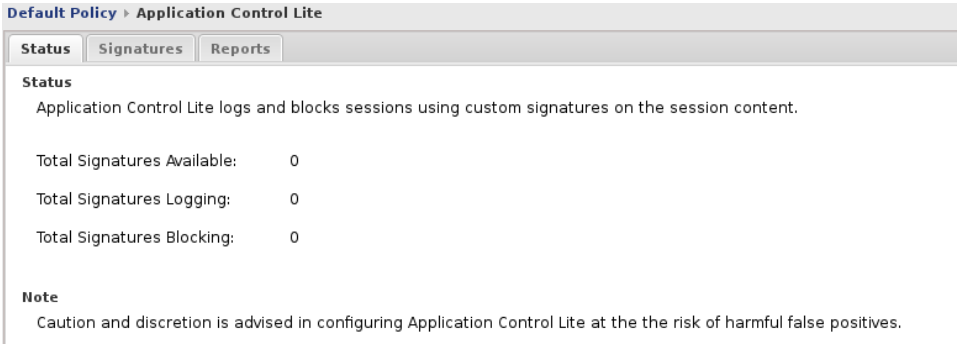


Figura 35: Control de aplicaciones capa 7

También dispone de un portal captivo, con apariencia personalizable, que se puede configurar para exigir a los usuarios la visualización y aceptación de políticas de uso aceptable. Para la autenticación de usuarios se pueden usar repositorio local al dispositivo, directorio activo (AD) y RADIUS. Este portal se puede mostrar sólo a determinadas redes, tipos de dispositivos o sistemas operativos. Además, se puede mostrar un aviso a los usuarios por exceso de cuotas o si son marcados por comportamiento no aceptable por parte de un administrador.

Figura 36: Conexión con AD y RADIUS

También es posible configurar un firewall muy sencillo, un sistema IPS con múltiples reglas actualizadas desde el proyecto SNORT, y un sistema de bloqueo de anuncios publicitarios. Este último, aunque no parezca especialmente enfocado a la seguridad, puede ser útil en las cada vez más frecuentes campañas de malvertising [40], en las que los atacantes aprovechan campañas publicitarias para extender malware entre los usuarios.

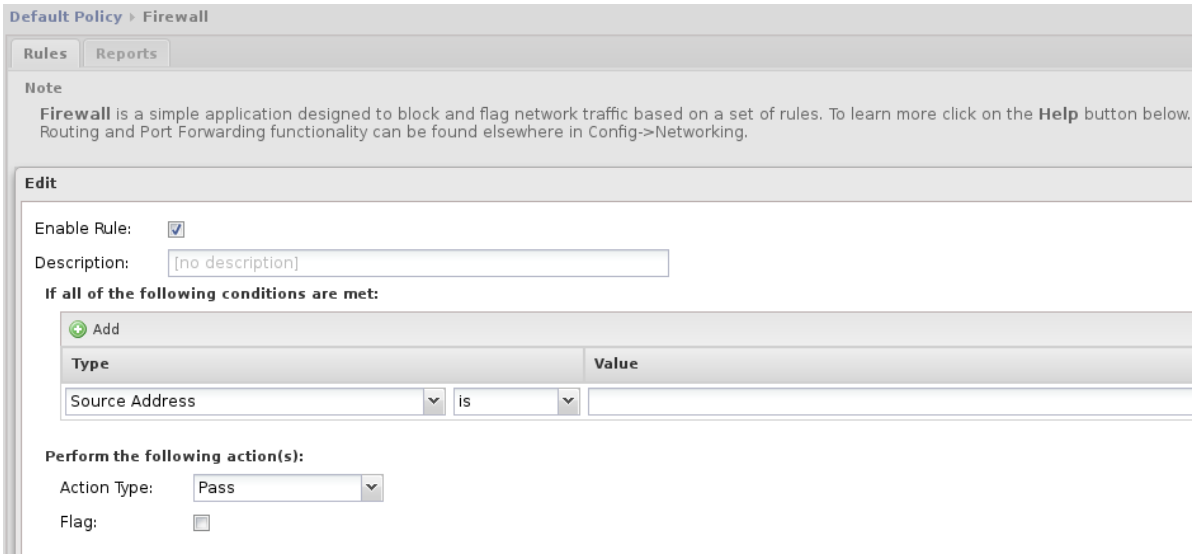


Figura 37: Firewall de Untangle

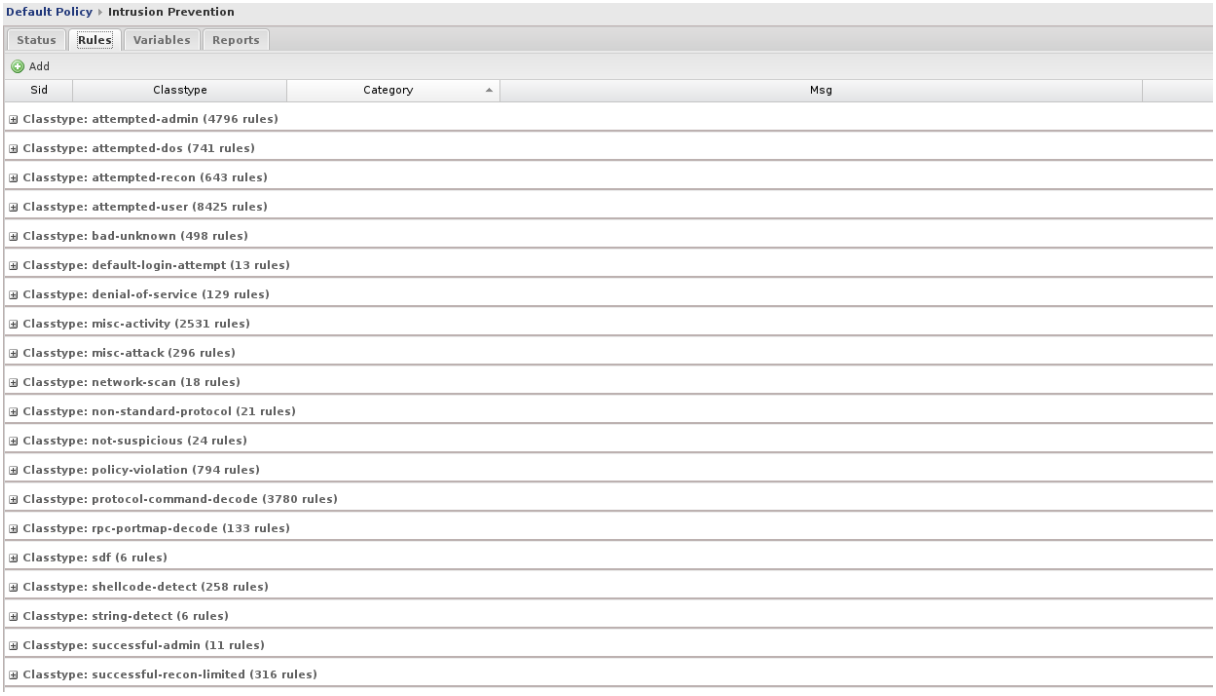


Figura 38: Filtros IPS

Figura 39: Filtros de publicidad web y de cookies

Finalmente también existe un módulo de instalación de clientes y servidor OpenVPN, y un módulo para la gestión y generación de informes.

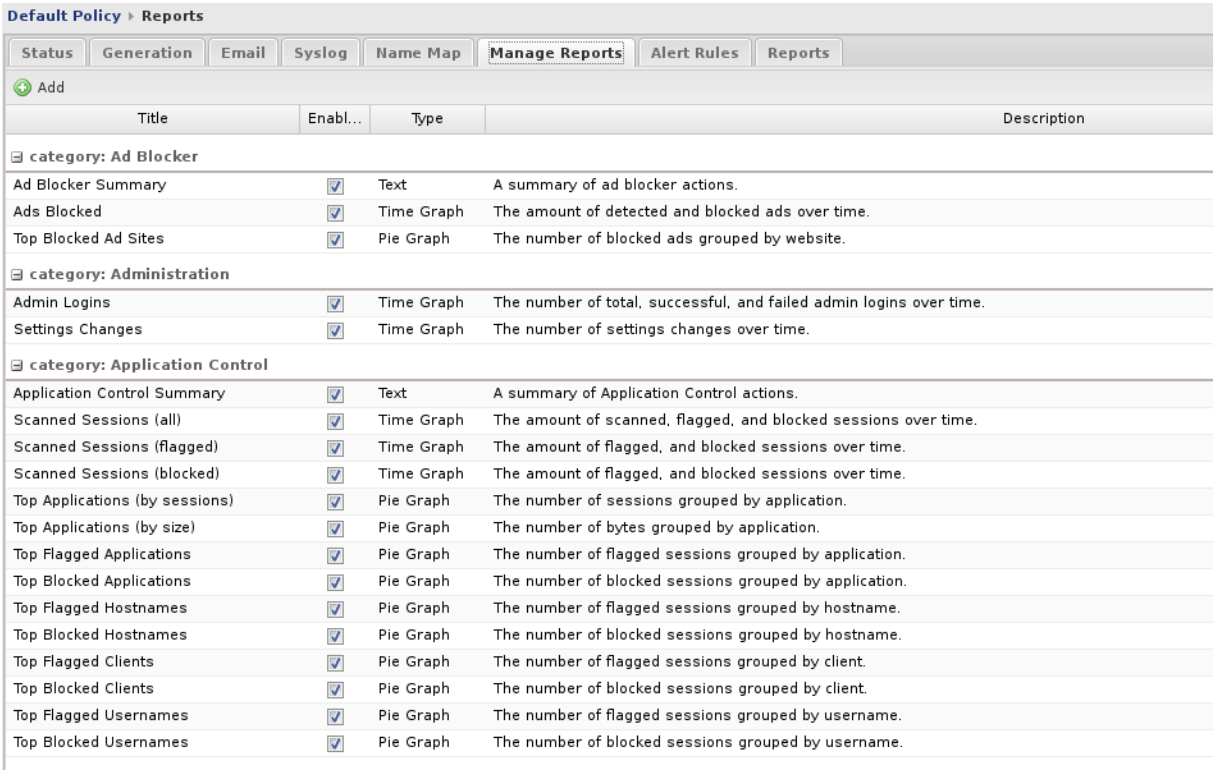


Figura 40: Módulo de informes.

La versión de pago incluye soporte, las versiones completas de todas las funcionalidades, y además ofrece los módulos de inspección de tráfico HTTPs, de control de ancho de banda, balanceo y failover WAN, caché web, VPN IPSec, gestor de políticas, un conector mejorado de directorios, y la posibilidad de configurar el UTM para adaptarlo a nuestra marca comercial. El módulo antivirus, por su parte, utiliza tecnología más avanzada de Bitdefender, que también permite la desinfección de los archivos.

2.3.3 Endian

Endian se trata de una solución software libre con licencia GPL. Este producto se puede adquirir como producto gratuito, o en su versión de pago que incluye soporte y funcionalidades extra. Ambas versiones pueden ser utilizadas libremente en entornos comerciales [27] [28].

En el cuadro de mandos principal podemos ver las características del dispositivo, el nivel de parcheo, la información de recursos consumidos, y estadísticas del tráfico en las interfaces de red. También es posible acceder a dashboards específicos para cada módulo, con gráficos y estadísticas, y la posibilidad de comprobar el estado activo o apagado de cada módulo.

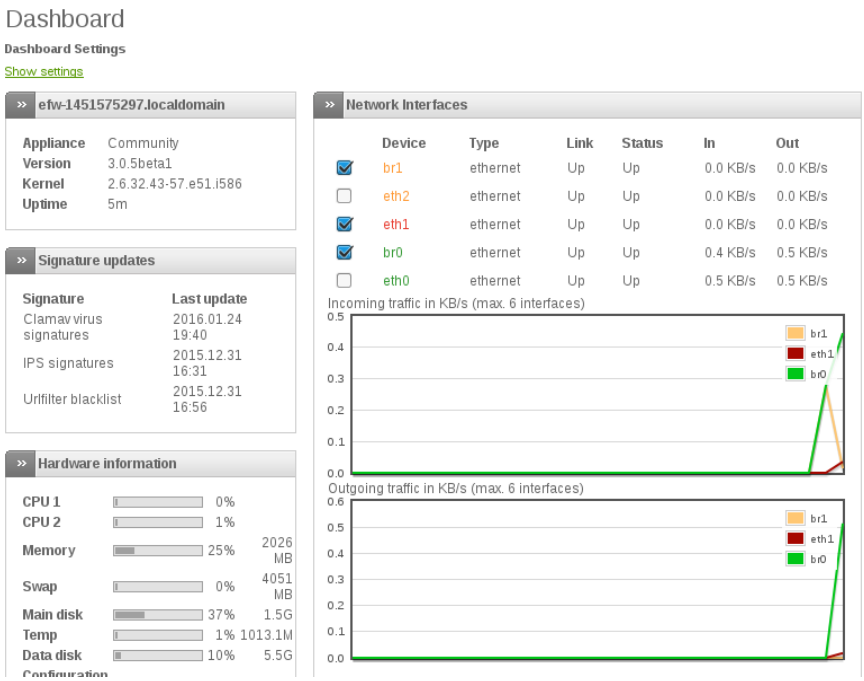


Figura 41: Cuadro de mandos principal de Endian

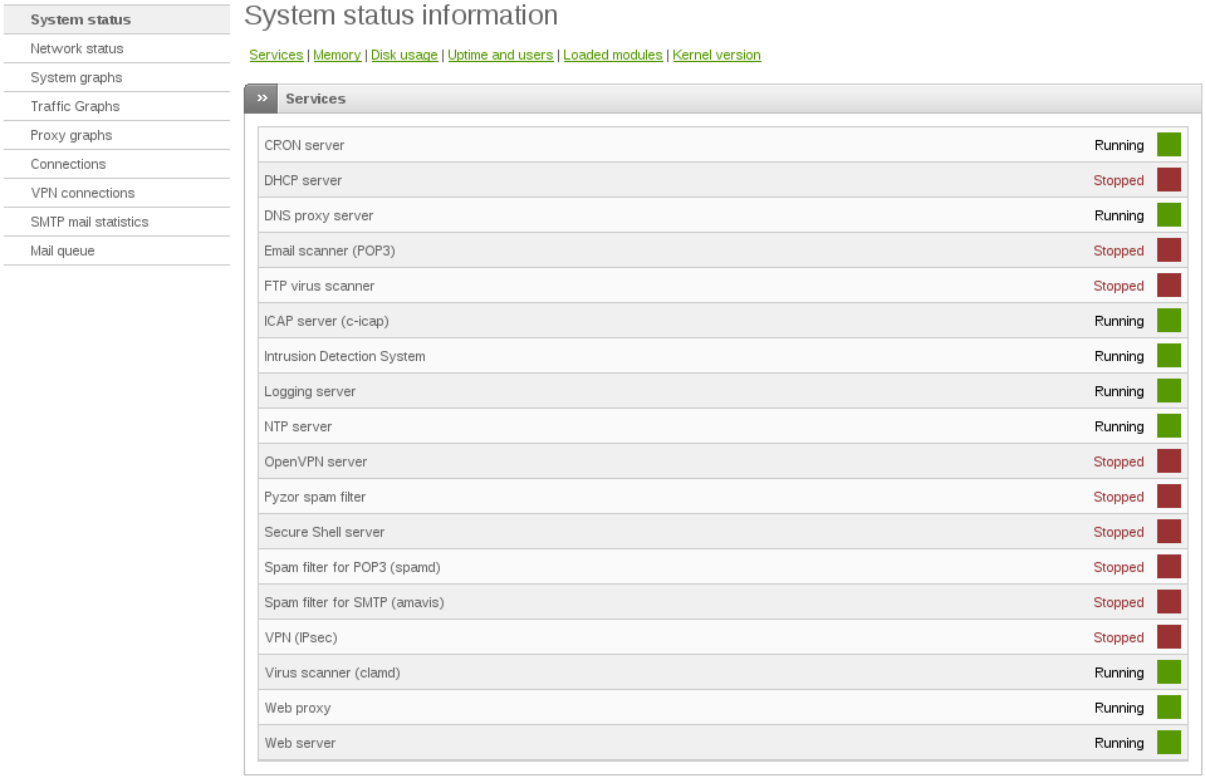


Figura 42: Gráficos y estadísticas de los módulos

La pestaña de configuración de red permite crear hosts, rutas y administrar las interfaces, pudiendo hacer uso de múltiples WAN con failover automático.

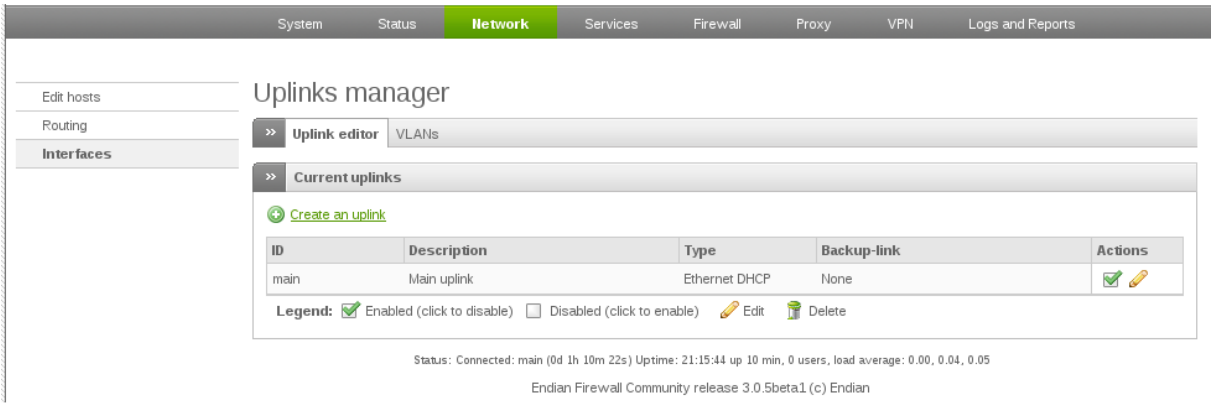


Figura 43: Configuración de red

En la de servicios podemos configurar QoS, DNS dinámicas, el motor antivirus (ClamAV), los servidores DHCP, SNMP y NTP, el motor de aprendizaje contra spam y phishing), así como la monitorización de tráfico y módulos de IPS.

