

Web Proxy transparente con antivirus y chequeo de lista negra de Urls

NOTA: la versión 1.0.beta9 de Zeroshell tiene algunos errores en el módulo de Proxy, por lo cual se necesita instalar el parche A500.

El propósito de este documento es describir la creación de un Proxy Web con un chequeo de antivirus de páginas Web y las listas negras y blancas. El documento se divide en las siguientes secciones:

- ¿Por qué usar un Proxy Web con un chequeo de antivirus?
- Modo de Proxy transparente
- Configuración y activación del servicio de Proxy
 - Registro de acceso y privacy
 - Antivirus de verificación de las imágenes
 - La actualización automática de las firmas ClamAV
- Página Web de listas negras y listas blancas
- Pruebas de Proxy y función antivirus

¿Por qué usar un Proxy Web con un chequeo de antivirus?

Las páginas Web son cada vez más los medios mas frecuentes por los que los gusanos y los virus se propagan en la Internet. Ya sea intencionalmente o porque son vulnerables y por lo tanto modificables sin el conocimiento de los autores legítimos, las paginas Web a veces tienen referencias de código ejecutable que puede infectar las computadoras de los usuarios. Además, la situación ha empeorado desde que una serie de vulnerabilidades en el sistema de visualización de las imágenes ha permitido a los virus portarse dentro de

archivos JPEG. Últimamente, el creciente uso de los applets de Java está aumentando el número de virus multiplataforma que se propagan a través de HTTP y su funcionamiento es independiente de la plataforma (PC, ordenador de bolsillo, teléfono móvil) o del sistema operativo en que trabajan.

La mejor solución para este tipo de problema es proporcionar a todos los dispositivos cliente que se conectan a Internet con un buen programa antivirus con protección en tiempo real, comprobando todos los archivos de entrada. Sin embargo, esto puede no ser suficiente por dos razones:

- ningún programa antivirus, incluso los que sí tienen firma de mecanismos de actualización, puede proporcionar una garantía del 100% contra todos los virus;
- la verificación en tiempo real del contenido entrante es bastante pesada en términos de cálculo y en particular en los dispositivos cuyo funcionamiento no es demasiado bueno, puede ralentizar el sistema hasta el punto de hacer que los usuarios deshabiliten la protección en tiempo real del antivirus.

Por estas razones, el chequeo de virus se realiza cada vez más en capas superiores, antes que virus potenciales puedan llegar los usuarios. En otras palabras, los sistemas centralizados de antivirus se utilizan en los servidores que ofrecen un servicio en particular. El ejemplo más extendido es el de los servidores de correo electrónico, que tienen un sistema que analiza los mensajes entrantes y salientes a través de SMTP y analizan los archivos adjuntos en busca de virus. En este caso, la aplicación de verificación de antivirus en una puerta de enlace SMTP es muy natural, ya que los correos electrónicos están obligados a pasar por ella, antes de llegar al buzón del usuario. Para el servicio HTTP, esto no es tan insignificante, ya que un cliente potencial de Internet se puede conectar directamente a cualquiera de los servidores Web disponibles en Internet. La solución a este problema consiste en la introducción de un nivel de aplicación de puerta de enlace a la red local para recoger las peticiones HTTP de clientes y los remitirá a los servidores Web pertinentes. Este aplicación de puerta de enlace se denomina Proxy Web y ya que es capaz de interpretar el protocolo HTTP, no sólo filtra sobre la base de las URL sino que también puede controlar el contenido transportado (HTML, JavaScript, Java Applet, imágenes,...) y los explora en busca de virus. Una de las

funciones más comunes de los Proxy hasta el momento han sido las cachés Web, es decir, archivos almacenados de las páginas Web que ya han sido visitadas, con el fin de acelerar la visualización de las mismas URL para las solicitudes posteriores. El objetivo de esto es también reducir el consumo de ancho de banda en Internet y uno de los más conocidos Proxy, capaz de realizar funciones de Web Cache es Squid, distribuido con licencia Open Source.