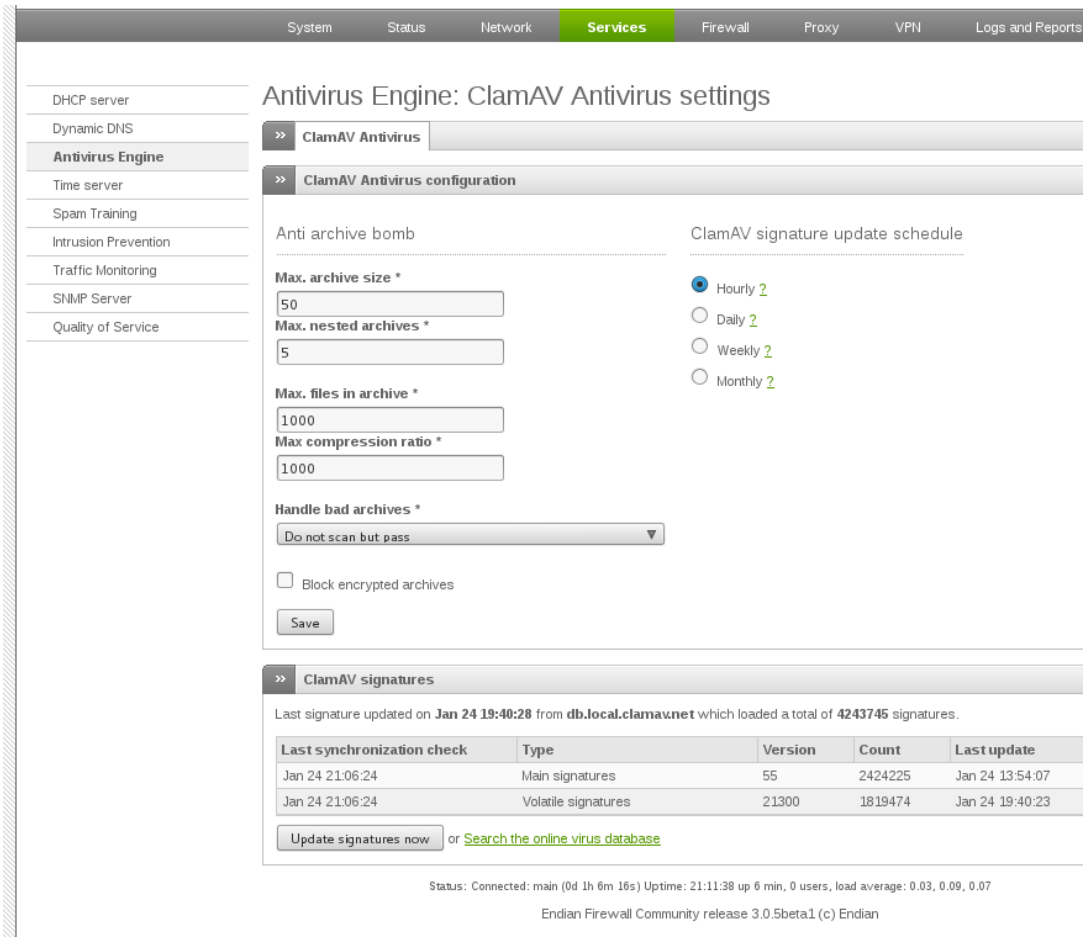


Figura 44: Endian dispone del motor antivirus ClamAV

Un detalle a tener en cuenta es que el motor antivirus, en su licencia gratuita, sólo permite la detección y cuarentena de las muestras, pero nunca la desinfección.

El sistema de prevención de intrusos tiene filtros agrupados en categorías, en un formato muy similar al resto de soluciones de seguridad (basadas en Snort), y permite habilitar, deshabilitar o configurar las reglas por grupos e individualmente.

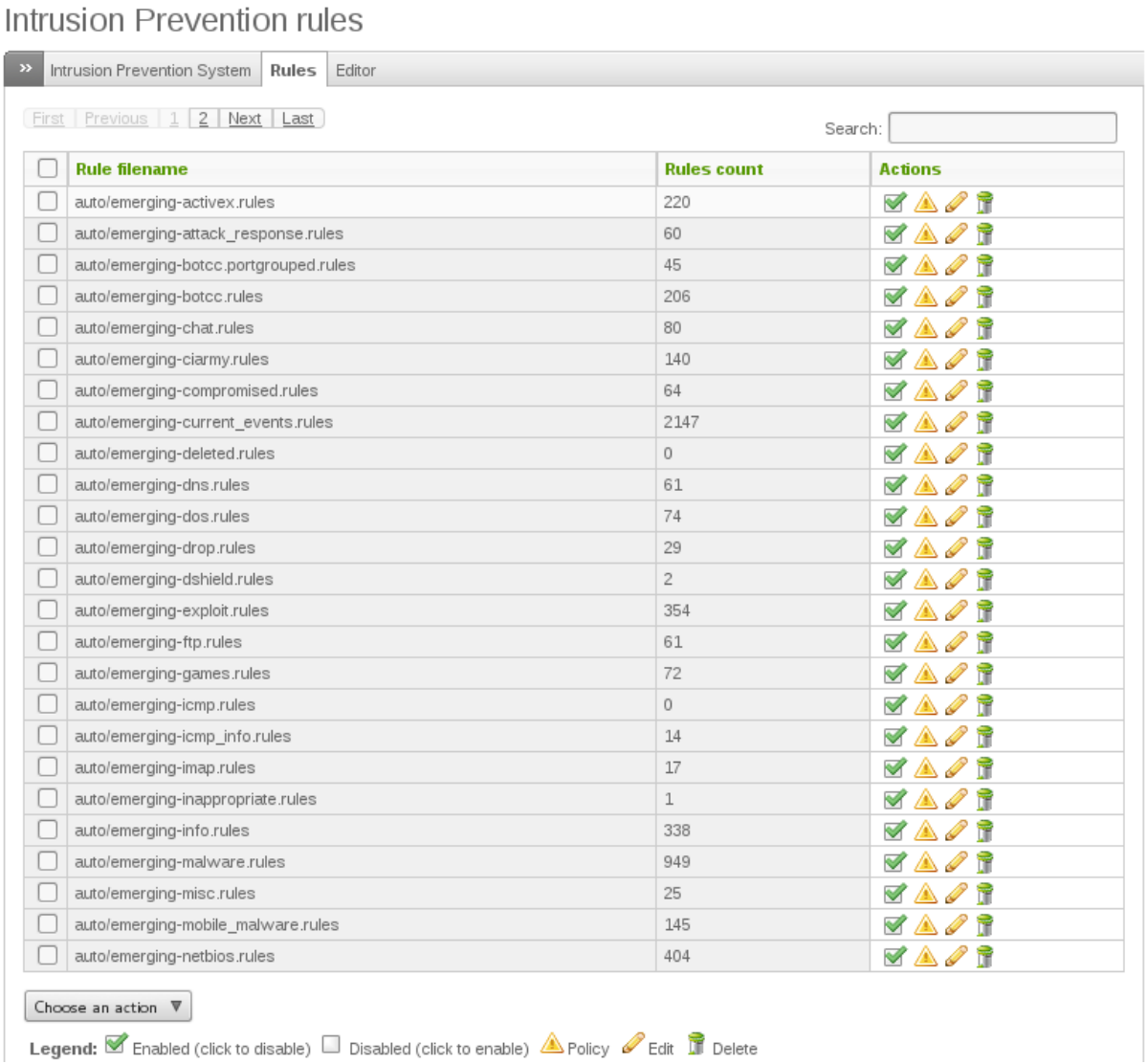


Figura 45: Reglas IPS

Endian dispone de un firewall de estado. Una de sus características más interesantes es el firewall de zonas, que permite establecer políticas en función de cada una de las zonas de la red que hemos configurado, ayudando a la gestión mediante un código de colores.

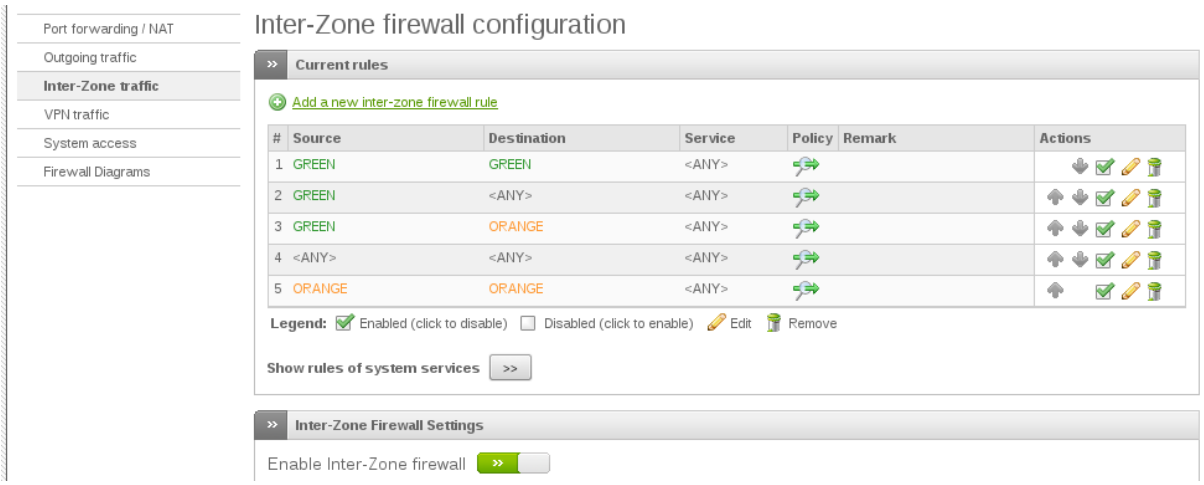


Figura 46: Firewall Inter-Zona de Endian

En cuanto a la seguridad web, la licencia gratuita de Endian permite el acceso al proxy con capacidad de inspección de tráfico cifrado HTTPs. Para esta función se pueden exportar los certificados que se deberán importar en los puntos finales para que los navegadores no muestren mensajes de error de certificado. Esta característica, como veremos en las pruebas, es muy importante para mantener un grado de seguridad alto y evitar que las amenazas pasen desapercibidas por canales cifrados. El filtro de contenidos básico, sin embargo, sólo tiene 1.8 millones de URLs categorizadas. También hay proxies para HTTP y FTP, y la autenticación puede ser local, en RADIUS, AD, o LDAP.

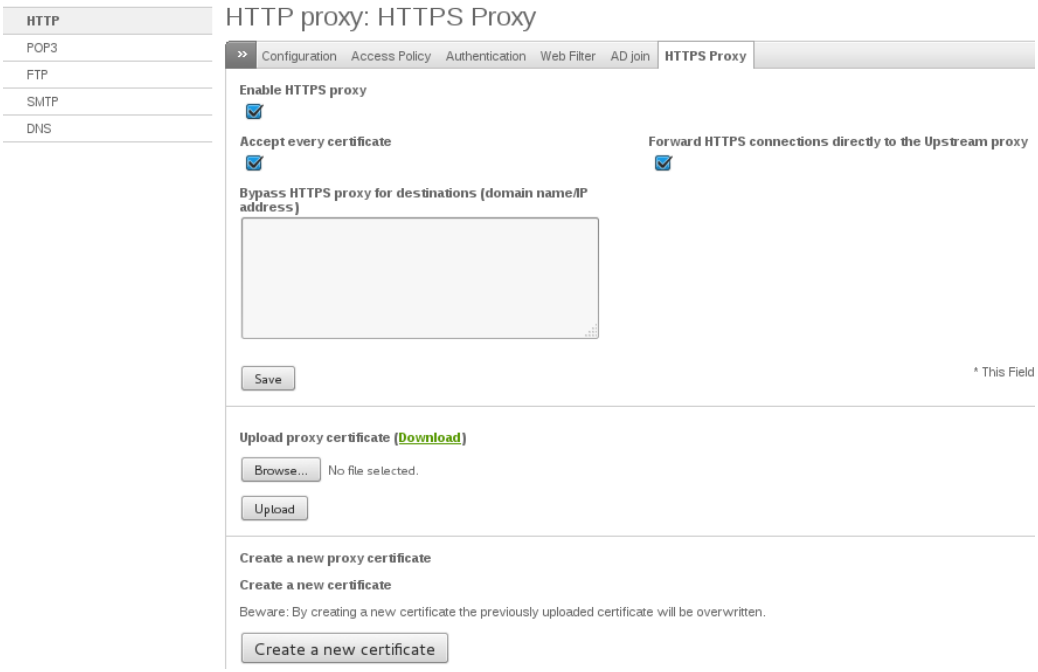


Figura 47: Proxy HTTPs para inspección de tráfico cifrado

Dentro de la creación de VPNs se ofrece soporte para SSL e IPSec, pudiendo usar tanto un servidor OpenVPN como establecer nuevos túneles como cliente VPN.

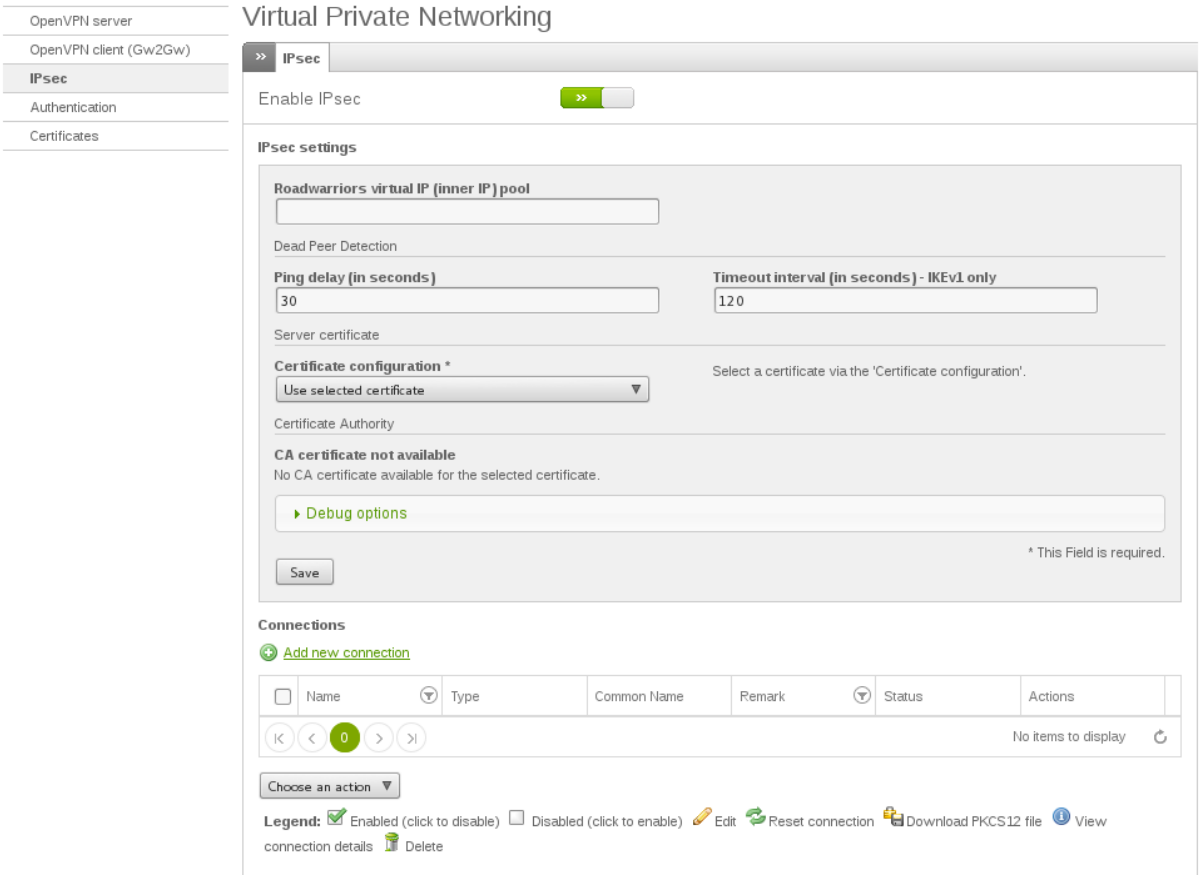


Figura 48: Características de configuración VPN

En cuanto a los registros, aparte de ver los informes históricos se pueden ver los registros en tiempo real para cada uno de los módulos.

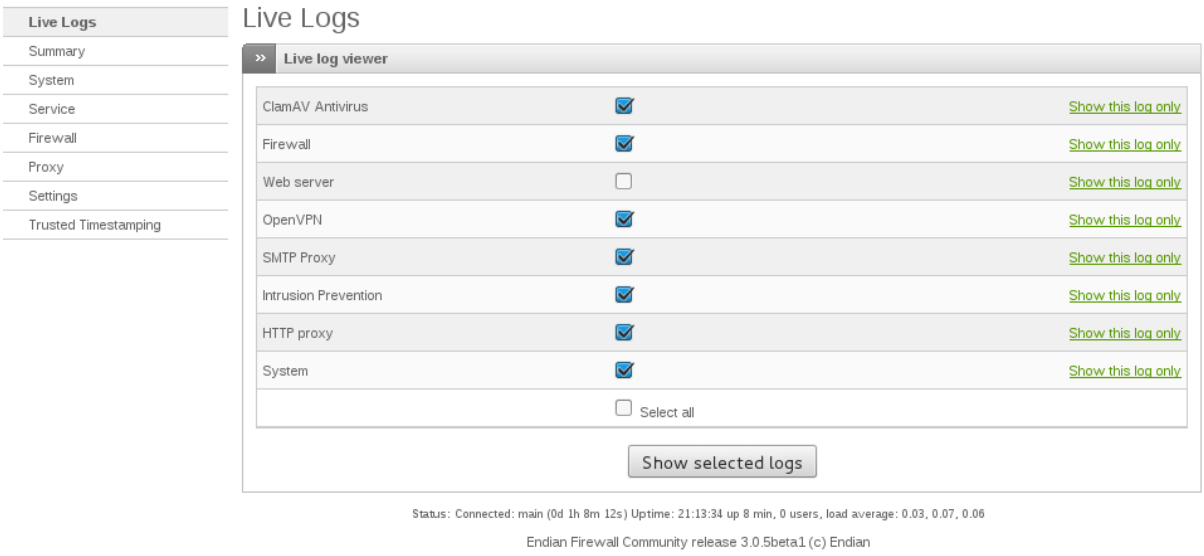


Figura 49: Registros en tiempo real

Las características de la licencia comercial incluyen versiones mejoradas de algunas funciones, como un doble motor antivirus (ClamAV & Panda) que añade capacidad de desinfección, un filtro de contenidos mucho más completo que hace uso del feed de Cyren, con más de 150 millones de URLs categorizadas, así como el filtro de la misma compañía contra spam, y más posibilidades de configuración de VPNs como One Time Passwords (OTP), y soporte L2TP o XAuth. Igualmente, se añaden nuevas características como control de aplicaciones en capa 7, posibilidad de configuraciones en alta disponibilidad, gestión centralizada de dispositivos, y posibilidad de configurar las notificaciones vía Python que posteriormente pueden ser enviadas a través de SMS.

2.3.4 Uso de soluciones sin soporte en entornos comerciales

El objetivo del estudio es analizar la seguridad de soluciones UTM de libre acceso. La facilidad de acceso a estos productos permite su investigación a cualquier interesado, y frente a situaciones de escaso presupuesto, conseguir un producto de seguridad que siempre será preferible frente a la ausencia total de seguridad. Sin embargo, a la hora de utilizar soluciones gratuitas en un entorno comercial hay que tener diferentes aspectos en cuenta:

- Las soluciones gratuitas o de comunidad no tienen soporte del fabricante. Ante cualquier eventualidad la única información disponible es la que se puede encontrar públicamente en foros y páginas web de Internet.
- Habitualmente no se tratan de productos estables, puesto que los fabricantes aprovechan estas versiones para probar nuevas funcionalidades de sus productos antes de introducirlas en las versiones comerciales, una vez que los principales fallos han sido corregidos.
- El número de actualizaciones es mucho menor, generalmente, ante la aparición de cambios mayores. En ese sentido, las ventanas de tiempo en las que el dispositivo no está actualizado frente a las últimas amenazas son mucho mayores que en un dispositivo comercial.

Teniendo todo esto en cuenta no se recomendaría hacer un uso indefinido de productos de este tipo en un entorno comercial. La recomendación es usarlos para el ámbito doméstico, o para la realización de estudios previos ante la posible adquisición de productos comerciales en un futuro cercano.

3. Desarrollo del Estudio

3.1 Creación del Laboratorio Virtual

Para la creación del laboratorio se ha utilizado el software de virtualización VirtualBox. Dentro del laboratorio se han usado cuatro máquinas virtuales, cada una con roles diferentes dentro de las pruebas realizadas.