Zeroshell no se integra con Squid, ya que no recoge las páginas Web. La tarea de un programa de antivirus centrada en la red y el filtrado de contenidos, utilizando las listas negras de URL, es manejado por HAVP como sistema de representación y ClamAV como antivirus. Ambos se distribuyen bajo licencia GPL.

Modo de Proxy transparente

Uno de los mayores problemas cuando se utiliza un servidor Proxy es la de la configuración de todos los navegadores Web para usarlo. Por tanto, es necesario especificar su dirección IP o nombre de Host y el puerto TCP en el que responde (por lo general el puerto 8080). Esto podría ser una carga en el caso de redes de área local con numerosos usuarios, pero peor aún, no se podría garantizar que los usuarios no eliminen esta configuración para obtener acceso directo a la Web, evitando así la verificación de antivirus, el registro de acceso y listas negras.

Para resolver este problema, Zeroshell utiliza el modo de Proxy transparente que implica automáticamente la captura de las solicitudes de cliente en el puerto TCP 80.

Obviamente, para Zeroshell poder captar estas peticiones Web, debe ser configurado como un Gateway de la red, de modo que el tráfico de Internet de los cliente pase a través de ella. Zeroshell automáticamente captura las peticiones HTTP si se trata de un nivel 2 de puerta de enlace (puente entre Ethernet, WiFi o la interfaz VPN) o de la capa 3 de puerta de enlace (enrutador). Sin embargo, es importante especificar las interfaces de red IP o subredes a las que las solicitudes deben ser redirigidas. Esto se hace mediante la adición de las llamadas HTTP Capturing Rules (Reglas de Capturas de HTTP), como se muestra en la siguiente figura:

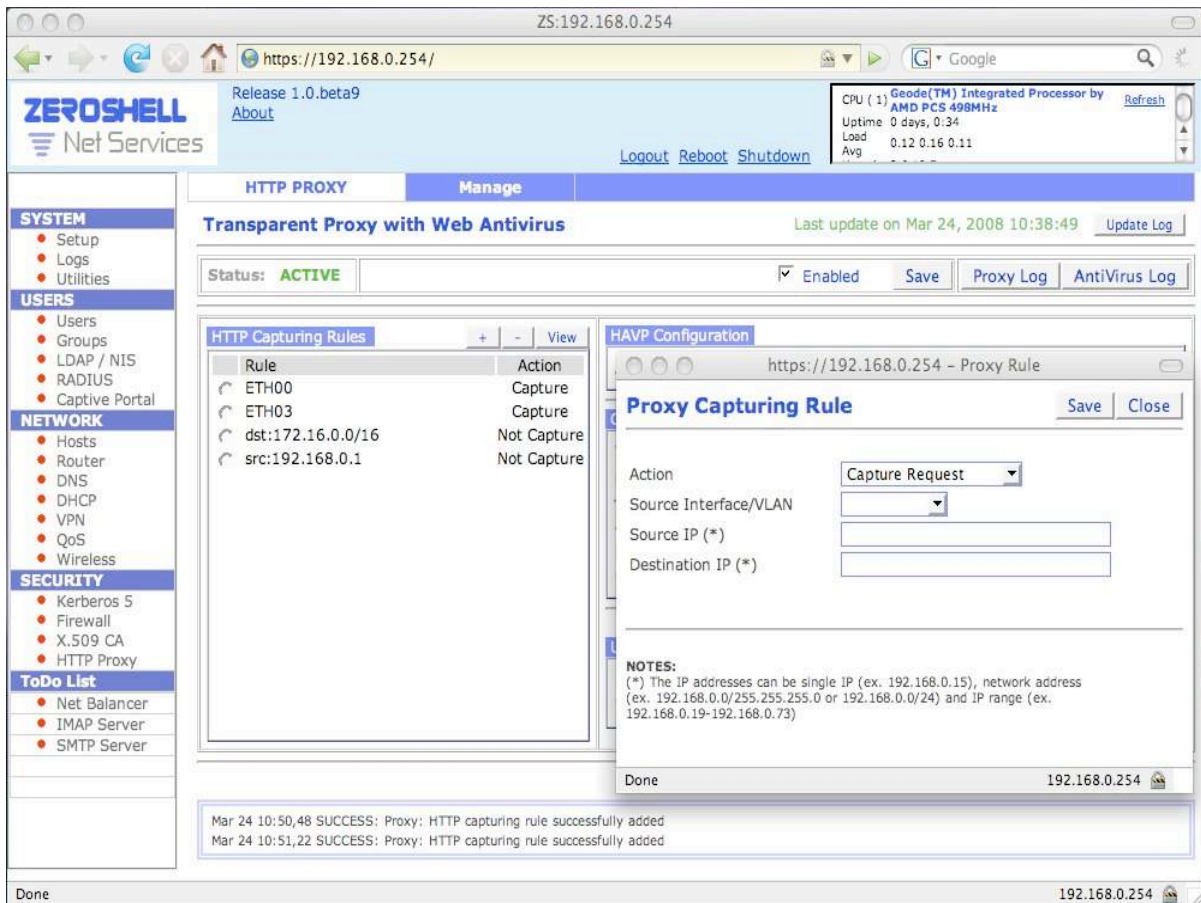


Figure 1 Configuración de las reglas de capturas Http.

En el ejemplo de la figura, se recogen las peticiones HTTP de ETH00 y las interfaces de red ETH03. Quedan excluidas de estas peticiones las dirigidas a los servidores Web que pertenecen a la subred 172.16.0.0/16 IP y los de los clientes con la dirección IP 192.168.0.1. Puede haber varias razones por las que es necesario excluir la intervención del Proxy transparente en algunos clientes y otros servidores Web. Por ejemplo, un servidor Web puede restringir el acceso sólo a los clientes con una dirección IP determinada en su ACL. En este caso, si las solicitudes de Proxy capturado en el servidor anterior, se llegaría a través de su IP y esto le impedirá el acceso. Por otra parte, no sería posible autorizar la dirección IP del Proxy en las ACL del servidor Web, ya que esto significaría que permite el acceso indiscriminado a todos los clientes mediante el Proxy. Es claro, entonces, que la única solución es evitar la captura de las solicitudes por el Proxy transparente.

Por último, tenga en cuenta que las reglas de IPTABLES para redirigir hacia el servicio de Proxy (8080 TCP) se sitúan en niveles inferiores de los que intervienen en el Captive Portal. Gracias a esto, el Captive Portal y el Proxy transparente pueden ser activados de manera simultánea en la misma interfaz de red.

Configuración y activación del servicio de Proxy

Como se ilustra en la figura siguiente, la configuración de Proxy con el servicio de verificación de antivirus es muy simple. Después de configurar el cuadro de Zeroshell para actuar como un router y después configurarlo en los clientes como la puerta de enlace predeterminada, o configurarlo como un puente, e interponerla en un punto de la LAN donde el tráfico fluye hacia y desde Internet, simplemente habilite la bandera [Enabled] para que el Proxy puede empezar a trabajar. Como se menciona en el párrafo anterior, las peticiones Web que en realidad son interceptadas y sometidas a la representación son especificadas a través de la configuración de *[HTTP Capturing Rules]*.