Kali. Esta primera máquina del entorno, cuyo sistema operativo es Kali Linux, es la máquina que cubre tanto los perfiles del atacante activo como del usuario que conecta con un servidor bloqueado, o que intenta servir malware al usuario. En resumen, las actividades realizadas han sido:

- Desde esta distribución se han lanzado los escaneos de puertos y búsqueda de servicios activos en las máquinas vulnerables. La herramienta escogida para realizar el escaneo de puertos ha sido nmap.
- También se ha usado para lanzar escaneos automatizados sobre un servidor web vulnerable de la red. Como veremos posteriormente, la herramienta escogida para el análisis de vulnerabilidades web ha sido Arachni.
- Se ha comprobado el correcto funcionamiento de los filtros de contenidos a través de protocolos HTTP y HTTPS. Además, se han realizado descargas de software malicioso a través de HTTP y HTTPs para verificar la eficacia de los motores antivirus.
- Finalmente, se ha usado para intentar transmitir información al exterior a través de puertos abiertos en los UTM (puerto 80, tráfico HTTP) mediante la utilización de otro tipo de tráfico al esperado en dichos puertos.

UTM. Esta es la máquina cuya seguridad y funcionalidades van a ser analizadas. Durante el estudio se han instalado máquinas virtuales para las tres soluciones propuestas:

1. Sophos UTM Home Edition
2. Untangle
3. Endian Firewall Community

Wavsep. Esta máquina del laboratorio, con sistema operativo Debian, ejecuta el servidor Apache Tomcat que sirve la aplicación Wavsep.

Wavsep, o *Web Application Vulnerability Scanner Evaluation Project*, es una aplicación utilizada como benchmark para herramientas de análisis de vulnerabilidades. Esta aplicación sirve una serie de páginas con vulnerabilidades conocidas de tipo XSS, SQLi, LFI y RFI, así como páginas creadas para producir falsos positivos. Su objetivo es poder comparar la cantidad de detecciones de cada herramienta de análisis frente al total de fallos existentes en la aplicación, permitiendo así la comparación de las capacidades de distintas herramientas de análisis. Esta es la máquina que será expuesta al escaneo de vulnerabilidades mediante Arachni.

Metasploitable. En una de las máquinas del laboratorio se ha instalado la distribución Linux Metasploitable. Esta distribución está específicamente construida con una gran cantidad de software vulnerable, y cuyo objetivo es ofrecer un entorno de entrenamiento para aprender el uso del framework Metasploit. Esta distribución ofrece numerosos servicios que abren puertos en la red, y que nos servirán como benchmark para probar la eficacia de los UTM a la hora de impedir los escaneos de puertos.

3.2 Escenarios propuestos

En este apartado se muestran los diagramas de red que reflejan el entorno de red virtualizado que se ha usado para probar cada una de las soluciones UTM.

3.2.1 Escenario 1 (Sophos)

El siguiente diagrama muestra la red desplegada para probar Sophos UTM Home Edition. Desde la red de Kali (192.168.2.0) se han lanzado ataques a la red de Wavsep (192.168.3.0), atravesando los motores del IPS. Además, al realizar peticiones desde la red de Kali hasta Internet se pasa por los filtros de contenidos y motores antivirus que protegen al usuario final.

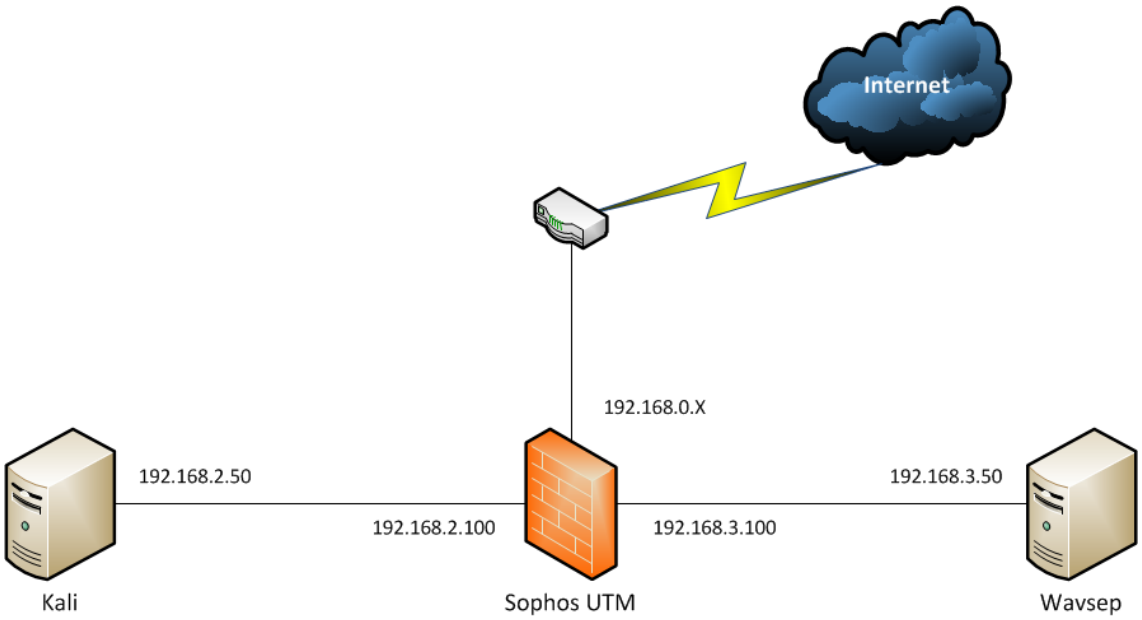


Figura 50: Escenario de pruebas para análisis de vulnerabilidades con Arachni usando la protección de Sophos.

3.2.2 Escenario 2 (Untangle)

El escenario para Untangle es exactamente el mismo, cambiando el dispositivo de protección usando las mismas redes y topología.

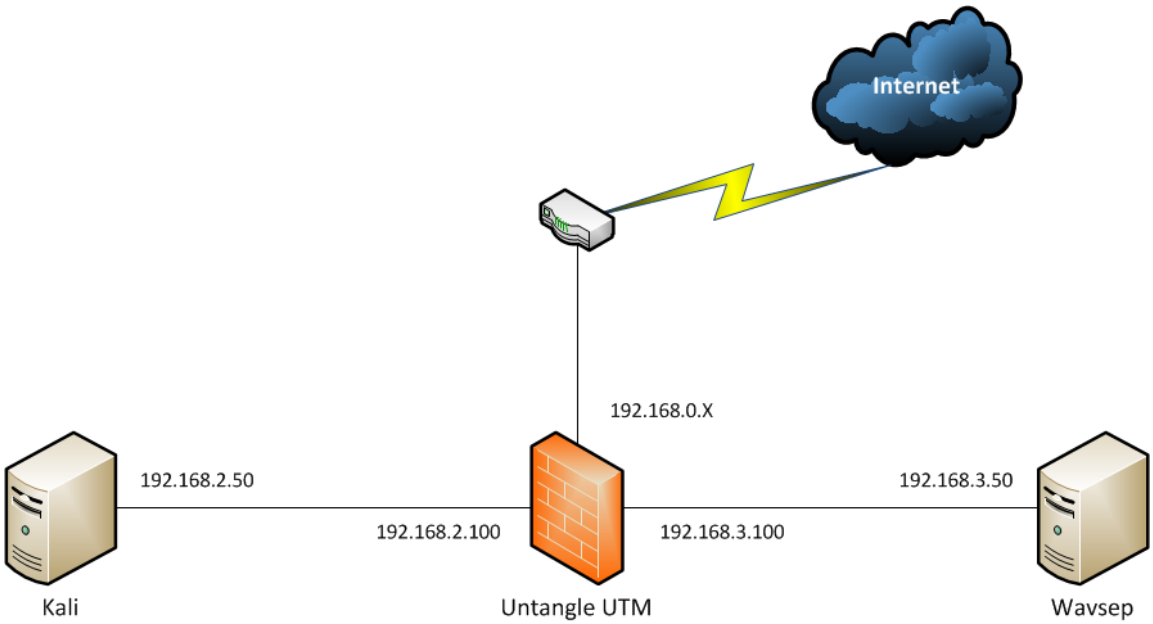


Figura 51: Escenario de pruebas para análisis de vulnerabilidades con Arachni usando la protección de Untangle.

3.2.3 Escenario 3 (Endian)

El escenario para Endian también comparte el mismo diagrama, situándose al atacante o usuario a proteger en la red 192.168.2.0, y los servicios vulnerables en la red 192.168.3.0.

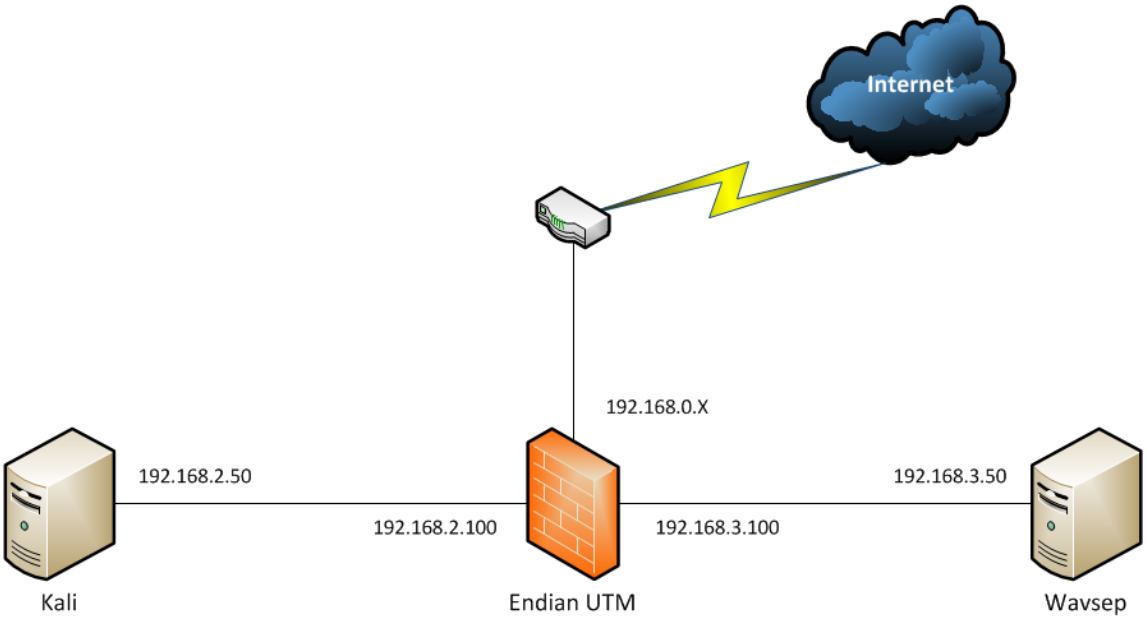


Figura 52: Escenario de pruebas para análisis de vulnerabilidades con Arachni usando la protección de Endian.

3.2.4 Escenario 4 (Port-Scanning)

En este último escenario se usa la misma topología, pero se sustituye la máquina Debian que contiene Wavsep por la distribución Metasploitable. Desde la red atacante (192.168.2.0) se ejecuta un escáner de puertos y servicios para comprobar la visibilidad de la máquina con Metasploitable, en la red 192.168.3.0. Este escenario se ha repetido una vez por cada UTM a analizar.

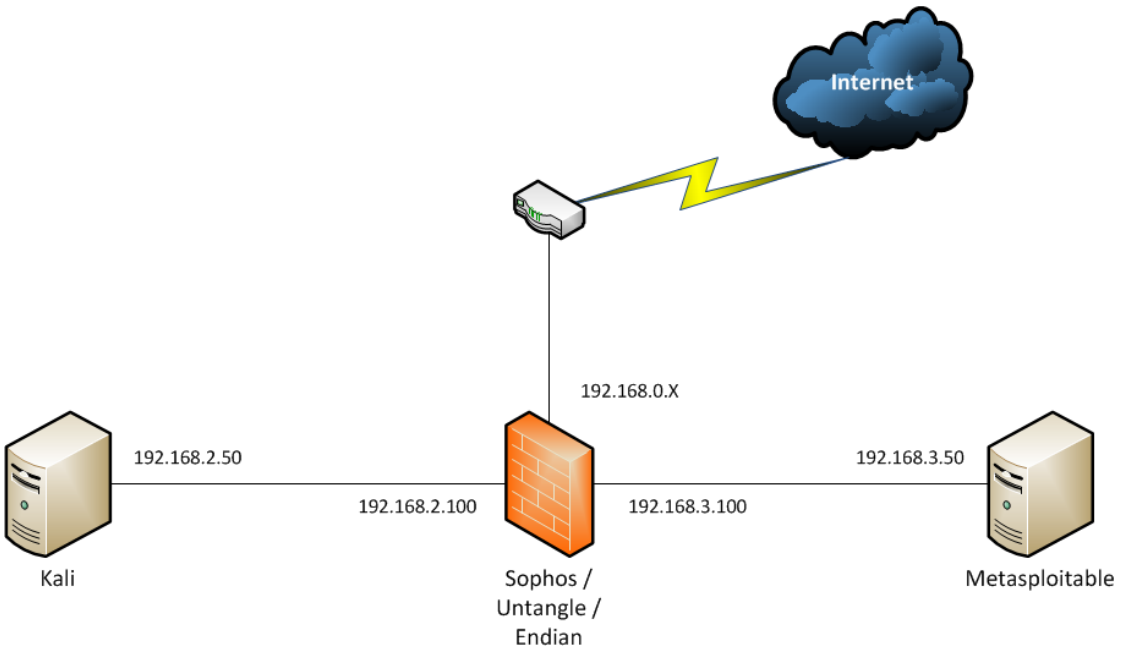


Figura 53: Escenario de pruebas para escaneo de puertos abiertos y servicios con nmap usando la protección de los distintos UTMs.

3.3 Ataques básicos

En esta categoría se han incluido varios ataques que se han considerado como básicos debido a que la dificultad para detectarlos y detenerlos es inferior a los de la categoría de ataques avanzados. En esta categoría se incluyen escenarios como un análisis de puertos, la protección de un servidor web, el filtro de contenidos en protocolo HTTP y la descarga de software malicioso ya conocido.

3.3.1 Servidor WEB protegido tras el UTM

El objetivo de esta prueba ha sido comprobar si el UTM es capaz de proteger un servidor vulnerable a distintos tipos de vulnerabilidades web. Para ello se ha lanzado la aplicación de análisis de vulnerabilidades web Arachni contra el sistema que aloja Wavsep. En primera instancia se ha usado la herramienta directamente contra el servidor vulnerable, para posteriormente comparar los resultados obtenidos tras proteger el servidor con cada solución UTM.

Las vulnerabilidades analizadas y que serán utilizadas como benchmark han sido:

- XSS (Cross-Site-Scripting)

Este tipo de ataques permiten inyectar código Javascript en páginas visitadas por el usuario de tal forma que evitamos la protección de *Same Origin Policy*. Esta política impide que scripts que provengan de distintos orígenes puedan compartir recursos (datos, métodos, etc).

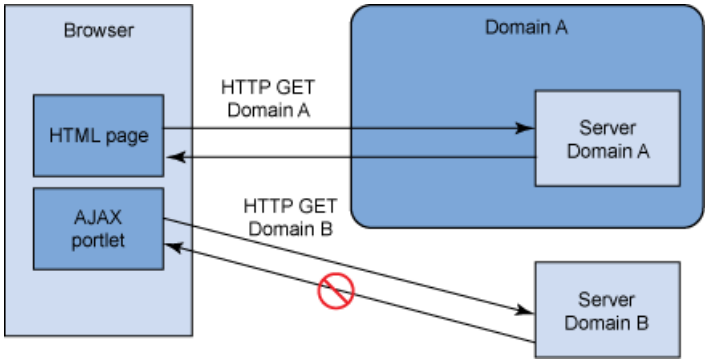


Figura 54: Same Origin Policy

Por ejemplo, en condiciones normales los recursos del dominio B no podrá leer el valor de una cookie enviada hasta el navegador por el dominio A. Para determinar el origen se tiene en cuenta el protocolo, el puerto, y el host:

Compared URL	Outcome	Reason
http://www.example.com/dir/page.html	Success	Same protocol and host
http://www.example.com/dir2/other.html	Success	Same protocol and host
http://www.example.com:**81**/dir/other.html	Failure	Same protocol and host but different port
https://www.example.com/dir/other.html	Failure	Different protocol
http://**en.example.com**/dir/other.html	Failure	Different host
http://**example.com**/dir/other.html	Failure	Different host (exact match required)
http://**v2.www.example.com**/dir/other.html	Failure	Different host (exact match required)

Figura 55: Condiciones de éxito y fallo de la política de mismo origen

Sin embargo y como adelantábamos, un ataque XSS consigue inyectar el código Javascript en la respuesta del servidor A, de tal forma que el código pasa a formar parte del mismo host y por tanto tendrá acceso a cualquier recurso compartido en este origen.

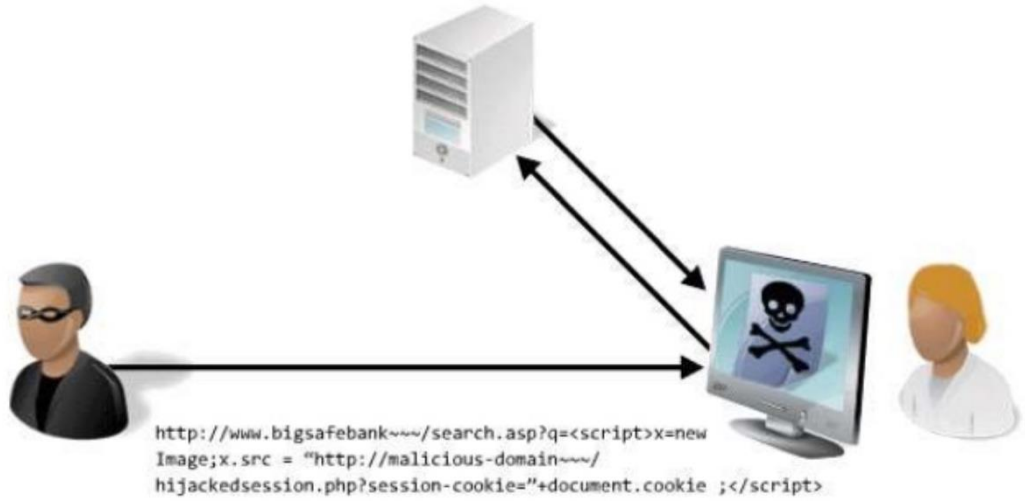


Figura 56: *Un atacante lanza un XSS*

En el ejemplo de la *Figura X* el atacante consigue inyectar el siguiente código: <script>x=newImage;x.src = *http://malicious-domain.com/hijackedsession.php?session-cookie="+document.cookie* ; </script>

Este código será reflejado por el servidor en respuesta al click del usuario, y el atacante conseguirá robar la cookie de sesión y enviarla a un dominio bajo su control.