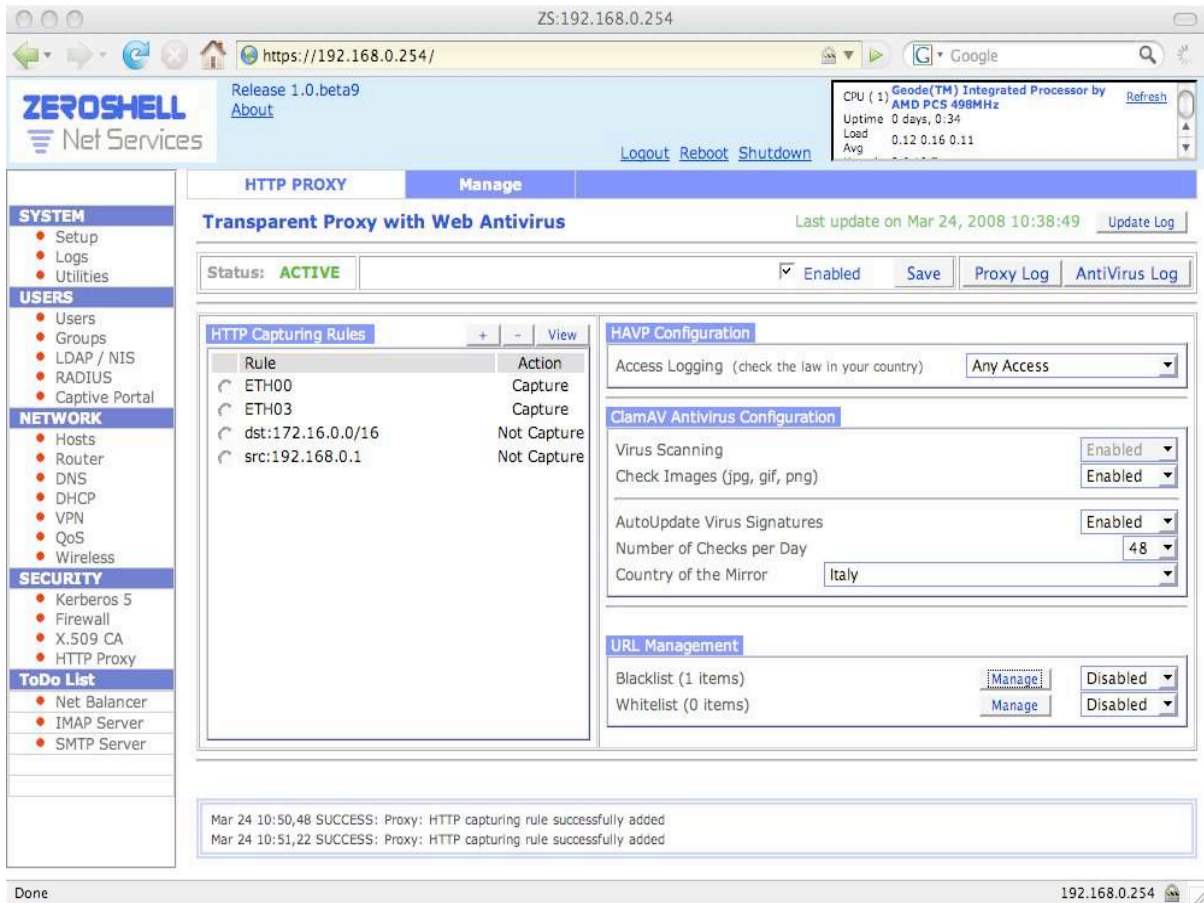


Figure 2 Configuración Proxy de las interfaces Web.

Tenga en cuenta que la puesta en marcha del servicio de Proxy es muy lenta en comparación con otros servicios, y en un hardware que no es muy rápido puede tardar hasta 30-40 segundos. Esto se debe a la necesidad de las bibliotecas de antivirus ClamAV de cargarse y descifrar un gran número de firmas de virus en su memoria. Para evitar el bloqueo de la interfaz de configuración Web y puesta en marcha de las secuencias de comandos para los intervalos de tiempo, el servicio se inicia de forma asincrónica. Por lo tanto, cuando el Proxy está activado o configurado de nuevo, el ítem correspondiente a estado (Status) no se muestra como Activo (verde) de inmediato, pero pasa primero por el estado inicial (naranja) que muestra que el servicio está cargando las firmas. Para saber cuándo comienza realmente la ejecución del Proxy, haga clic en [Administrar] para volver a cargar la página de configuración, o simplemente haga clic en [Registros del

Proxy] para ver el mensaje de inicio del *havp daemon*. Durante el período de arranque del demonio *havp*, las reglas de IPTABLES para la captura de peticiones HTTP son retiradas temporalmente, permitiendo el tráfico de Internet fluya con regularidad, pero sin que se analice en busca de virus.