- SQL Injection

Esta vulnerabilidad se produce cuando los datos no validados introducidos por el usuario se utilizan directamente dentro de la construcción de peticiones SQL. Con este tipo de vulnerabilidad se puede llegar a leer información sensible de la BBDD, modificarla (insertar, actualizar, borrar), ejecutar tareas administrativas (como apagar el gestor de BBDD), e incluso inyectar comandos al sistema operativo y conseguir una Shell remota. A continuación se puede observar un ejemplo de vulnerabilidad SQLi.

```
String query = "SELECT * FROM user_data WHERE last_name = '"
    + accountName + "'";
ec.addElement(new PRE(query));

try
{
Statement statement = connection.createStatement(
    ResultSet.TYPE_SCROLL_INSENSITIVE,
    ResultSet.CONCUR_READ_ONLY);
ResultSet results = statement.executeQuery(query);
```

Figura 57: Inyección SQL

Como podemos ver, el código construye una sentencia SQL introduciendo directamente el valor *accountName* dentro de la variable *query*, que es ejecutada directamente unas líneas más tarde. Al no existir validación alguna, un usuario malicioso podrá inyectar cualquier código que considere oportuno. Por ejemplo, usando *accountName = 'or '1'='1* se genera la siguiente petición que siempre se cumple:

*SELECT * FROM user_data WHERE last_name = '' or '1'='1'*

- Local File Inclusion (LFI)

Esta vulnerabilidad permite al atacante incluir en la respuesta un fichero del servidor web a través de algún script que no valide correctamente sus entradas. Por ejemplo, modificando el parámetro que recibe el script se podrían llegar a leer ficheros como /etc/passwd u otros ficheros de configuración del sistema, usando payloads como el siguiente:

/vulnerable.php?id=/etc/passwd%00

3.3.2 Escaneo de puertos

En esta prueba se ha comprobado si los UTM son capaces de detener un escaneo de puertos mediante Nmap. La etapa de escaneo de puertos, dentro del reconocimiento, es una de las etapas más importantes dentro del pentesting. En esta etapa el atacante puede identificar servicios que están a la escucha en un determinado host, y mediante técnicas de banner-grabbing y fingerprinting consistentes en analizar las respuestas del servidor, poder llegar a detectar versiones del software o incluso el sistema operativo que utiliza el servidor.

Cuantos más puertos abiertos encuentre un atacante mayor será su superficie de ataque, lo que aumenta su probabilidad de éxito. Hay que tener en cuenta que cuanta más información consiga extraer de las versiones instaladas y del sistema operativo utilizado, más podrá acotar su investigación y búsqueda de exploits, aumentando también notablemente su probabilidad de éxito [38].

3.3.3 Acceso a direcciones web maliciosas

Los filtros de contenidos son un tipo de mecanismo de seguridad que impide el acceso a determinadas categorías previamente seleccionadas de páginas web.

Los motivos detrás del bloqueo de contenidos pueden ser la protección de los menores, evitando su acceso a páginas de adultos o con cualquier tipo de contenido cuestionable, o en el caso de las empresas, se busca el cumplimiento de normativas y políticas de seguridad. Así, es factible pensar que un entorno corporativo se bloquee el acceso a pornografía por la normativa de uso y, que además, se impida el acceso a categorías de hacking que puedan introducir malware en la red, o a proxies web que puedan ayudar en la evasión de las propias políticas de seguridad corporativa.

Los filtros de contenido funcionan de diferentes formas, entre las que se encuentran:

- La consulta de bases de datos de URLs previamente analizadas e incluidas en categorías como: drogas, alcohol, armas, violencia, hacking, etc.
- Los filtros basados en reputación, que analizan diferentes aspectos de la página web como son la antigüedad, su localización y redes utilizadas, o el análisis de determinados parámetros de la propia web.

- La detección de palabras clave, tanto en la propia url como dentro del contenido de la página web, que previamente han sido escogidas y configuradas por el administrador.

- La detección de ficheros con extensiones peligrosas, como los ficheros .exe, .vbs, .bat, etc.

Los filtros de contenidos, además, pueden configurarse para permitir o denegar el acceso en función del origen, de la franja horaria y otros parámetros diferentes. Los más avanzados suelen estar actualizados a través de redes de inteligencia con actualizaciones muy frecuentes que impiden el acceso a páginas web en las que recientemente se han detectado infecciones, ataques de tipo phishing, u otro tipo de actividades maliciosas.

Una de las características más deseables en los filtros de contenidos es la capacidad de realizar inspección de tráfico HTTPs. Ya que este tráfico está cifrado, una solución incapaz de interceptar el contenido e inspeccionarlo no podrá aplicar las políticas de seguridad definidas y tendrá que dejar pasar los datos. Las soluciones que sí permiten inspección de tráfico generan certificados (válidos únicamente dentro de la organización) que deben ser exportados en los clientes, de tal forma que todo el tráfico cifrado se intercambia entre el cliente y la solución de seguridad, donde el tráfico se descifra y analizado, para posteriormente volver a cifrarlo y proceder a su envío al destino final.

Figura 58: Certificado emitido por la solución Sophos UTM

3.3.4 Descarga de software malicioso EICAR

En esta prueba se pretende comprobar la capacidad de análisis de software malicioso en protocolos no cifrados, siendo el escenario más común la descarga de ficheros maliciosos vía HTTP.

El EICAR Test [31] es un fichero considerado el estándar para la comprobación del correcto funcionamiento de los motores de detección de malware basados en firmas. Este fichero permite comprobar que el motor antivirus está activo sin peligro de infección, ya que se trata de un simple fichero de texto con una cadena de caracteres que es puesta en común con todos los fabricantes de soluciones malware. La cadena utilizada es la siguiente:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Figura 59: Cadena contenida en el fichero EICAR

La página web del Eicar Test permite el análisis de hasta 8 escenarios, cuatro de ellos con tráfico no cifrado, y cuatro de ellos con tráfico HTTPs y que requerirán de la capacidad de inspección de tráfico para poder ser bloqueados.

3.4 Ataques avanzados

En esta categoría se han incluido varios ataques que se han considerado como avanzados debido a que la dificultad para detectarlos y detenerlos es mayor, y a que requieren de mejores mecanismos tecnológicos. En esta categoría se incluyen escenarios que necesitan de inspección de tráfico cifrado, de la detección de muestras malware modificadas para la evasión del antivirus, y de la capacidad de evitar técnicas de evasión de los motores antivirus presentes en el UTM.

3.4.1 Descarga de software malicioso en protocolo cifrado

Los desarrolladores de malware están en una constante búsqueda de métodos de infección que puedan evadir los productos de seguridad. Las pasarelas de análisis de malware buscan dentro de los contenidos enviados a través del protocolo HTTP para detectar y eliminar el malware antes de que llegue al destino final dentro de la red. Sin embargo, no todas las pasarelas son capaces de analizar el tráfico cifrado. Por este mismo motivo, una de las técnicas utilizadas por los atacantes para ocultar su malware consiste en realizar las descargas desde servicios protegidos por SSL/TLS.

Como segundo escenario de descarga de software malicioso se propone analizar la capacidad de análisis través del protocolo HTTPs, que dificulta la tarea de detección a las soluciones de seguridad.

3.4.2 Descarga de software malicioso codificado

La detección de un malware conocido es una tarea relativamente sencilla, ya que el antivirus tan sólo tiene que comparar el fichero con su base de datos de firmas. En escenarios más avanzados los atacantes hacen uso de malware personalizado, ya sea mediante la creación de un nuevo malware, o mediante la modificación de muestras ya conocidas con técnicas de ofuscación. Veil Framework es una herramienta que, entre otras funciones, permite generar ficheros ejecutables maliciosos que puedan evadir los motores antivirus. Para esta prueba vamos a crear un payload malicioso usando esta herramienta y comprobaremos si el fichero es bloqueado por cada solución UTM.

3.4.3 Evasión

Como ya hemos mencionado, uno de los principales vectores de infección es la propia navegación web. Aunque habitualmente los usuarios descargan software de orígenes poco confiables e infectan sus ordenadores, cada vez es más frecuente que el usuario se vea afectado sin necesidad de que descargue manualmente un fichero malicioso. El simple hecho de utilizar navegadores o plugins desactualizados, como puedan ser Java o Flash, y llegar a una página maliciosa o que haya sido comprometida para redirigir al *landing-page* de un *exploit kit* puede suponer la infección del usuario.

A continuación se muestra un gráfico que detalla los pasos básicos de una infección mediante un exploit-kit genérico. Como podemos apreciar el usuario simplemente llega a una web comprometida, y es esta la que abre comunicaciones con el servidor del exploit-kit, en el que se analizan tanto el sistema operativo, como las versiones del navegador y plugins instalados en él. A continuación y con la información recopilada se lanzan automáticamente una batería de exploits que puedan afectar a las versiones detectadas del software instalado en el pc del usuario y se completa la infección.

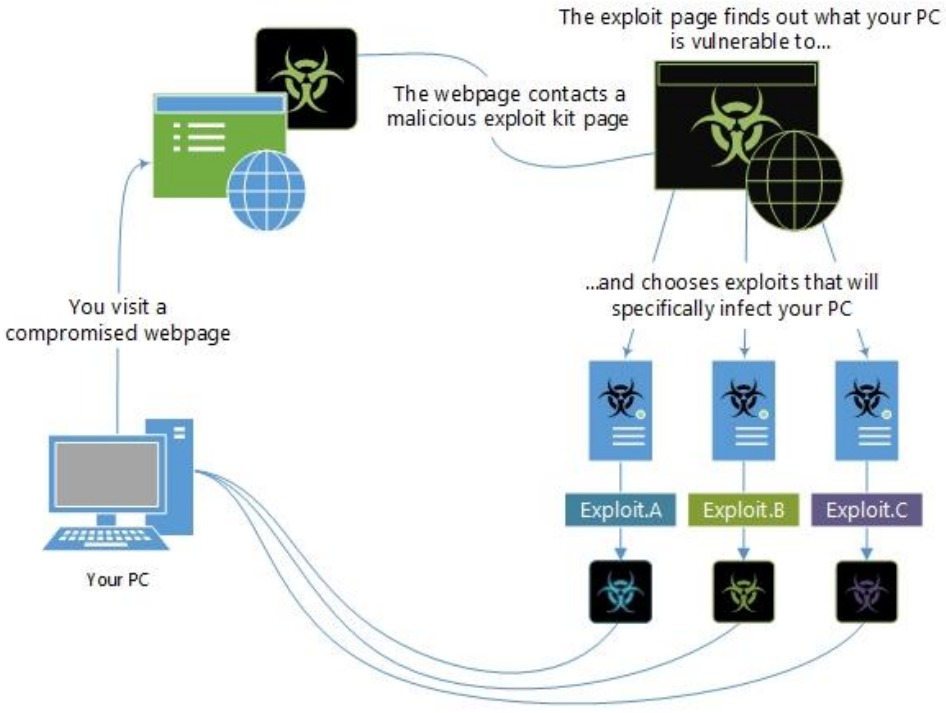


Figura 60: Gráfico de infección vía exploit-kit [33].

Debido a la facilidad con la que un usuario incauto puede acabar infectado a través de la navegación web, es imprescindible que el motor de análisis antivirus y tráfico web no sea fácil de evadir. De poco sirve tener firmas actualizadas si el motor es incapaz de extraer

adecuadamente el payload del tráfico http, y por tanto, se acaban analizando datos incorrectos y que nunca llevarán a una detección, aunque los datos transmitidos sean de hecho los de un fichero malicioso válido y ejecutable.

HTTP Evader es una herramienta que realiza un análisis automático de numerosas técnicas de evasión conocidas [30]. Entre ellas se usan respuestas inválidas pero que finalmente son interpretadas correctamente por el navegador, y otras respuestas válidas que son extrañas o raramente utilizadas por los servidores web. Frente a estas respuestas tanto el firewall como los distintos navegadores tienen un comportamiento diferente, por tanto, a pesar de que el Firewall decida dejar pasar la información como inofensiva, en ocasiones el navegador será capaz de reconstruir correctamente la petición y dará lugar a una transmisión correcta del fichero malicioso.

La prueba, en la que se intentan hasta un total de 651 tipos diferentes de evasión, se ha realizado con el navegador Firefox y los resultados obtenidos para cada uno de los productos analizados son:

Producto	Nº de Evasiones	Falsos Positivos
Sophos	43	0
Endian	18	0
Untangle	111	1

Figura 61: Posibilidades de evasión detectadas con HTTP Evader (menor es mejor)

Como podemos comprobar, el UTM que ha permitido un número mayor de evasiones ha sido Untangle, que además ha bloqueado una petición perfectamente legítima como si se tratase de una petición maliciosa. En cuanto a los otros dos productos, Endian obtiene los mejores resultados al permitir tan sólo 18 evasiones del total.

3.4.4 Control de protocolo

El puerto 80, dedicado a la navegación web http, es uno de los puertos que con más frecuencia se encuentra abierto en los firewalls corporativos. Por este motivo, el malware utiliza esta vía para extraer información evadiendo la seguridad perimetral [29], siendo uno de los mecanismos preferidos junto al uso de canal HTTPs o FTP [36].

En esta prueba se ha comprobado si las soluciones de seguridad bloquean el tráfico no estándar a través del puerto 80, una práctica que habitualmente se consigue a través de la utilización de servidores proxy [37].

4. Plan de pruebas y resultados

4.1 Objetivos y metodología

El objetivo de las pruebas ha sido comparar el rendimiento de cada una de las soluciones frente a los escenarios propuestos en el anterior apartado.

Como ya se ha mencionado anteriormente, una de las ventajas de los UTM es la existencia de un punto central de gestión de todas las funciones de seguridad que además están integradas en una única plataforma. Esto deriva en una mayor facilidad de uso, y en una menor necesidad de formación. Por este motivo, y ya que nos encontramos frente a soluciones gratuitas de uso ideal para entornos domésticos o de pequeñas oficinas, se ha valorado la facilidad de uso y configuración de dichas funcionalidades. Por ello, los pasos seguidos han sido el despliegue del producto como Gateway de seguridad en el mismo punto crítico de la red, la configuración de las comunicaciones para permitir los flujos de información, y la activación de los mecanismos de seguridad utilizando la política más restrictiva disponible a través de la interfaz web. Por ejemplo, ante la posibilidad de elegir uno o dos motores antivirus para la detección de malware, se escoge la segunda opción.

A continuación detallamos la metodología seguida y los resultados obtenidos para cada uno de los ataques propuestos en los apartados 3.3 y 3.4.

4.1.1 Servidor web protegido tras una solución UTM

La metodología seguida para la realización de esta prueba ha consistido, primero, en el lanzamiento de la herramienta Arachni contra la aplicación vulnerable en una conexión directa y sin existencia de medidas de protección. Una vez que se han registrado los fallos detectados por la herramienta en ausencia de medidas de seguridad, se ha repetido el mismo procedimiento para lanzar los ataques contra la aplicación web vulnerable, esta vez, forzando a que dichas peticiones pasen a través de cada una de las soluciones UTM.

Los resultados obtenidos tras usar Arachni contra Wavsep en una conexión directa y sin ningún mecanismo de protección son los siguientes:

Protección Básica				
	Urls Analizadas	Seguras	Inseguras	Vulnerabilidades
XSS	83	19	64	80
SQLi	143	11	132	214
LFI	831	627	204	228

Figura 62: Análisis realizado con Arachni contra wavsep sin solución de seguridad.

A continuación mostramos los resultados de los análisis realizados con la protección de Sophos UTM Home Edition. En el caso de Sophos, el servidor web queda protegido en el backend tras un Firewall de Aplicaciones (WAF) que analiza todas y cada una de las peticiones realizadas.

En el primer análisis automático la solución de seguridad ha conseguido impedir que la herramienta detecte cualquier tipo de vulnerabilidad. Lo que está sucediendo en este escenario es que el WAF ha detectado el *user-agent* utilizado por Arachni y bloquea directamente todas sus peticiones.

Sophos (User-agent por defecto)				
	Urls Analizadas	Seguras	Inseguras	Vulnerabilidades
XSS	1	1	0	0
SQLi	1	1	0	0
LFI	1	1	0	0

Figura 63: Análisis con Sophos y Arachni usando el user-agent por defecto

Teniendo acceso a los registros podemos observar la detección, mediante ModSecurity, del user-agent de Arachni:

2015:12:09-20:37:00 sophosutm reverseproxy: [Wed Dec 09 20:37:00.774411 2015] [security2:error] [pid 5968:tid 3929172848] [client 192.168.2.50] ModSecurity: Warning. **Matched phrase "arachni" at REQUEST_HEADERS:User-Agent**. [file "/usr/apache/conf/waf/modsecurity_crs_bad_robots.conf"] [line "20"] [id "990002"] [rev "2"] [msg "**Request Indicates a Security Scanner Scanned the Site**"] [data "**arachni/v1.3.2**"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.7"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "www.wavsep.com"] [uri "/wavsep/active/index-xss.jsp"] [unique_id "VmiC3MCoAmQAABdQHvoAAAAY"]

Este comportamiento aumenta la seguridad del entorno frente a ataques automatizados de agentes que, por falta de experiencia o por falta de acceso a los logs, no sean conscientes de que la herramienta está siendo bloqueada. Sin embargo, esta solución no es infalible.

El user-agent es una cabecera del protocolo HTTP, y los navegadores la envían como mecanismo de negociación de contenidos, de tal forma que el servidor pueda servir un contenido u otro en función de la información contenida en dicha cadena. Por ejemplo, si la cadena identifica un dispositivo Android, el servidor podrá servir la página en su versión personalizada para móviles, y si por el contrario la cadena identifica un dispositivo Windows 10 podrá servir la página web para ordenadores de escritorio. Alguno de los datos que un user-agent puede ofrecer son el tipo de navegador, su versión, o el sistema operativo utilizado por el usuario [39]. Sin embargo, esta cadena puede ser modificada de forma trivial, y es una función que incluso se encuentra presente en algunos navegadores.

Para evadir este mecanismo de seguridad ha sido necesario realizar el ataque modificando la cadena del user-agent que Arachni envía por defecto por la de un navegador de escritorio. Para ello se ha añadido el siguiente flag a los parámetros utilizados durante el ataque:

```
--http-user-agent "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0"
```

Una vez realizada esta modificación en el análisis comprobamos que los resultados obtenidos son los siguientes:

Con WAF + user-agent modificado				
	Urls Analizadas	Seguras	Inseguras	Vulnerabilidades
XSS	81	69	12	13
SQLi	143	143	0	0
LFI	830	788	42	42

Figura 64: Análisis con Sophos y Arachni enviando un user-agent alterado

Si comparamos con el análisis sin seguridad, el número de descubrimientos se ha reducido aproximadamente en un 84%, 100% y casi un 82% en las tres respectivas categorías analizadas.

En el caso de Untangle los resultados son muy parecidos a los obtenidos en ausencia de un producto de seguridad. Es decir, aparentemente la protección del servidor web vulnerable no ha aumentado significativamente.

Untangle				
Protección Básica				
	Urls Analizadas	Seguras	Inseguras	Vulnerabilidades
XSS	83	19	64	80
SQLi	143	11	132	194
LFI	831	627	204	228

Figura 65: Análisis con Untangle y Arachni

Existe una única categoría, la de inyecciones SQL, en la que la cifra se ha reducido frente al análisis inicial. En concreto, se ha pasado de 214 detecciones a 194, lo que supone un total de 20 detecciones menos. Sin embargo, accediendo a los logs de la herramienta se ha podido comprobar que dichas inyecciones no estaban siendo detectadas, y que si Arachni ha detectado menos vulnerabilidades ha sido por factores externos.

En concreto, dentro de las inyecciones SQL existe una categoría llamada *"Blind Sql Injection"* en las que el servidor web no devuelve mensajes de error para determinar si existe una vulnerabilidad, y por tanto el atacante debe decidir si existe o no un error de inyección "a ciegas" [40]. Habitualmente se hace uso de peticiones de tipo verdadero o falso para distinguir si existe una vulnerabilidad. Por ejemplo, supongamos que tenemos una web que devuelve una noticia:

```
http://newspaper.com/items.php?id=2
```

Sobre esa URL el atacante intentará realizar una inyección y comprobar el comportamiento del servidor, por ejemplo, introduciendo la siguiente sentencia.

```
http://newspaper.com/items.php?id=2 and 1=2
```

Esta petición debería devolver siempre falso, ya que 1 es distinto de 2, y por tanto no debería devolver la noticia. Si esto se confirma el atacante probará la siguiente posibilidad, que es inyectar una sentencia que siempre se cumpla.

http://newspaper.com/items.php?id=2 and 1=1

Si el servidor devuelve la noticia, afectado por la condición 1=1 que siempre se cumple, quiere decir que la inyección está funcionando y que el servidor web es vulnerable.

Por otro lado existe otra categoría de inyección basada en tiempo, y son las llamadas "*Time Based SQL Injections*". La idea es introducir de forma deliberada instrucciones que pausan la base de datos durante un tiempo determinado. La cantidad de tiempo debe ser suficientemente alta como para decidir que existe una vulnerabilidad y que el retardo no es debido a factores externos, como son la carga del servidor o la latencia en la red, pero a la vez debe ser lo suficientemente baja para no provocar interrupciones que puedan llamar la atención de un administrador. Este tipo de inyecciones es, lógicamente, muy sensible a la carga del servidor y a problemas de latencia. Dado que el laboratorio consiste en tres máquinas virtuales en un mismo ordenador, y debido a la inexistencia de mensajes en los registros, se puede afirmar que Arachni no ha conseguido detectar una serie de vulnerabilidades por factores externos y no debido a la seguridad del UTM.

Esta situación se puede explicar por la inexistencia de un WAF específico que trabaje en la capa de aplicación, y a que el módulo IPS está enfocado a la búsqueda de otro tipo de amenazas distintas a los ataques web, como son los ataques en la capa de red.

El comportamiento de Endian ha sido muy similar al de Untangle, aunque esta vez el número de detecciones ha sido idéntico al del análisis original. Por tanto, podemos afirmar que Endian tampoco ofrece una seguridad significativa de cara a proteger el servidor web.

Endian				
Protección Básica				
	Urls Analizadas	Seguras	Inseguras	Vulnerabilidades
XSS	83	19	64	80
SQLi	143	11	132	214
LFI	831	627	204	228

Figura 66: Análisis con Untangle y Arachni

4.1.2 Escaneo de puertos

Como ya reflejamos en la descripción de este escenario, durante esta prueba se hace uso de Metasploitable, una distribución Linux que viene con numerosos servicios vulnerables y abiertos a la red instalados por defecto.

Antes de comprobar la eficacia a la hora de detener un port-scanning de las tres soluciones de seguridad, se ha lanzado un primer análisis directo y sin productos de seguridad para anotar el número de puertos abiertos y las versiones detectadas. Posteriormente, se ha comparado esta información con los resultados obtenidos tras poner entre el servicio vulnerable y la máquina atacante el sistema de seguridad.

El tipo de escaneo utilizado ha sido el siguiente, del que a continuación se explica cada uno de los flags

```
nmap -sS -sV -PN -p 1-65535 -r -vv ipDestino -oN escaneoDirecto.txt
```

-sS: Escaneo de tipo SYN, que envía un paquete SYN como si fuese a abrir una conexión real, y que marca el puerto como abierto si recibe un SYN/ACK , como cerrado si recibe un RST, o como filtrado si después de varios intentos no recibe respuesta alguna o recibe un ICMP unreachable error.

-sV: Escaneo de servicio, intenta adivinar el servicio detrás de cada puerto abierto.

-PN: Forzar escaneo, no comprobar si el host responde a ping o no.

-p 1-65536: Comprobar todos los puertos del sistema

-r: Comprobar los puertos de forma consecutiva, sin randomizar. Útil de cara a la comparativa.

-vv: Aumenta el nivel de información mostrada por pantalla

ipDestino: la ip a escanear en la red

-oN escaneoDirecto.txt: Guardar salida en formato normal en el fichero “escaneoDirecto.txt”

Los resultados obtenidos han sido los siguientes:

Visibilidad sin seguridad			
Puerto	**Estado**	**Servicio**	**Versión**
21	Abierto	ftp	vsftpd 2.3.4
22	Abierto	Ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	Abierto	telnet	Linux telnetd
25	Abierto	Smtp	Postfix smtpd
53	Abierto	Domain	ISC BIND 9.4.2
80	Abierto	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	Abierto	Rpcbind	2 (RPC #100000)
139	Abierto	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445	Abierto	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
512	Abierto	Exec	netkit-rsh rexecd
513	Abierto	Login?	--
514	Abierto	Tcpwrapped	--
1099	Abierto	rmiregistry	GNU Classpath grmiregistry
1524	Abierto	Shell	Metasploitable root shell
2049	Abierto	Nfs	2-4 (RPC #100003)
2121	Abierto	ftp	ProFTPD 1.3.1
3306	Abierto	Mysql	MySQL 5.0.51a-3ubuntu5
3632	Abierto	Distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	Abierto	Postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	Abierto	Vnc	VNC (protocol 3.3)
6000	Abierto	X11	(access denied)
6667	Abierto	Irc	Unreal ircd
6697	Abierto	Irc	Unreal ircd
8009	Abierto	Ajp13	Apache Jserv (Protocol v1.3)
8180	Abierto	http	Apache Tomcat/Coyote JSP engine 1.1
8787	Abierto	Drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33409	Abierto	Status	1 (RPC #100024)
42566	Abierto	Mountd	1-3 (RPC #100005)
49035	Abierto	Unknown	--
57401	Abierto	nlockmgr	1-4 (RPC #100021)

Figura 67: Análisis de visibilidad sin solución de seguridad

Como podemos ver el número de puertos abiertos asciende a 30, y en numerosas ocasiones se obtiene información complementaria de la versión del servicio que se mantiene a la escucha. Esta información, como ya adelantábamos, permite al atacante acotar las posibilidades para dirigir su ataque con mayor precisión.

Visibilidad con Sophos			
Puerto	**Estado**	**Servicio**	**Versión**
80	Abierto	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443	Abierto	https?	--

Figura 68: Análisis de visibilidad con Sophos

En el caso del escenario con la protección de Sophos, nmap sólo ha detectado 2 puertos abiertos. El puerto para https (443) no se trata de un servicio real de Metasploitable, sino que aparece abierto por algún mecanismo del UTM. Si se intenta realizar una conexión a dicho puerto la conexión se cierra inmediatamente. El único puerto que queda visible es el puerto 80, y en general estaría protegido bajo la capa de seguridad del WAF. En cualquiera de los casos y cómo podemos observar, la superficie de ataque se ha visto muy reducida gracias al servicio de seguridad específico para evitar escaneos de puertos.

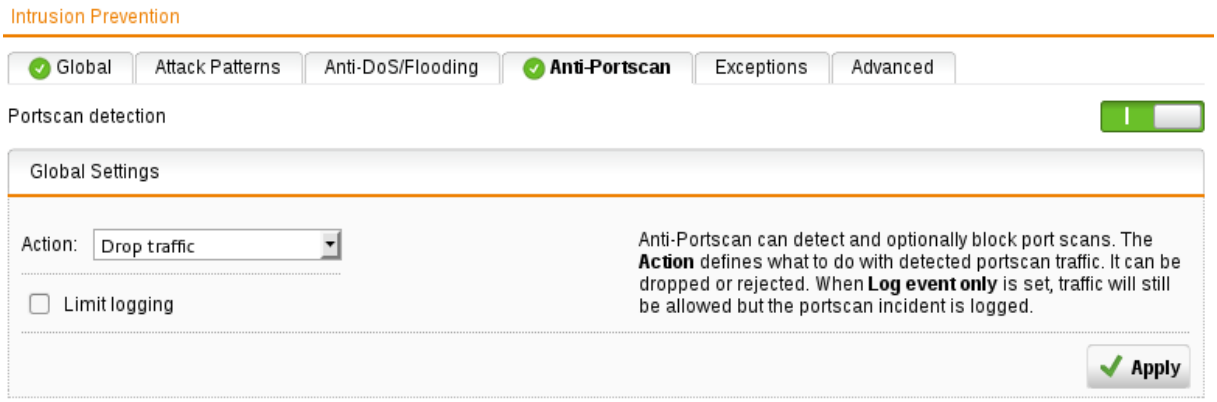


Figura 69: Sistema Anti-Portscan de Sophos.

Visibilidad con Endian			
Puerto	**Estado**	**Servicio**	**Versión**
21	Abierto	ftp	vsftpd 2.3.4
22	Abierto	Ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	Abierto	telnet	Linux telnetd
25	Abierto	Smtp	Postfix smtpd
53	Abierto	Domain	ISC BIND 9.4.2
80	Abierto	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111	Abierto	Rpcbind	2 (RPC #100000)
139	Abierto	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445	Abierto	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
512	Abierto	Exec	netkit-rsh rexecd
513	Abierto	Login?	--
514	Abierto	Tcpwrapped	--
1099	Abierto	rmiregistry	GNU Classpath grmiregistry
1524	Abierto	Shell	Metasploitable root shell
2049	Abierto	Nfs	2-4 (RPC #100003)
2121	Abierto	ftp	ProFTPD 1.3.1
3306	Abierto	Mysql	MySQL 5.0.51a-3ubuntu5
3632	Abierto	Distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	Abierto	Postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	Abierto	Vnc	VNC (protocol 3.3)
6000	Abierto	X11	(access denied)
6667	Abierto	Irc	Unreal ircd
6697	Abierto	Irc	Unreal ircd
8009	Abierto	Ajp13	Apache Jserv (Protocol v1.3)
8180	Abierto	http	Apache Tomcat/Coyote JSP engine 1.1
8787	Abierto	Drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35792	Abierto	Mountd	(RPC #100005)
45000	Abierto	Unknown	--
57655	Abierto	Status	(RPC #100024)
60826	Abierto	nlockmgr	1-4 (RPC #100021)

Figura 70: Análisis de visibilidad con Endian

El UTM de Endian ha permitido que nmap detecte los 30 puertos abiertos y sus correspondientes versiones, por lo que la seguridad no se ha visto incrementada gracias al UTM.

Visibilidad con Untangle			
Puerto	**Estado**	**Servicio**	**Versión**
21	Abierto	ftp	vsftpd 2.3.4
22	Abierto	Ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	Abierto	telnet	--

25	Abierto	Smtp	--
53	Abierto	Domain	--
80	Abierto	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	Abierto	Rpcbind	--
139	Abierto	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
161	Filtrado	Snmp	--
162	Filtrado	Snmptrap	--
705	Filtrado	Agentx	--
1080	Filtrado	Socks	--
3128	Filtrado	Squid-http	--
3632	Abierto	Tcpwrapped	--
5900	Abierto	Vnc	VNC (protocol 3.3)
6000	Abierto	X11	(access denied)
8080	Filtrado	http-proxy	--
8180	Abierto	tcpwrapped	--
8787	Abierto	tcpwrapped	--
15104	Filtrado	unknown	--

Figura 71: Análisis de visibilidad con Untangle

En el caso de Untangle se han detectado 13 puertos abiertos, consiguiendo reducir casi en tres partes la visibilidad de servicios vulnerables expuestos. Se puede observar que para numerosos servicios aparece el estado filtrado. Esto significa que nmap es incapaz de distinguir si el puerto está abierto o cerrado [34], probablemente, porque el filtro de paquetes de Untangle está descartándolos e impidiendo que lleguen a su destino.

4.1.3 Acceso a direcciones web maliciosas

En esta prueba se pretende comprobar la eficacia del filtro de contenidos. Para ello se ha bloqueado el acceso a una categoría sensible, como es la de proxies y navegación anónima, y se ha procedido a intentar acceder a cuatro páginas que presumiblemente deberían estar bloqueadas para así comprobar los resultados.

Durante las pruebas se ha intentado conectar a la página web en texto claro, así como en su versión cifrada mediante HTTPs. Para la inspección de tráfico HTTPs en las soluciones que dispongan de esta característica, se ha importado el certificado generado por la solución UTM en el navegador de usuario, para así evitar los mensajes de error de

certificados autofirmados. Las cuatro muestras utilizadas y los resultados obtenidos son los siguientes:

Muestra 1 – http://www.kproxy.com/ y https://www.kproxy.com/

Muestra 2 – http://www.proxysite.com/ y https://www.proxysite.com/

Muestra 3 – https//www.proxfree.com/ y https://www.proxfree.com/

Muestra 4 – http://www.hidemyass.com/ y https://www.hidemyass.com/

	Sophos		Untangle		Endian	
	HTTP	HTTPs	HTTP	HTTPs	HTTP	HTTPs
Muestra 1	Bloqueada	Bloqueada	Bloqueada	No Bloq.	Bloqueada	Bloqueada
Muestra 2	Bloqueada	Bloqueada	No bloq.	No Bloq.	Bloqueada	Bloqueada.
Muestra 3	Bloqueada	Bloqueada	Bloqueada	No Bloq.	Bloqueada	Bloqueada
Muestra 4	Bloqueada	Bloqueada	Bloqueada	No Bloq.	Bloqueada	Bloqueada

Figura 72: Accesos vía HTTP y HTTPs a categorías no permitidas por política de accesos.

Como podemos ver la solución de Sophos bloquea las cuatro muestras, tanto para tráfico HTTP como para tráfico HTTPs. Este mismo comportamiento es el ofrecido por Endian, que como Sophos tiene capacidad de inspección de tráfico cifrado. Sin embargo, en el caso de Untangle la inspección de tráfico https no está habilitada en la licencia gratuita, lo que ha permitido el acceso a las cuatro muestras cuando se hace uso del protocolo HTTPs. Además, la redirección automática de HTTP a HTTPs que se produce en la muestra 2 hace que el tráfico no sea bloqueado y el usuario pueda acceder al contenido. En el Anexo I se muestran las capturas de pantalla realizadas durante el estudio.

4.1.4 Descarga de software malicioso

En esta prueba se ha realizado la descarga de los cuatro escenarios no cifrados del EICAR test, consistentes en la descarga de:

1. Fichero con extensión .com
2. Fichero renombrado y con extensión .txt
3. Fichero comprimido en .zip
4. El anterior fichero, comprimido de nuevo en otro fichero .zip.

El primer escenario es el básico, en el que no sólo se transmite la firma de un malware sino que además se usa una extensión potencialmente maliciosa. El segundo escenario pretende comprobar si el cambio de nombre y extensión es suficiente para evadir el

antivirus. El tercero sirve para comprobar si el motor antivirus es capaz de analizar ficheros comprimidos. El último y más complejo de todos ellos, pretende comprobar si el antivirus es capaz de descomprimir ficheros de más de un nivel de profundidad, como el caso de un fichero .zip comprimido dentro de otro.

- El UTM de Sophos permite analizar los ficheros con hasta dos motores antivirus, Sophos y Avira. Para las pruebas ha sido configurado el análisis con ambos motores.
- El UTM de Untangle protege del malware a través del módulo Virus Blocker, basado en el motor de análisis del antivirus BitDefender.
- Finalmente, Endian hace uso del motor software libre ClamAV.

	Sophos	Untangle	Endian
Muestra 1	Bloqueado	Bloqueado	Bloqueado
Muestra 2	Bloqueado	Bloqueado	Bloqueado
Muestra 3	Bloqueado	Bloqueado	Bloqueado
Muestra 4	Bloqueado	Bloqueado	Bloqueado

Figura 73: Tabla de detección del Eicar Test en descargas HTTP

Como podemos observar, todas las muestras han sido bloqueadas. En el Anexo II se adjuntan las capturas de pantalla de Untangle bloqueando el fichero Eicar.

4.1.5 Descarga de software malicioso en protocolo cifrado

Para hacer las comprobaciones se ha vuelto a utilizar el estándar EICAR Test, esta vez haciendo uso de las descargas a través de direcciones HTTPs.

En este caso, la solución de seguridad debería disponer de capacidad de inspección de tráfico cifrado, de lo contrario no podrá detectar las muestras de malware. Tanto Sophos como Endian permiten la inspección de tráfico en su versión gratuita, no así Untangle, que necesita de una licencia de pago para activar esta característica. Los resultados obtenidos han sido los siguientes:

	Sophos	Untangle	Endian
Muestra 1	Bloqueado	Descargado	Bloqueado
Muestra 2	Bloqueado	Descargado	Bloqueado
Muestra 3	Bloqueado	Descargado	Bloqueado
Muestra 4	Bloqueado	Descargado	Bloqueado

Figura 74: Tabla de detección del Eicar Test en descargas HTTPs

Como podemos apreciar, los resultados obtenidos son los esperados. Ya que Untangle no permite inspección de tráfico cifrado en su licencia gratuita, las cuatro muestras han evadido la protección y por tanto han conseguido entrar al perímetro que se pretendía proteger. Por su parte, tanto Sophos como Endian han bloqueado las muestras de forma efectiva. En el Anexo III se muestran las capturas de pantalla de Endian bloqueando el fichero Eicar Test a través de HTTPs. Dado que Sophos ha bloqueado todas las muestras, para dicha solución sólo se mostrarán las capturas de pantalla relacionadas con la siguiente prueba.

4.1.6 Descarga de software malicioso codificado

Como ya avanzamos, para realizar esta prueba se va a generar un ejecutable malicioso que ha sido generado a través de Veil Framework, una herramienta capaz de reducir la probabilidad de detección de las muestras generadas

En concreto vamos a generar un ejecutable que tiene como payload un meterpreter que realiza una conexión inversa mediante HTTP. Meterpreter es un intérprete de comandos que permite interactuar con un sistema vulnerado a través de Metasploit.

Una vez generado el fichero se alojará en un servidor web al que se intentará acceder a través de los distintos UTM. Esta descarga se servirá a través de protocolo no cifrado HTTP para que los tres productos tengan la posibilidad de detectar la muestra a través de sus motores antivirus. Si el fichero es descargado la prueba habrá fallado, y por tanto, se entenderá que el fichero malicioso ha entrado hasta el perímetro protegido.

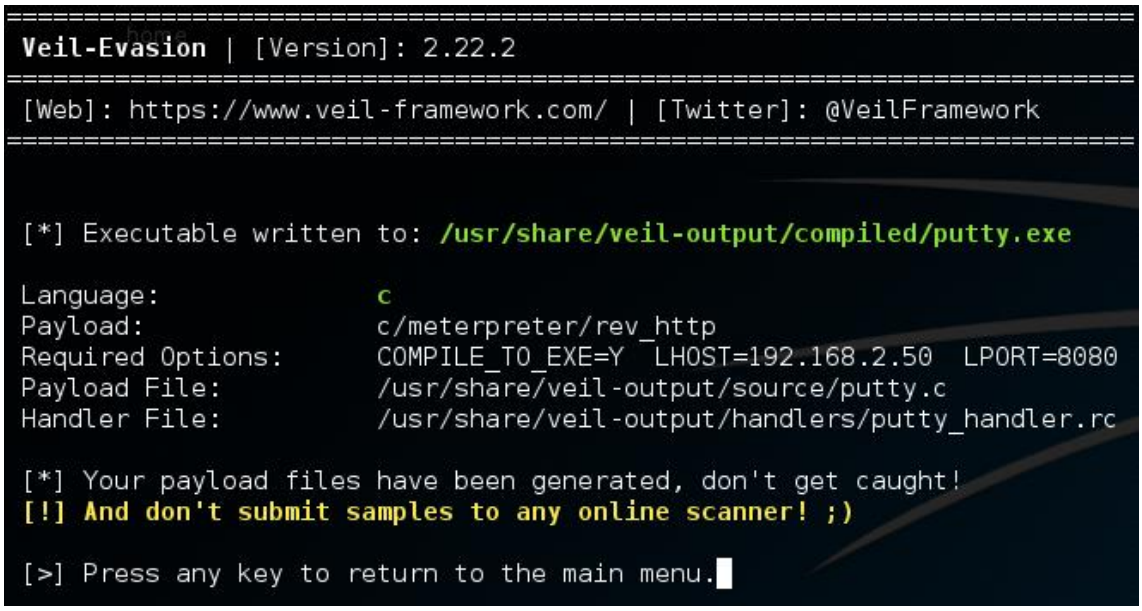


Figura 75: Creando un Meterpreter inverso HTTP mediante Veil Framework

Los resultados obtenidos durante la prueba han sido los siguientes:

Sophos	Untangle	Endian
Bloqueado	No Bloqueado	No Bloqueado

Figura 76: Detección del fichero codificado por los motores antivirus de los UTM

En este escenario la única solución capaz de detener la infección ha sido Sophos. Tanto Untangle como Endian han dejado pasar la muestra sin detectar ninguna anomalía. En el caso de Sophos, la solución no detecta un malware específico, sino que informa de una categoría genérica relacionada con comportamientos maliciosos llamada "*CXweb/OddDld-A*", y que podría llegar a generar falsos positivos. En este caso, ha sido capaz de proteger al usuario que realizaba la descarga.