Algunos elementos de configuración se analizan con más detalle en los párrafos siguientes.

Registro de acceso y privacy

Para ser una aplicación Gateway capaz de interpretar las peticiones HTTP, con el fin de que funcione correctamente, un Proxy Web descifra las URL visitadas por los usuarios. De forma predeterminada, Zeroshell no envía esta información a los registros del sistema, que, si se asocia con la dirección IP de los clientes que solicitan las páginas Web, puede ayudar a determinar el contenido visitado de los usuarios.

Sin embargo, el registro de esta información puede ser activado mediante la modificación del ítem [Registro de acceso] (*Access Logging*) a partir de "*Only URL containing Virus*" a "*Any Access*". De esta manera, todas las URL visitadas se registran en el registro de asociados con la dirección IP del cliente. Es necesario, antes de habilitar esta opción, consultar la legislación local en su país para verificar que el registro de las direcciones URL visitadas no está en contra de las leyes de privacidad nacional.

Además, es importante tener en cuenta que, tal como permite el NAT en un router de acceso a Internet, cada solicitud de cliente externo es hecha por el propio router, en la misma manera en que las peticiones pasan a través de un Proxy aparecen con la dirección IP del el servidor Proxy. Esto puede causar dificultades en el rastreo de la identidad de un usuario que ha llevado a cabo acciones ilícitas en servidores remotos. Una posible solución a este problema, que es menos invasiva en términos de privacidad, es activar el registro de la conexión de seguimiento (desde la interfaz Web Zeroshell [Firewall] [*Connection Tracking*]). De esta manera, cualquier conexión TCP / UDP se registran en los registros que muestra la dirección IP de origen, puerto de origen, IP de destino y puerto de destino. Por lo tanto, no será posible rastrear el contenido de la actividad del

usuario, pero quedará un rastro de las conexiones realizadas. Una vez más, en este caso es necesario consultar la legislación local antes de habilitar el seguimiento de la conexión.

Antivirus de verificación de las imágenes

Durante mucho tiempo se pensó que un archivo que contiene una imagen JPEG o GIF no puede contener un virus, porque esta simplemente compuesto de datos formateados en un formato preestablecido, interpretables por el sistema de visión del sistema operativo. Sin embargo, recientemente algunos componentes de la imagen de representación han demostrado que son vulnerables si no son actualizados con parches. Una imagen de construcción adecuada podría crear un desbordamiento de búfer y ejecutar código arbitrario en el sistema. Es fácil comprender la gravedad de esta, dado que el contenido de la mayoría de hipertexto de la WWW es en forma de imagen.

El Proxy HAVP configurado en Zeroshell, por defecto escanea las imágenes utilizando el programa antivirus ClamAV. Sin embargo, en un hardware lento, la digitalización de las imágenes podría retrasar la apertura de páginas Web con muchas imágenes. En este caso es posible deshabilitar la opción de escaneo de archivos que contienen imágenes, estableciendo las imágenes de chequeos [(jpg, gif, png)] de "Enabled" a "Disabled"

La actualización automática de las firmas ClamAV

La velocidad con que los virus nuevos se colocan en la Internet y se identifica, significa que las firmas antivirus se incrementan y se modifican con frecuencia. La base de datos de ClamAV no es la excepción, que, gracias al demonio freshclam, puede ser actualizada en línea a intervalos regulares.

Zeroshell freshclam configura de forma predeterminada para comprobar la base de datos de la firma 12 veces al día. Este intervalo se puede ajustar con el parámetro [Número de controles por día] (*Number of Checks per Day*), desde un mínimo de 1 a un máximo de 48 chequeos por día. También es importante establecer el [País del Espejo] (*Country of the Mirror*) de manera correcta, a través del cual freshclam elige el sitio más cercano desde el que descargar las firmas de virus. Tenga en cuenta, sin embargo, que la actualización periódica es una operación rápida, que no genera mucho tráfico, ya que se utiliza un sistema de actualización diferencial.

Página Web de listas negras y listas blancas

A menudo es necesario bloquear una serie de sitios Web, ya que su contenido no se considera adecuado para los usuarios del servicio Web. Un ejemplo son los materiales sólo para adultos, que no debe mostrarse en las computadoras en la que los niños tienen acceso. Una solución muy eficaz para este problema es forzando a los clientes Web acceder a Internet a través de un Proxy, que, a través de programas de filtrado de contenido, tales como DansGuardian, examina el contenido de las páginas HTML de bloqueo que se cree que pertenece a una categoría no deseada. Los mecanismos de estos filtros pueden ser comparados con los de los sistemas de antispamming.

Lamentablemente, sin embargo, no está claro si el permiso de liberación DansGuardian es compatible para la integración en un sistema como el Zeroshell y, por tanto, no se utilizan para evitar el riesgo de violación de la licencia.

Por el momento, la única manera de bloquear o permitir la visualización de páginas Web es la lista negra y lista blanca de páginas Web como se muestra en la figura.