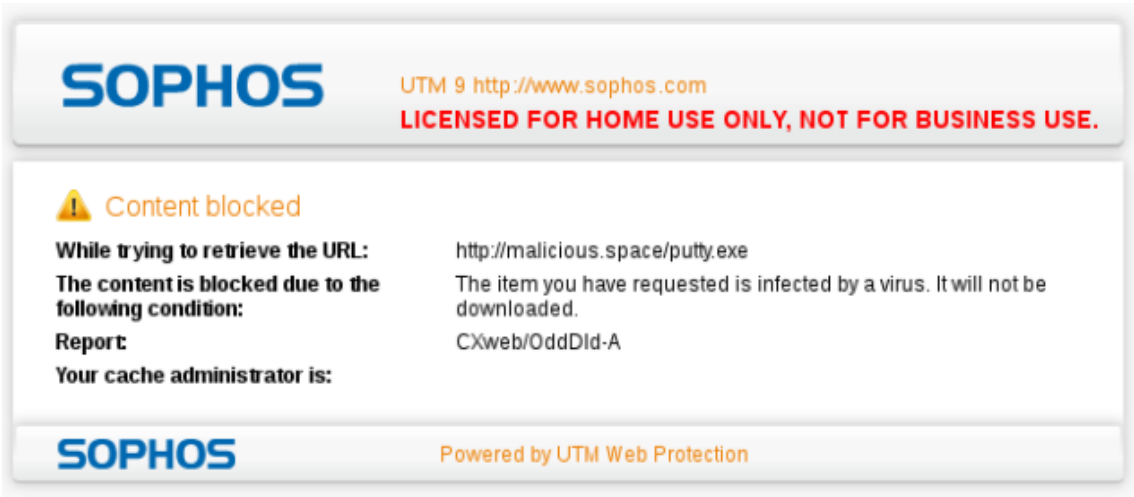


Figura 77: Sophos bloquea el fichero generado con Veil Framework.

4.1.7 Evasión

En esta prueba se hace uso de HTTP Evader para probar hasta 615 mecanismos de evasión para la transmisión de contenido malicioso. Como se indicó anteriormente, esta herramienta se aprovecha de la diferencia de comportamiento entre el firewall y el navegador al recibir datos de un servidor, consiguiendo que el navegador finalmente construya una petición con datos maliciosos que, de cara al firewall, no tenía una carga maliciosa. Esta prueba, por tanto, depende del navegador utilizado ya que no todos los navegadores se comportan igual ante las respuestas de un servidor. Esta herramienta también utiliza el fichero EICAR test como carga maliciosa que debería ser detectada por las soluciones de seguridad.

Para las pruebas se ha hecho uso del navegador Firefox y los resultados obtenidos para cada uno de los productos analizados son los siguientes:

Producto	Nº de Evasiones	Falsos Positivos
Sophos	43	0
Endian	18	0
Untangle	111	1

Figura 78: Posibilidades de evasión detectadas con HTTP Evader (menor es mejor)

Como podemos comprobar, el UTM que ha permitido un mayor número de evasiones ha sido Untangle, que además ha bloqueado una petición perfectamente legítima como si se tratase de una petición maliciosa. En cuanto a los otros dos productos, Endian obtiene los mejores resultados al permitir tan sólo 18 evasiones del total. En el Anexo IV se muestran los resultados de HTTP Evader para cada una de las soluciones.

4.1.8 Control de Protocolo

Para la realización de esta prueba se ha levantado un servidor escuchando en el puerto 80 mediante el uso de *netcat*, y se ha intentado enviar información conectando con un cliente netcat que envía datos no http. Para comprobar el correcto funcionamiento de la conexión, previamente se ha intercambiado una petición http válida que nos permita verificar que el canal permite el intercambio de datos válidos.

Los comandos utilizados en netcat son:

- Para levantar el servidor
  - netcat –lvp 80
- Para enviar la petición http válida se ha enviado mediante un pipe el contenido del fichero *peticionValida* hasta el servidor remoto:
  - cat peticionValida | nc 192.168.3.50 80

  El contenido de peticionValida se puede comprobar en el Anexo V.
- Para enviar datos no http simplemente se ha conectado al servidor y de forma interactiva se han mandado datos que no se corresponden con el formato de una conexión http.
  - nc 192.168.3.50 80

	Tráfico HTTP transmitido	Tráfico no estándar enviado
Sophos	Sí	No
Untangle	Sí	Sí
Endian	Sí	No

Figura 79: Detección de tráfico no estándar en puerto 80

Como podemos ver, el tráfico válido ha sido enviado en todas las situaciones, permitiendo verificar que la conexión estaba siendo correctamente establecida. En cuanto al tráfico no estándar, tanto Sophos como Endian han conseguido bloquear el tráfico de forma automática y sin necesidad de realizar ningún tipo de configuración manual. Esto se consigue, en ambos casos, mediante la existencia de un proxy http que comprueba que las conexiones realizadas a través del puerto 80 sean válidas.

En el caso de Sophos, cualquier tipo de tráfico no http provoca el cierre inmediato de la conexión sin que estos datos lleguen a su destino.

Figura 80: Cierre de conexión ante tráfico no http

Por su parte, Endian usa Squid para devolver al cliente un mensaje de error *400 Bad Request*, que indica que la petición no pudo ser entendida por la presencia de sintaxis incorrecta, y que el cliente no debe volver a intentar esa misma petición sin modificarla previamente [35].

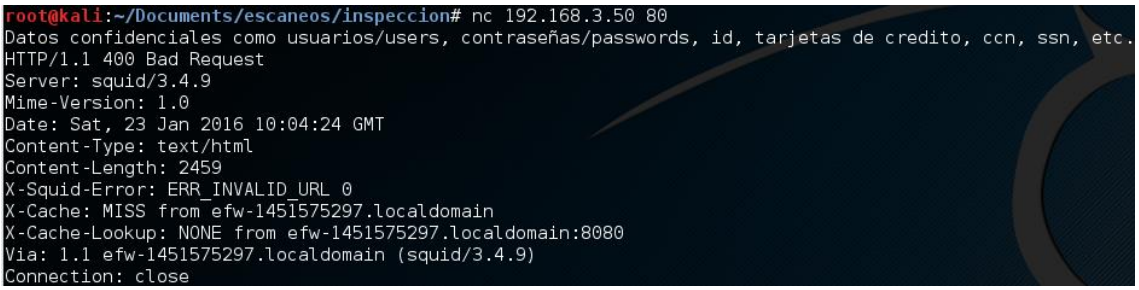


Figura 81: 404 Bad Request devuelto por el proxy Squid de Endian

Como adelantábamos, Untangle es el único producto que no pasa las peticiones HTTP a través de un proxy y que por tanto, permite enviar cualquier tipo de información a través de ese canal.

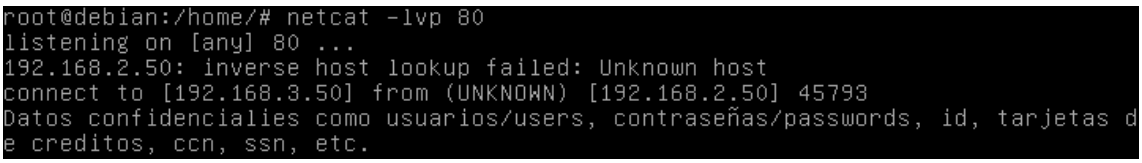


Figura 82: Untangle no impide que el servidor reciba datos no estándar a través del puerto 80

5. Conclusiones y trabajos futuros

El objetivo de este estudio ha sido analizar la seguridad ofrecida por diferentes soluciones UTM de libre acceso. Frente a la dificultad de acceder a soluciones comerciales avanzadas, ofrecidas por fabricantes como Bluecoat o McAfee, se ha propuesto comprobar las capacidades de protección que perfiles como el de un usuario doméstico, un entusiasta de la seguridad, o una pequeña empresa pueden llegar a alcanzar usando estos productos gratuitos. Para ello se han escogido tres soluciones UTM que cumplen estas características: Sophos UTM Home Edition, Endian Firewall Community y Untangle NG Firewall, y se han creado una serie de escenarios de amenazas mediante el uso de máquinas virtuales en los que comprobar la eficacia de dichas soluciones. Estos escenarios han intentado reflejar un conjunto de las amenazas más frecuentes hoy en día, como son los ataques vía web, la descarga de malware, o los intentos de atacar un servidor web vulnerable.

Tras el análisis de todas las soluciones podemos extraer diferentes conclusiones.

Si nos centramos en el número de características ofrecidas por cada solución, el producto de Sophos es el que ofrece un conjunto mayor de posibilidades. El hecho de que se trate de un producto comercial que es válido incluso para grandes empresas, pero que permite su uso gratuito en entornos domésticos, hace posible prácticamente cualquier tipo de configuración. Endian y un Untangle ofrecen un conjunto de características muy similar entre ellos, aunque inferior al de Sophos, y teniendo Untangle la ventaja de permitir contratar e instalar cada una de las funciones existentes de forma modular. Esto permite personalizar la solución de seguridad y ahorrar espacio en disco, mientras que en las otras soluciones esta característica no es posible y debemos limitarnos a desactivar cualquier función no necesaria.

Desde el punto de vista de las pruebas realizadas también podemos afirmar que la solución que mejores resultados ha ofrecido ha sido la de Sophos. De nuevo debemos reconocer que estamos enfrentando una solución que, de forma gratuita, permite el acceso al catálogo completo de funcionalidades y actualizaciones presentes en su versión comercial. Esta es una ventaja competitiva clara para el usuario doméstico, que tiene al alcance de su mano un producto de calidad empresarial y perfectamente actualizado sin necesidad de hacer ninguna inversión económica. Por su parte, tanto Endian como Untangle permiten acceder durante un tiempo de prueba al catálogo completo de funciones, pero una vez terminada la prueba se debe decidir si adquirir el producto de pago o usar la licencia

gratuita con las funcionalidades limitadas. Esto puede ser útil de cara a decidir si queremos la versión comercial o no, pero no es válido si lo que queremos es mantener la solución de forma continuada en el tiempo.

De las ocho pruebas realizadas, en siete de ellas Sophos ha ofrecido igual o mejor rendimiento que sus alternativas. Por su parte, Endian ha sido la que mejor rendimiento ha ofrecido en la prueba de evasión, siendo la que ha permitido el menor número posible de evasiones al servidor de HTTP Evader. Untangle tan sólo ha podido alcanzar el mismo rendimiento que sus alternativas en el análisis del Eicar Test en protocolo no cifrado, ofreciendo peores resultados en todas las pruebas restantes.

	Sophos	Untangle	Endian
Prueba 1	Ganador	-	-
Prueba 2	Ganador	-	-
Prueba 3	Empate	-	Empate
Prueba 4	Empate	Empate	Empate
Prueba 5	Empate	-	Empate
Prueba 6	Ganador	-	-
Prueba 7	-	-	Ganador
Prueba 8	Empate	-	Empate

Figura 83: Resumen de resultados de las pruebas

El motivo por el que Untangle se ha visto tan penalizado es la ausencia de capacidad de inspección de tráfico cifrado en la licencia gratuita. Esta característica, que las otras dos soluciones ofrecen en sus versiones gratuitas, es indispensable para proteger el perímetro de la red frente a ataques avanzados. Sin capacidad de inspeccionar el tráfico cifrado una gran parte de las amenazas pueden pasar desapercibidas, y como ya hemos mencionado en el estudio, esta es una realidad de la que los atacantes son muy conscientes y de la que se aprovechan frecuentemente.

Finalmente y desde el punto de vista del licenciamiento hay que tener muy en cuenta que Sophos no permite el uso comercial gratuito de su solución. Por tanto y si lo que se busca es disfrutar de un entorno doméstico seguro, esta solución parece la mejor alternativa, sin embargo, si se pretende proteger el perímetro de un entorno comercial de forma gratuita, deberemos elegir entre la solución de Endian y Untangle.

	Sophos	Untangle	Endian
Uso comercial con licencia gratuita	No permitido	Permitido	Permitido

Figura 84: Licenciamiento de las soluciones UTM

Debido al menor número de evasiones permitidas por Endian y a su capacidad de inspección de tráfico HTTPs, esta podría ser la mejor opción.

Como ya se mencionó en el *Contexto del Trabajo*, se debe tener en cuenta que el uso de licencias gratuitas en entornos comerciales no está recomendado por los fabricantes. Esta situación se podría considerar una solución temporal de compromiso ante la ausencia de presupuesto de seguridad, o como piloto de pruebas antes de la adquisición de un producto, debido a que la ausencia de soporte y actualizaciones frecuentes hacen que esta no sea una solución final recomendable para un entorno de producción.

Dentro de las amenazas más frecuentes en Internet se han analizado, principalmente, amenazas relacionadas con la web y el malware. Queda para el análisis en futuros estudios la capacidad de detección y filtrado de correo electrónico malicioso, otra de las grandes amenazas de la red. Asimismo y dada la continua aparición de nuevas amenazas, se propone continuar actualizando el estudio ante la aparición de nuevos métodos de ataque y evasión, y de las correspondientes tecnologías que sirvan para su mitigación.

6. Referencias

1. IDC (September 2007). Unified Threat Management Appliances and Identity-based Security: The Next Level in Network Security. IDC Go-to Market Services. Recuperado el 21/10/2015 de: http://www.cyberoam.com/downloads/IDC/VendorSpotlight.pdf

2. Firstbrook, P., Orans, L., Hallawell, A. (4 June 2007). Magic Quadrant for Secure Web Gateway, 2007. Gartner Inc. 1-28. Recuperado el 21/10/2015 de: http://www.utilitas.hr/Pdf/Gartner_bluecoat_2327%5B1%5D.pdf

3. Cyberoam (2015). Cyberoam's Layer 8 Technology: Protecting the weakest link in your security chain – the USER! (Cyberoam – Sophos). Recuperado el 23/10/2015 de: www.cyberoam.com/downloads/Whitepaper/CyberoamLayer8Technology.pdf

4. Author Unknown. (2009). Definitions –Unified Threat Management. Search Security (Tech Target). Recuperado el 21/10/2015 de: http://searchsecurity.techtarget.com/dictionary/definition/what-is-unified-threat-management.html

5. Chirasota, Jena. (2008). SMBs Driving the Indian UTM Market. First Post Business. Recuperado el 21/10/2015 de: http://tech2.in.com/biz/india/features/security/smbs-driving-the-indian-utm-market/19851/0

6. Jacob, John. (2009). *The Rise of Integrated Security Appliances*. Channel Business. Recuperado el 21/10/2015 de: http://www.channelbusiness.in/index.php?Itemid=83&id=252&option=com_content&task=view

7. Joel M. Snyder. (2007). Unified Threat Management. Opus One. 6–24. Recuperado el 21/10/2015 de: http://www.opus1.com/www/presentations/smartdefense-UTM.pdf

8. FireEye. (2015). Spear Phising Attacks – Why They are Successful and How to Stop Them: Combating the Attack of Choice for Cybercriminals. Recuperado el 22/10/2015 de: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

9. Bright, Peter. (Apr 4, 2011). Spearphishing + zero-day: RSA hack not “extremely sophisticated”. Arstechnica. Recuperado el 22/10/2015 de: http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/

10. Hong, Jason. (Jan 2012). The State of Phishing Attacks. Communications of the ACM, Vol. 55 No. 1, 74-81. Recuperado el 22/10/2015 de: http://cacm.acm.org/magazines/2012/1/144811-the-state-of-phishing-attacks/fulltext

11. Infosec Institute. (May 5, 2015). Introduction: Spear phishing attacks. Infosec Institute. Recuperado el 22/10/2015 de: http://resources.infosecinstitute.com/spearphishing-a-new-weapon-in-cyber-terrorism/

12. O’gorman, G., McDonald, G. (2012). The Elderwood Project. Symantec Security Response. Recuperado el 12/01/2016 de: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

13. Bluecoat. (May 21, 2015). The Cost of Hacking. Bluecoat Blog. Recuperado el 20/12/2015 de: https://www.bluecoat.com/es/company-blog/2015-05-21/cost-hacking

14. Widmer, Lori. (Jun 18, 2015). The 10 most expensive data breaches: Insurers must prepare. Recuperado el 20/12/2015 de: http://www.lifehealthpro.com/2015/06/18/the-10-most-expensive-data-breaches?page=5

15. J. Schwartz, Mathew. (Apr 11, 2011). Epsilon Fell to Spear-Phising Attack. Dark Reading (InformationWeek). Recuperado el 20/12/2015 de: http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119?

16. Roman, Czaroma. (May 2, 2011). Total Cost of Epsilon E-Mail Dat Breach Could Reach $4 Billion. CloudTimes. Recuperado el 20/12/2015 de: http://cloudtimes.org/2011/05/02/total-cost-of-epsilon-e-mail-data-breach-could-reach-4-billion/

17. McAfee. (2015). McAfee Network Security Platform (Intel Security). Recuperado el 21/10/2015 de: http://www.mcafee.com/us/resources/data-sheets/ds-network-security-platform-ns-series.pdf

18. Rodriguez, Chris. (June 3, 2010). The Future of the Firewall Market: New Technology or Convergence? (Frost & Sullivan). Recuperado el 20/10/2015 de: http://www.slideshare.net/FrostandSullivan/the-future-of-the-firewall-market-new-technology-or-convergence

19. Sophos. (Nov, 2015). Acuerdo de licencia del usuario final de Sophos. Recuperado el 13/01/2015 de: https://www.sophos.com/en-us/medialibrary/PDFs/legal/sophoseulaesp.pdf

20. Ramos Fraile, Alejandro (Feb, 2011). Seguridad Perimetral (Intypedia: Information Security Encyclopedia). Recuperado el 23/10/2015 de: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

21. Scarfone, K., Mell, P. (Febrero 2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST). Recuperado el 23/10/2015 de: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

22. Bermejo, Javier. (2015). Apuntes asignatura “Análisis de Malware”, Máster Seguridad Informática (UNIR).

23. Bilogorskiy, N., Sharma, S. (2015). Anti-sandbox Malware Tricks (Cyphort). Recuperado el 18/01/2016 de: http://www.slideshare.net/Cyphort/mmw-antisandbox-techniques

24. Ortega, Alberto (2015). Pafish (Github): https://github.com/a0rtega/pafish/blob/master/CHANGELOG

25. Sophos (2015). Sophos UTM Feature List (Sophos). Recuperado el 23/10/2015 de: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-utm-feature-list-dsna.pdf

26. Untangle (2015). Individual Applications: NG Firewall. Recuperado el 23/10/2015 de: https://www.untangle.com/untangle-ng-firewall/applications/

27. Endian (2016). Home Vs Professional | Endian Firewall Community vs Endian UTM. Recuperado el 20/01/2016 de: http://www.endian.com/community/comparison/

28. Endian (2016). Open Source Firewall Features | Endian Firewall Community. Recuperado el 20/01/2016 de: http://www.endian.com/community/features/

29. TrendLabs (2013). Data exfiltration: How do threat actors steal your data? (TrendMicro). Extraído el 20/01/2016 de: http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf

30. Ullrich, Steffen (2014). Hiding malware in plain sight from online scanners. (Noxxi.de). Recuperado el 20/10/2015 de: http://noxxi.de/research/content-encoding-online-scanner.html

31. European Institute for Computer Anti-Virus Research. (2016). Antimalware Test File: Intended Use. Recuperado el 23/10/2015 de: http://www.eicar.org/86-0-Intended-use.html

32. Bluecoat (2015). Blue Coat Director Datasheet: Provide centralized configuration and policy management. (Bluecoat). Recuperado el 21/01/2016 de: https://www.bluecoat.com/documents/download/dd63dbd2-0393-4098-9acc-56ec10f46891/40bd54f3-63ac-4b32-bf30-e80edc83fe17

33. Microsoft (2015). The exploit malware family (Malware Protection Center). Recuperado el 20/10/2015 de: https://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx

34. Nmap.org (2015). Nmap Network Scanning. Port Scanning Basics, Chapter 15. Nmap Reference Guide. Recuperado el 20/10/2016 de: https://nmap.org/book/man-port-scanning-basics.html

35. World Wide Web Consortium (2015). RFC2626-Sec10: Status Code Definitions. (W3c). Recuperado el 21/01/2016 de: https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

36. Security Lancaster (2015). Detecting and Preventing Data Exfiltration (Lancaster University). Pg.7. Recuperado el 23/01/2016 de: https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf

37. Security Lancaster (2015). Detecting and Preventing Data Exfiltration (Lancaster University). Pg.12. Recuperado el 23/01/2016 de: https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf

38. McClure, S. et al (2005). Hacking Exposed (McGraw-Hill/Osborne).

39. World Wide Web Consortium (2016). RFC 7231: HTTP/1.1 Semantics and Content. 5.5.3: User-agent. (W3C). Recuperado el 24/01/2016 de: https://tools.ietf.org/html/rfc7231#page-46

40. Owasp (2015). Blind SQL Injection (Owasp.org). Recuperado el 24/01/2016 de: https://www.owasp.org/index.php/Blind_SQL_Injection

41. Malwarebytes Labs (2015). What is malvertising? (Malwerbytes.org). Recuperado el 25/01/2016 de: https://blog.malwarebytes.org/malvertising-2/2015/02/what-is-malvertising/

42. Fey, Michael (Apr, 2012). McAfee Vision (McAfee). Recuperado el 22/10/2015 de: http://www.slideshare.net/FedScoop/mcafee-vision

43. Bluecoat (May, 2014). Blue Coat Malware Analysis Appliance v4.11 Web User Guide (Bluecoat.org). Recuperado el 23/10/2015 de: https://bto.bluecoat.com/sites/default/files/tech_pubs/MAA_4.1.1_Web_User_Guide.pdf

44. McAfee (2015). Dos, DDoS Protection (McAfee.org). Recuperado el 25/20/2015 de: http://www.mcafee.com/es/resources/demos/nsp-demo-dos-ddos.html

45. Council of the European Union (Dec, 2015). Improving cyber security across the EU. (Europa.eu). Recuperado el 27/01/2016 de: http://www.consilium.europa.eu/en/policies/cyber-security/

46. European Comission (Mar, 2015). Digital Agenda for Europe: Network and Information Security (NIS) Directive. (Europa.eu). Recuperado el 27/01/2016 de: https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

7. Anexos

7.1 Anexo I – Capturas de pantalla de bloqueo web en HTTP y HTTPs

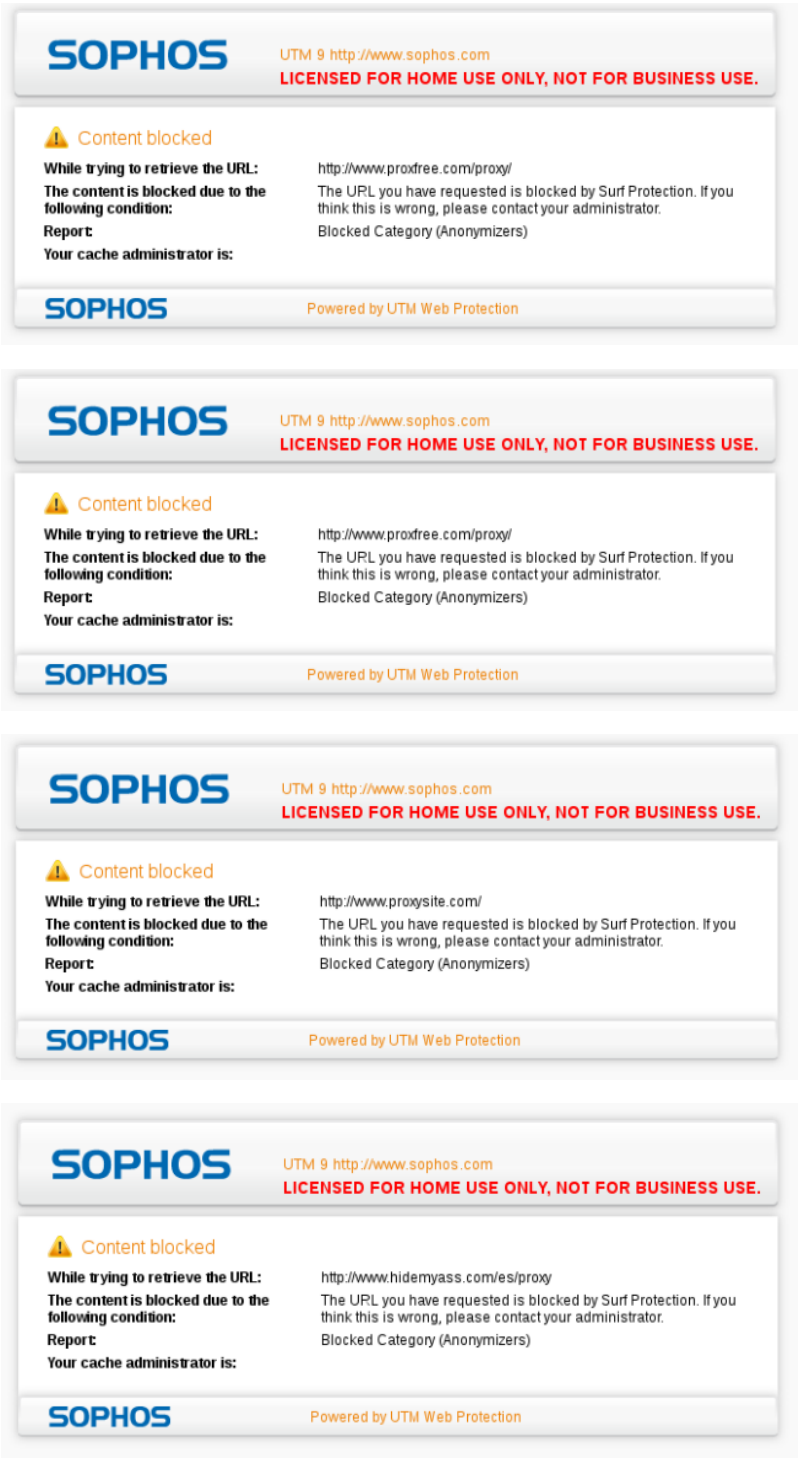


Figura 85: Filtro de contenidos HTTP (Sophos)

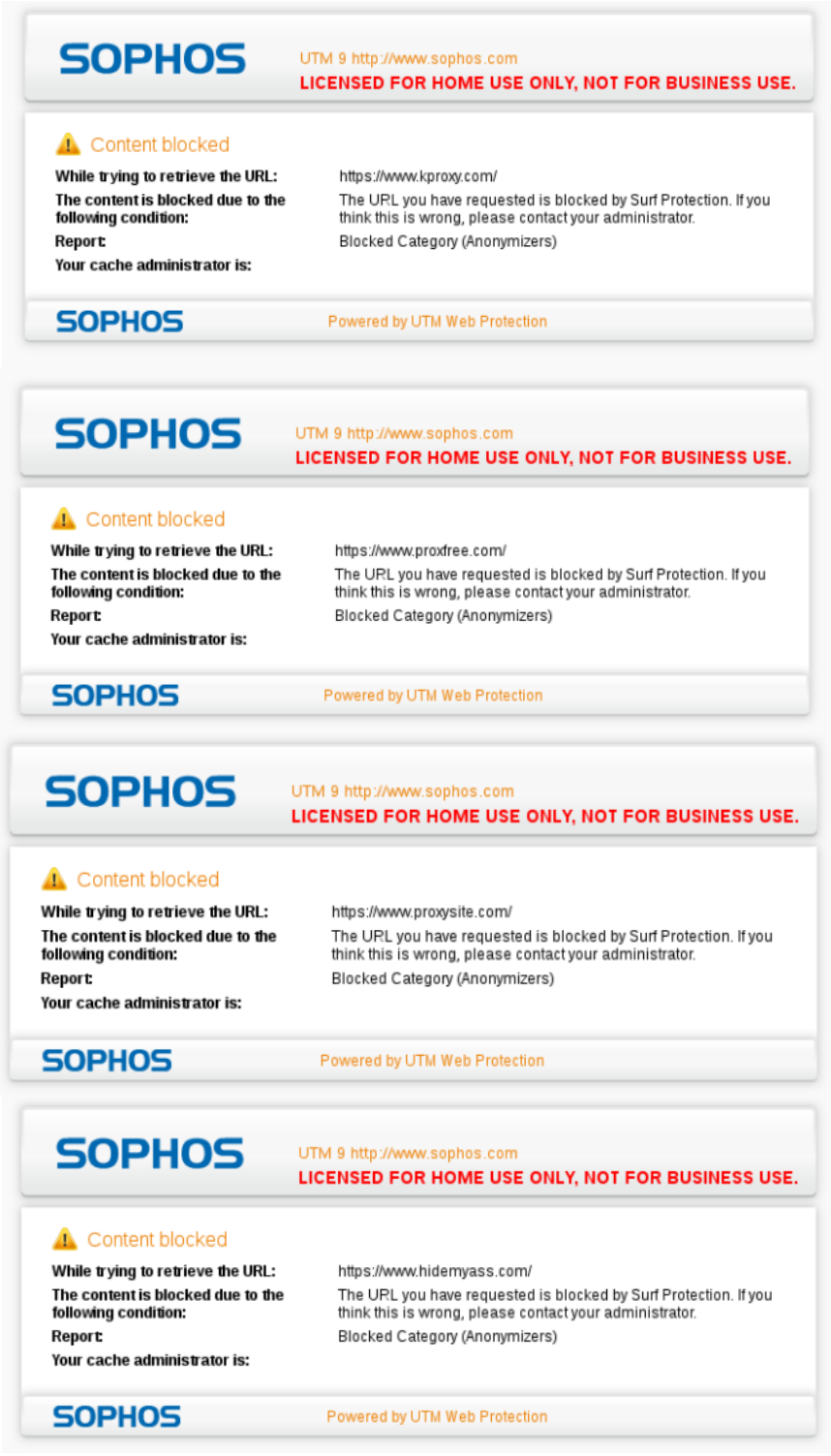
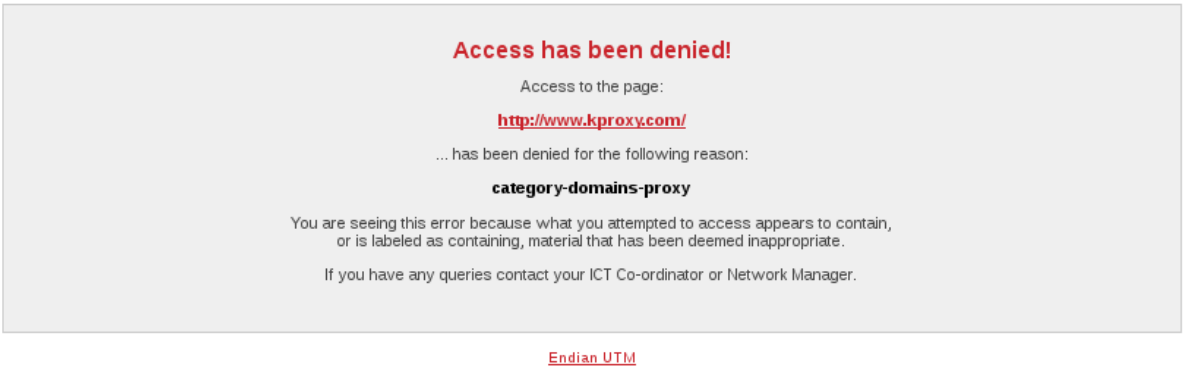


Figura 86: Filtro de contenidos HTTPs (Sophos)

Figura 87: Filtro de contenidos HTTP (Untangle). La muestra dos no fue bloqueada.



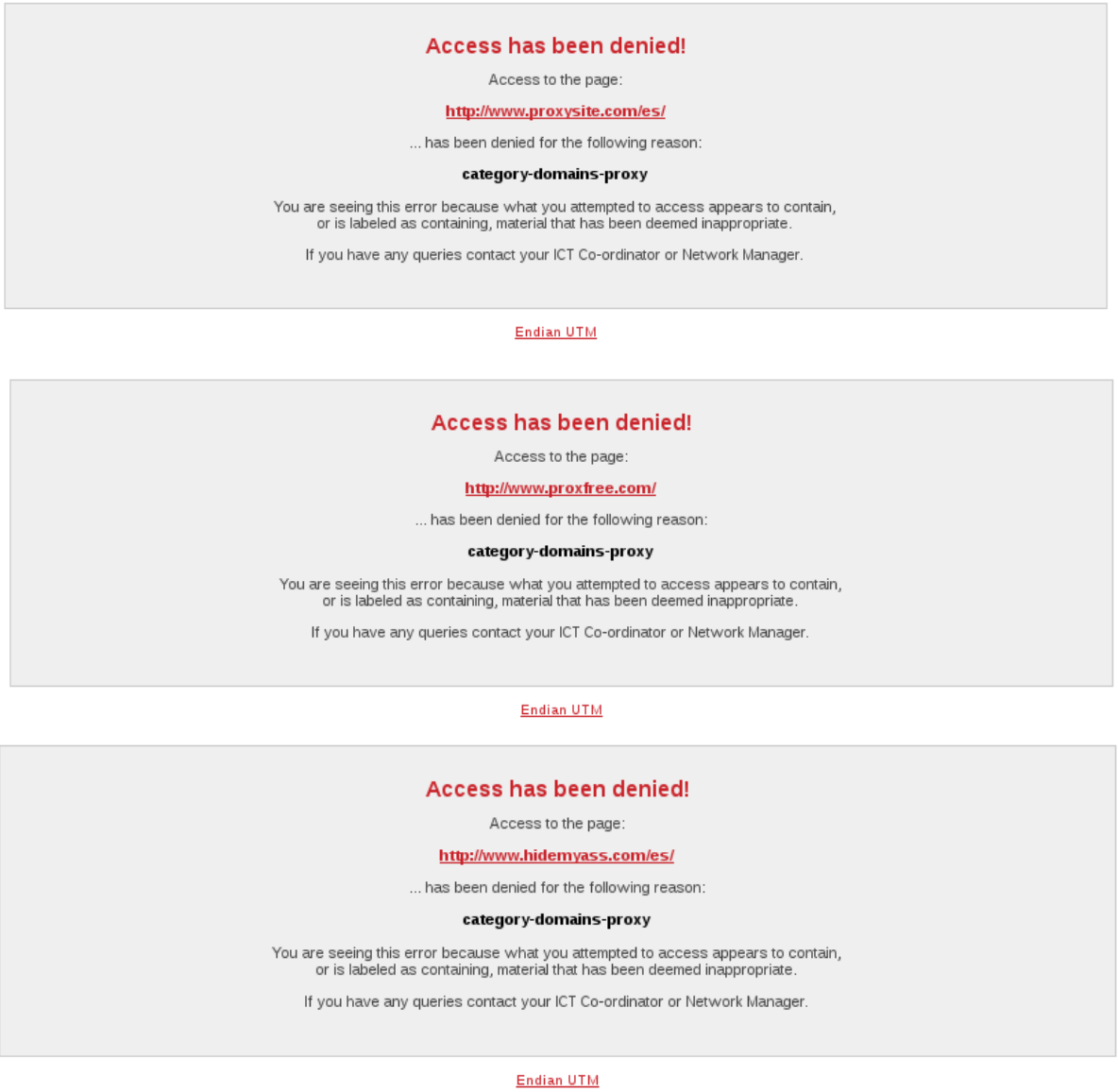
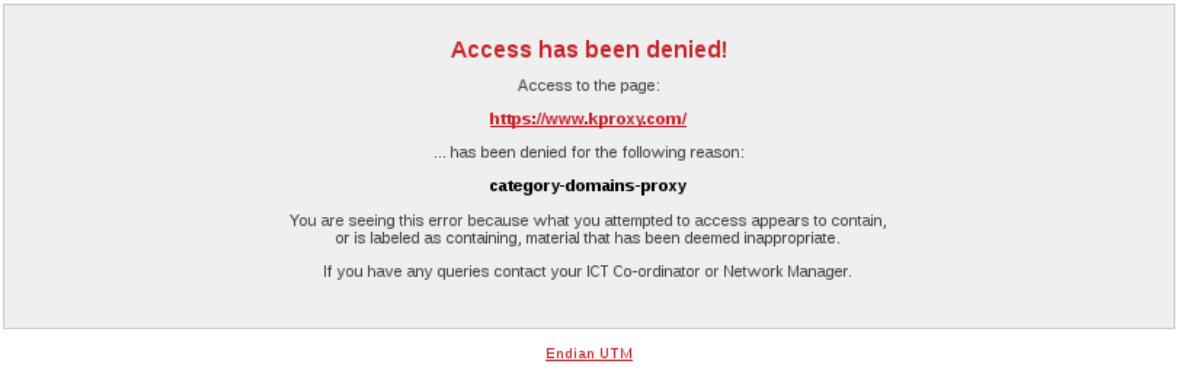


Figura 88: Filtro de contenidos HTTP (Endian).