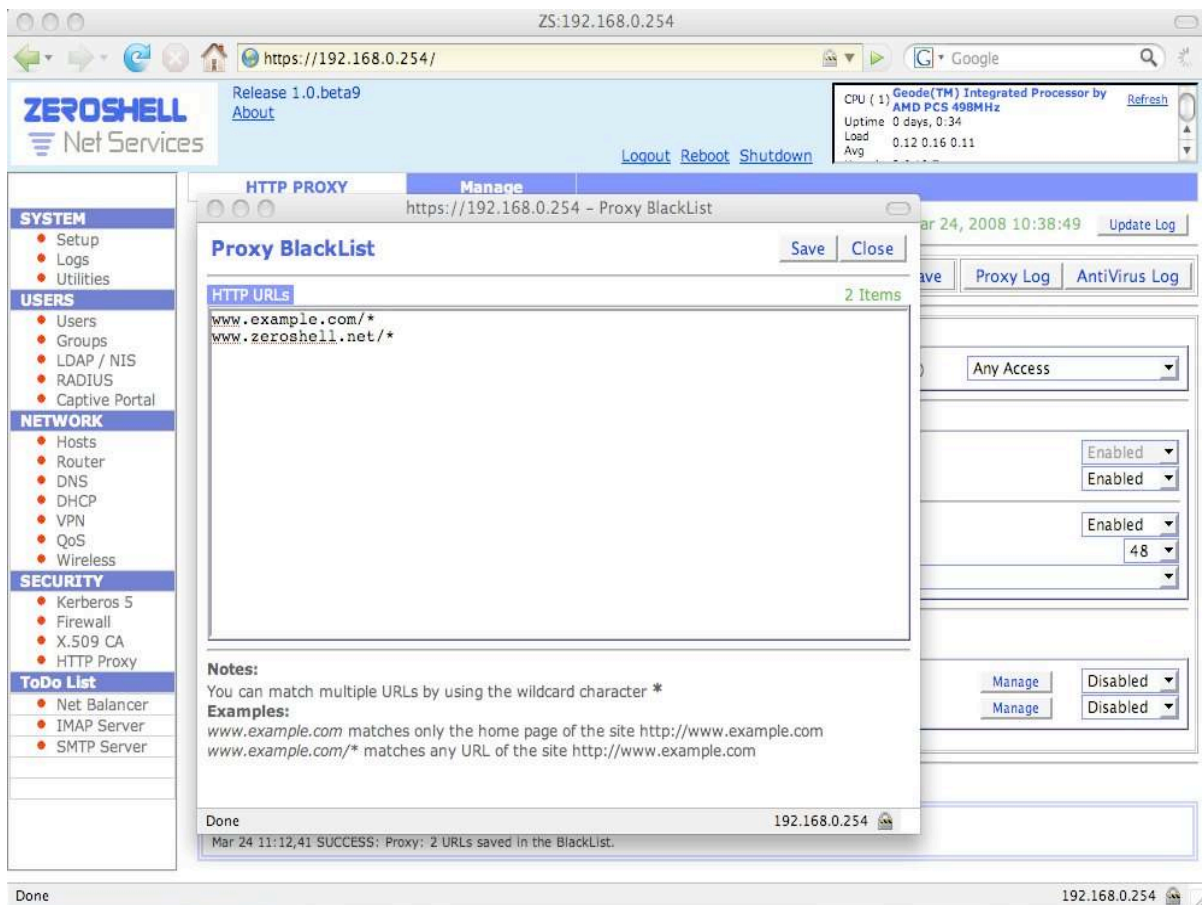


Figure 3 Configuración de las lista negras en el Proxy Web.

Las listas negras y listas blancas consisten en una secuencia de Urls dispuestas en líneas distintas. Cada línea puede corresponder a varias páginas Web cuando se utiliza el carácter *. Para bloquear el sitio *http://www.example.com* se sitúa *www.example.com/** en la lista negra, mientras que una línea como *www.example.com*, sin el *, sólo bloqueará la página principal de ese sitio.

La lista blanca tiene prioridad sobre la lista negra. En otras palabras, si una página Web corresponde a un elemento de la lista negra y, al mismo tiempo, se encuentra en la lista blanca, se permite el acceso a la página.

Además, tenga en cuenta que el propósito de la lista blanca no es sólo permitir el acceso a páginas que de otro modo estaría prohibido por la lista negra, sino también para comprobar la derivación de antivirus. Por favor tome nota de esto.

Si el administrador de la LAN quiere adoptar la política de proporcionar acceso a un

número limitado de sitios, s / se puede especificar el * / * Línea en la lista negra, lo que impedirá el acceso a todas las páginas, excepto los incluidos en la lista blanca.

Pruebas de Proxy y función antivirus

Existen básicamente dos razones por las que el Proxy no funcione correctamente. En primer lugar, es necesario asegurar que el cuadro de Zeroshell está configurado como un enrutador o un puente, y también que el tráfico hacia y desde Internet pasa a través de este. En segundo lugar, usted debe estar seguro de la correcta configuración de la *[HTTP Capturing Rules]*, que determinan que las solicitudes HTTP son en realidad redirigido hacia el proceso de Proxy (havy escucha en 127.0.0.1:8080). En particular, si la captura de peticiones http se impone en una interfaz de red que forma parte de un puente, tiene que estar seguro de que al menos una dirección IP ha sido definida en el segundo.

La forma más sencilla de comprobar si el Proxy funciona correctamente es habilitar temporalmente el registro de todos los accesos y mostrar el registro del Proxy, previa solicitud de las páginas Web de un cliente.

Una vez seguro de que el Proxy Web captura las solicitudes como se espera, verifique que el software de antivirus ClamAV este funcionando correctamente. Para ello, debe comprobar por primera vez en los registros freshclam que las firmas se actualizan regularmente. Luego, vaya a la URL http://www.eicar.org/anti_virus_test_file.htm para comprobar si el *EICAR-AV-Test* virus de prueba (que se dice ser inocente por los autores) es capturado y bloqueado.

Por último, tenga en cuenta que el Proxy no puede servir a las peticiones HTTPS (HTTP encriptada con SSL / TLS), dado que al no tener la clave privada del servidor Web, no se puede descifrar el contenido y la URL de esta petición es encapsulada en los túneles de cifrado.