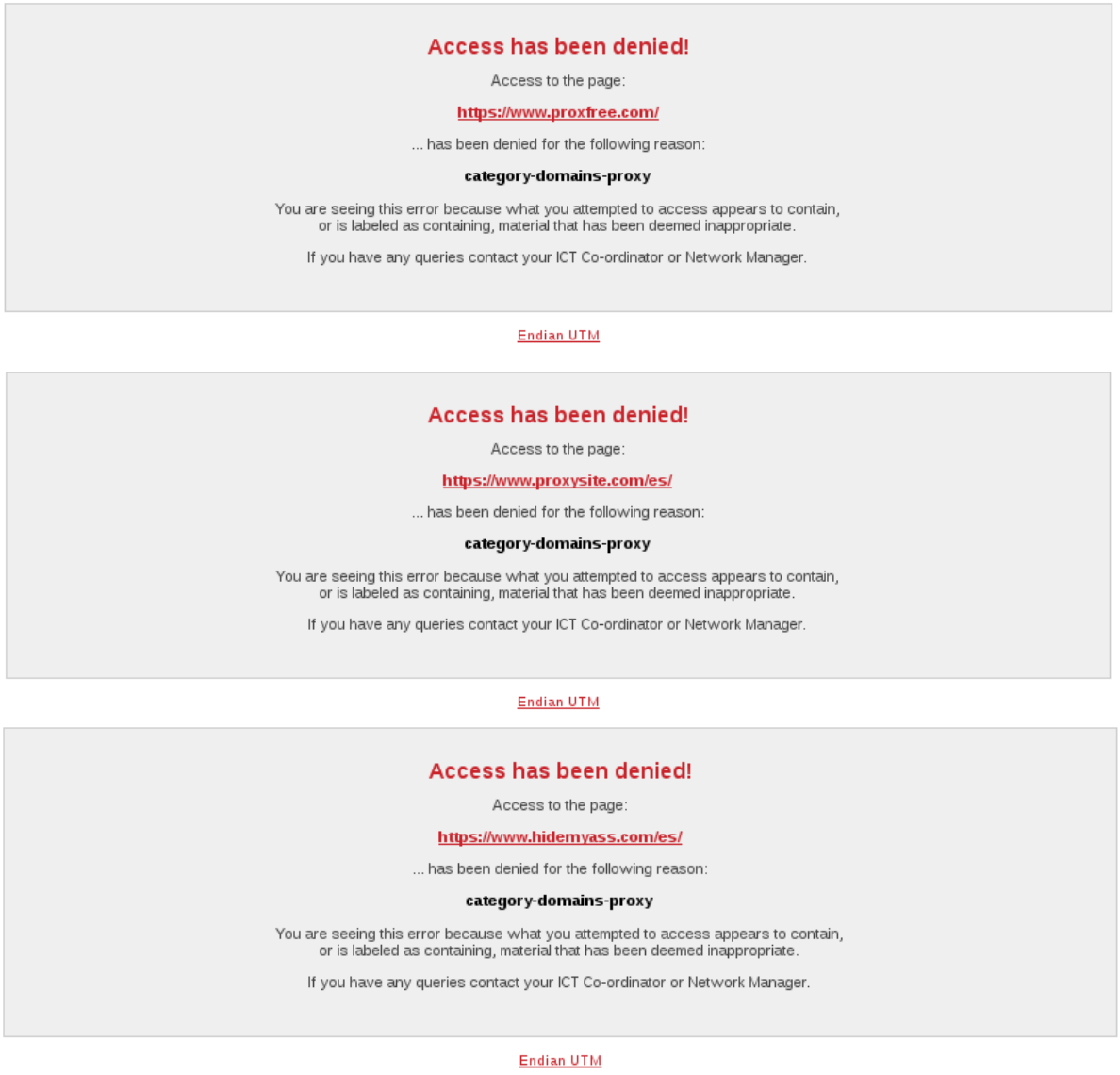


Figura 89: Filtro de contenidos HTTPs (Endian).

7.2 Anexo II – Bloqueo de malware en HTTP (Untangle)

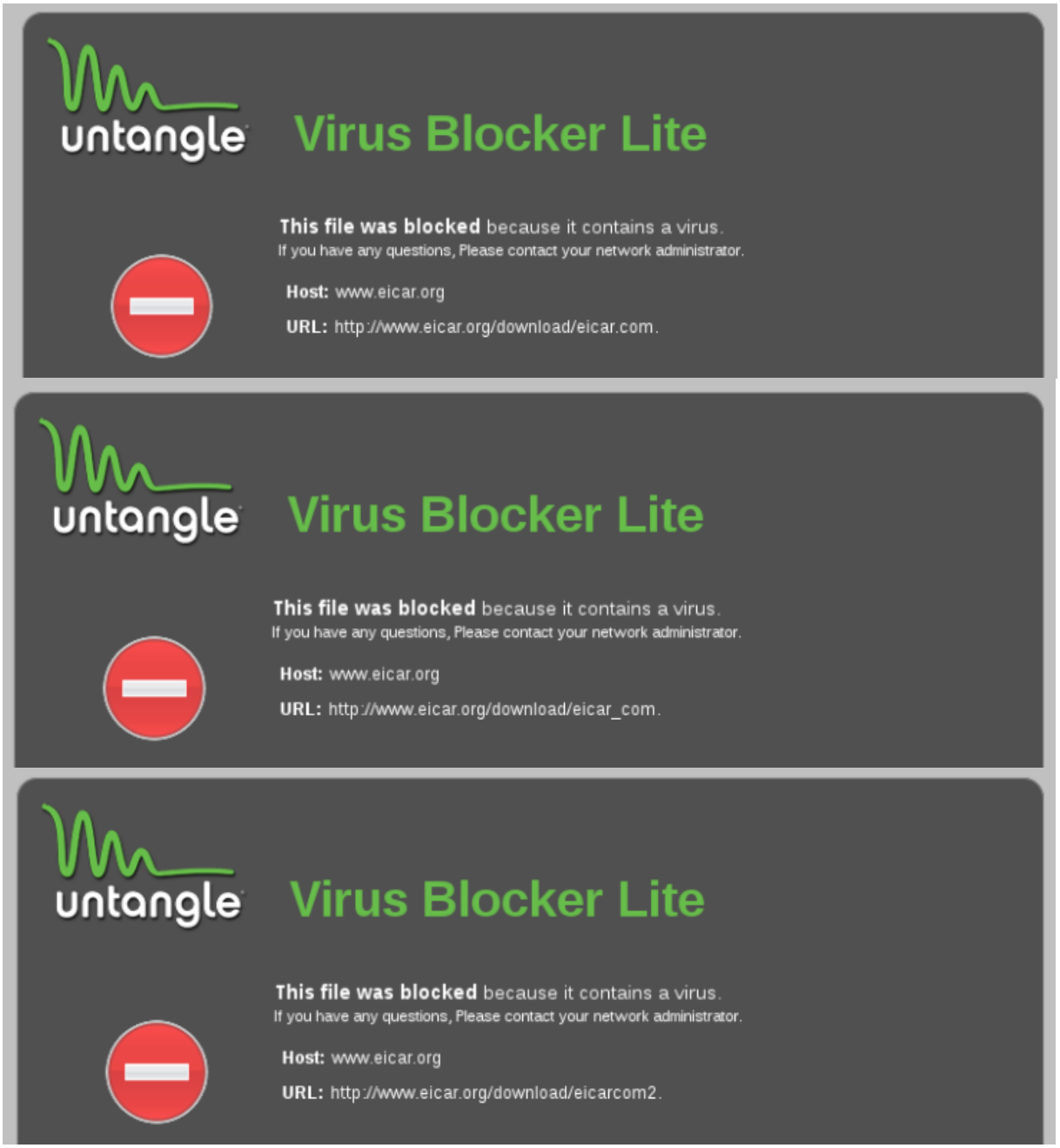


Figura 90: Bloqueo de malware en HTTP.

7.3 Anexo III – Bloqueo de malware en HTTPs (Endian)

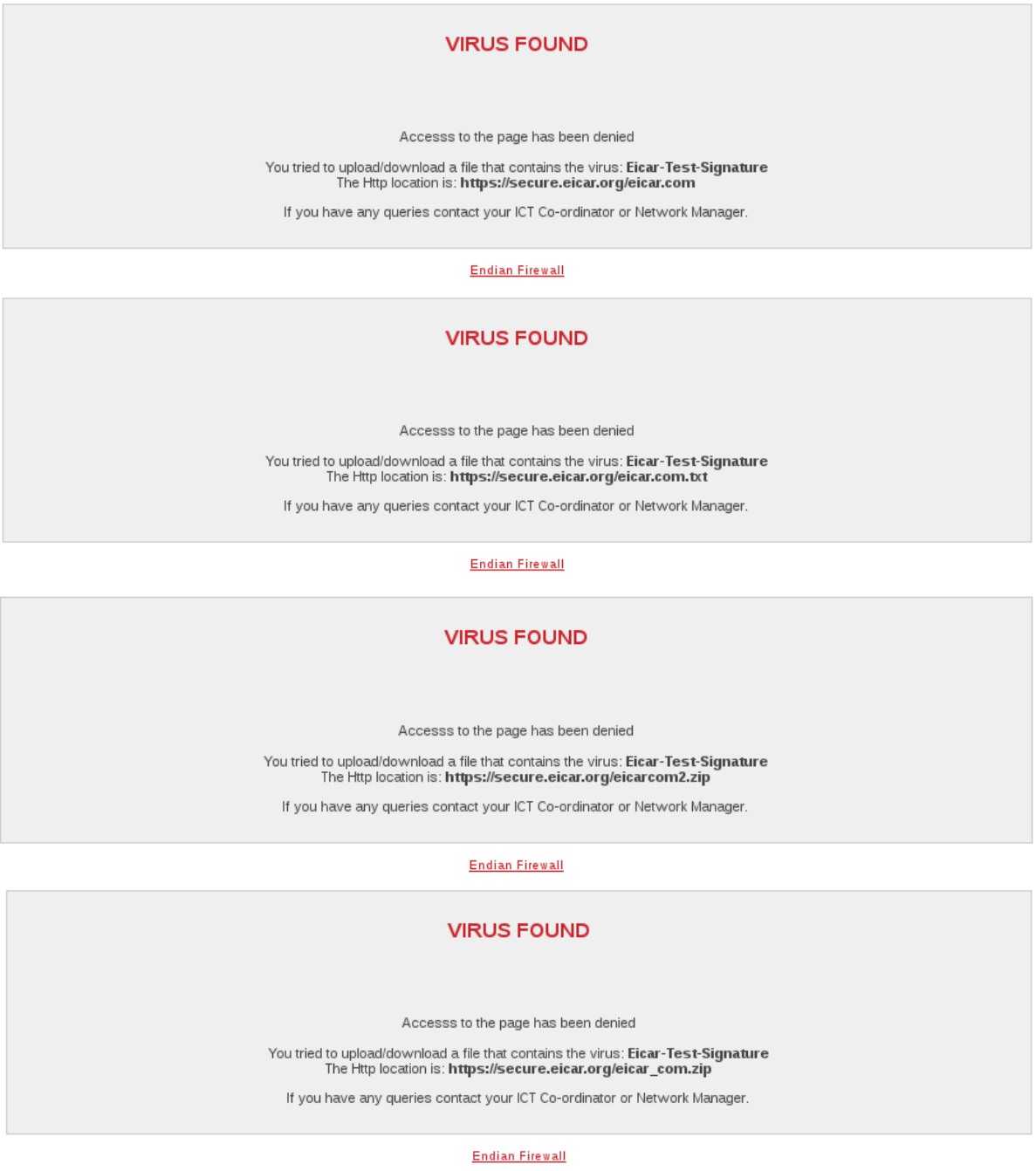


Figura 91: Bloqueo de malware en HTTPs.

7.4 Anexo IV – Resultados de HTTP Evader

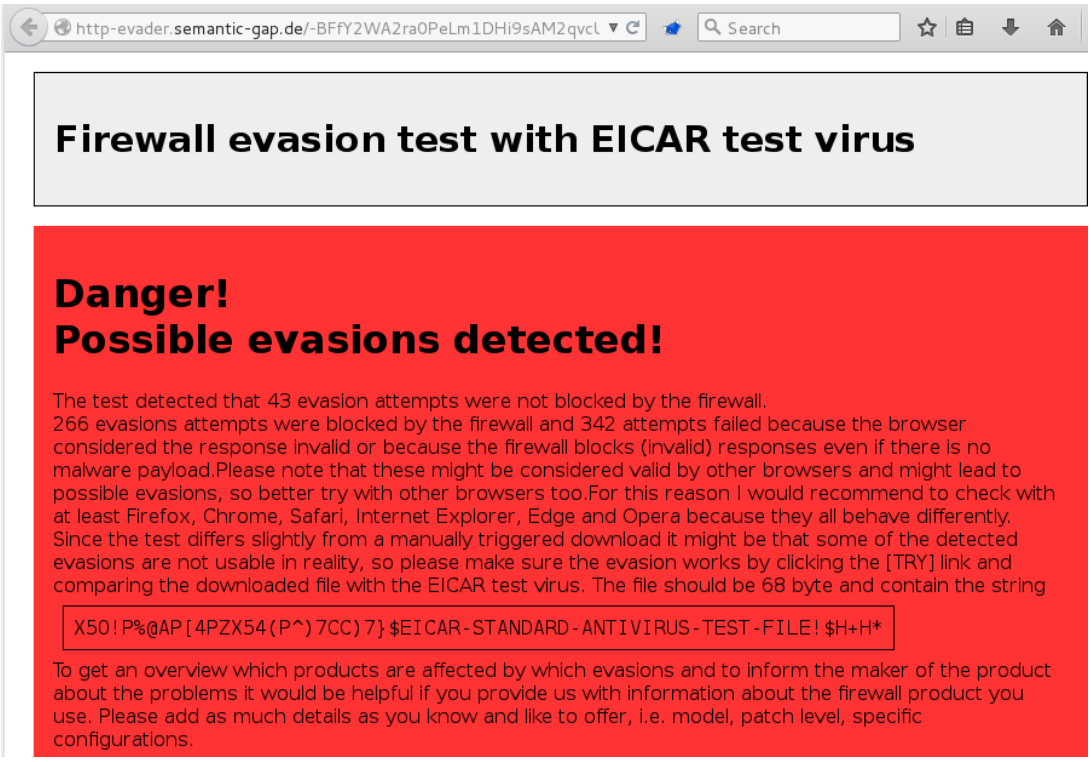


Figura 92: Evasiones del UTM Sophos.

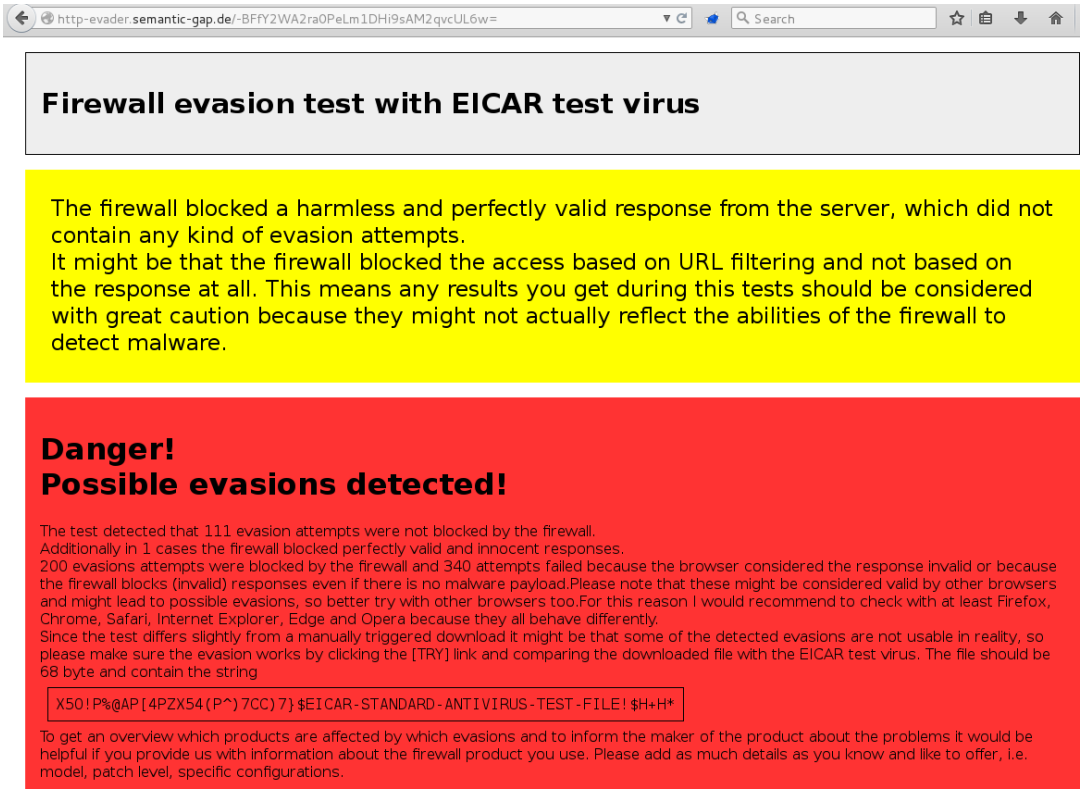


Figura 93: Evasiones del UTM Untangle.

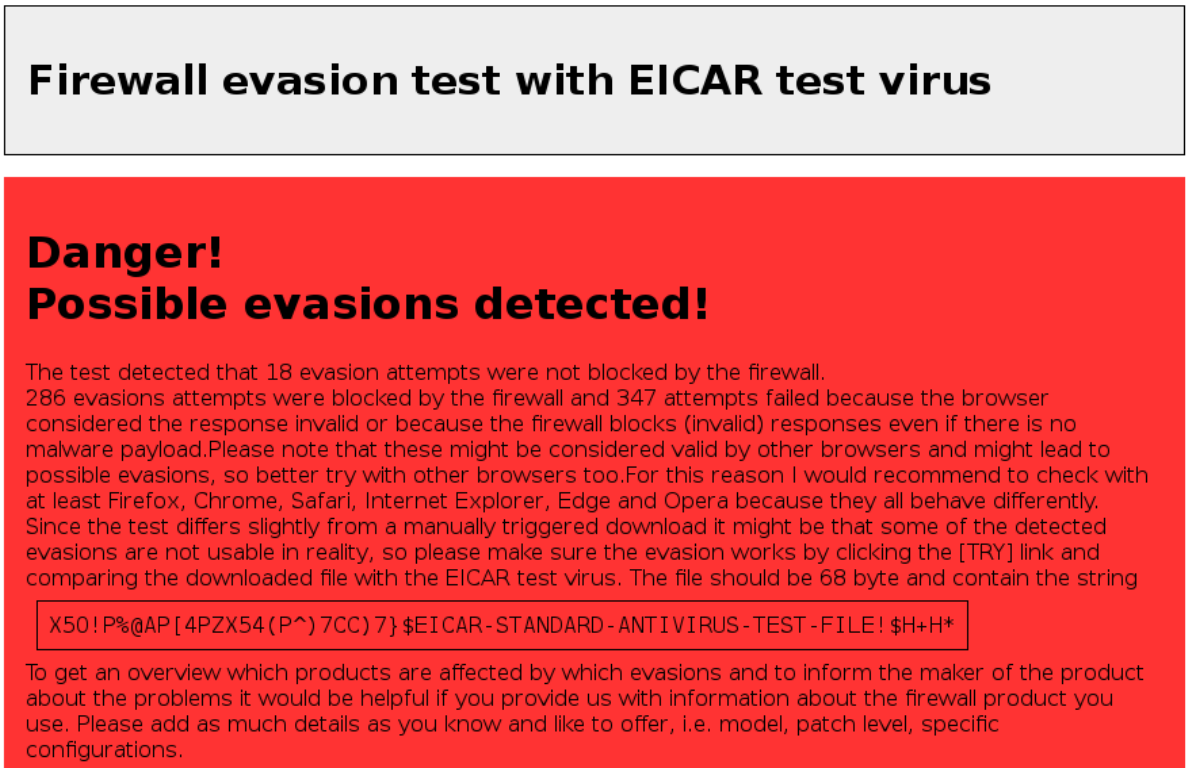


Figura 94: Evasiones del UTM Endian.

7.5 Anexo V – Peticion HTTP utilizada con netcat

GET / HTTP/1.1

Host: 192.168.3.50

Connection: Keep-alive