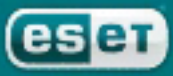


protegemos su mundo digital

ESET Gateway Security

Manual de instalación y documentación para el usuario

Contenidos

ESET Gateway Security, Primera Edición
Fecha de publicación 13 de marzo de 2007

Capítulo 1:

Introducción

Estimado usuario, Ud. acaba de adquirir ESET Gateway Security - probablemente el mejor sistema de seguridad en los sistemas operativos Linux y BSD. Como descubrirá muy pronto, el sistema, que utiliza el motor de análisis de última tecnología ESET, posee una velocidad de búsqueda y tasa de detección de virus hasta el momento insuperables, y el uso de recursos es tan bajo que lo convierte en la elección ideal para cualquier servidor con SO Linux o BSD.

En el resto del capítulo analizaremos las características principales del sistema.

• Los algoritmos del motor de análisis del antivirus ESET proveen la mayor tasa de detección de virus y las búsquedas más veloces.

• ESET Gateway Security está preparado para trabajar en unidades con un procesador o con procesadores múltiples.

• Incluye una heurística única y avanzada para la detección de gusanos y componentes de puerta trasera (*back-doors*) en Win32.

• Los archivos autoextraíbles no requieren el uso de programas externos.

• Para incrementar la velocidad y la eficiencia del sistema, su arquitectura se basa en un programa residente activo (*daemon*), donde se envían todos los pedidos de análisis.

• El sistema soporta la configuración selectiva para la identificación diferenciada del usuario o cliente/servidor.

• Se pueden configurar hasta seis niveles de registración de eventos (*logging*) para obtener información sobre la actividad del sistema y las infiltraciones.

• La instalación de ESET Gateway Security no requiere bibliotecas ni programas externos excepto la biblioteca estándar de C (*LIBC*).

• El sistema puede configurarse para notificar a una persona determinada en caso de que se detecte una infiltración.

Para un funcionamiento eficiente, ESET Gateway Security requiere tan solo 16MB de espacio en disco rígido y 32MB de memoria. Opera sin problemas con las versiones 2.2.x, 2.4.x. y 2.6.x del núcleo (kernel) del SO Linux y también con las versiones 5.x y 6.x del núcleo (kernel) de FreeBSD.

Desde pequeños servidores de oficina hasta servidores para proveedores de servicios de Internet con miles de usuarios, el sistema proporciona el rendimiento y la escalabilidad que se esperan de una solución basada en UNIX y la inigualable seguridad de los productos marca ESET.

Capítulo 2:

Terminología y abreviaciones

A continuación exponemos brevemente los términos y abreviaciones utilizados en este documento. Recuerde que en este documento en formato PDF se reserva el uso de la letra negrita para los nombres de componentes del producto y, en este capítulo, para abreviaciones y términos nuevos. También tenga en cuenta que los términos y abreviaciones explicados en este capítulo aparecerán en cursiva en el resto del documento.

ESETS

ESET Security (Seguridad) es el acrónimo que abarca todos los productos de seguridad desarrollados por ESET, spol. s r.o. para los sistemas operativos Linux y BSD. También es el nombre (o parte del nombre) del paquete de programas que contiene los diversos productos.

RSR

Es la abreviación de "RedHat/Novell(SuSE) Ready". También soportamos la variante del producto llamada "RedHat Ready y Novell(SuSE) Ready". La diferencia con la versión "estándar" de Linux es que el paquete RSR reúne criterios definidos por el documento *FHS* (Estándar de Jerarquía de Sistema de Ficheros definido como parte de la Base Estándar para Linux) requerido por la certificación RedHat Ready y Novell(SuSE) Ready. Esto significa que el paquete RSR, por ejemplo, se instala como una aplicación suplementaria, es decir, el directorio principal de instalación es '/opt/eset/esets'.

Daemon de ESETS (programa residente)

Es el sistema principal de control y análisis residente de *ESETS*: **esets_daemon.**

Directorio base de ESETS

Es el directorio donde se guardan los módulos ejecutables de *ESETS* que contienen, por ejemplo, bases de datos con firmas de virus. En este documento utilizaremos la abreviación **@BASEDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /var/lib/esets
Linux RSR: /var/opt/eset/esets/lib
BSD: /var/lib/esets
```

Directorio de configuración de ESETS

Es un directorio donde se guardan todos los archivos relacionados con la configuración de ESET Gateway Security. En este documento utilizaremos la abreviación **@ETCDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /etc/esets
Linux RSR: /etc/opt/eset/esets
BSD: /usr/local/etc/esets
```

Archivo de configuración de ESETS

Es el archivo de configuración principal de ESET Gateway Security. La ruta absoluta del archivo es la siguiente:

```
@ETCDIR@/esets.cfg
```

Directorio de archivos binarios de ESETS

Es el directorio donde se guardan los archivos binarios relevantes de ESET Gateway Security. En este documento utilizaremos la abreviación **@BINDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/bin
Linux RSR: /opt/eset/esets/bin
BSD: /usr/local/bin
```

Directorio de archivos binarios del sistema de ESETS

Es el directorio donde se guardan los archivos binarios del sistema relevantes de ESET Gateway Security. En este documento utilizaremos la abreviación **@SBINDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/sbin
Linux RSR: /opt/eset/esets/sbin
BSD: /usr/local/sbin
```

Directorio de archivos con códigos objeto de ESETS

Es el directorio donde se guardan los archivos con códigos objeto y bibliotecas relevantes de ESET Gateway Security. En este documento utilizaremos la abreviación **@LIBDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/lib/esets
Linux RSR: /opt/eset/esets/lib
BSD: /usr/local/lib/esets
```

Capítulo 3:

Instalación

Este producto se distribuye como un archivo binario:

```
esets.i386.ext.bin
```

donde 'ext' es un sufijo dependiente de la distribución del SO Linux/BSD, es decir, 'deb' para Debian, 'rpm' para RedHat y SuSE, 'tgz' para otras distribuciones del SO Linux, 'fbs5.tgz' para distribuciones de FreeBSD 5.xx y 'fbs6.tgz' de FreeBSD 6.xx respectivamente.

Tenga en cuenta que el formato de archivo binario para Linux *RSR* es:

```
esets-rsr.i386.rpm.bin
```

Para instalar o actualizar el producto, utilice el comando:

```
sh ./esets.i386.ext.bin
```

En la variante del producto para Linux *RSR*, utilice el comando:

```
sh ./esets-rsr.i386.rpm.bin
```

Como respuesta, aparecerá el Contrato de Licencia del producto para la aceptación por parte del usuario. Una vez confirmado el Contrato de Licencia, el paquete de instalación se ubica en el directorio activo actual y se imprime información relevante sobre el paquete de instalación, desinstalación o actualización en la terminal.

Una vez que el paquete está instalado y el servicio principal de *ESETS* está en funcionamiento, en el SO Linux se puede observar su desempeño usando el comando:

```
ps -C esets_daemon
```

En caso de que el SO sea BSD, se usa un comando similar:

```
ps -ax esets_daemon | grep esets_daemon
```

Como respuesta, verá el siguiente mensaje (o uno similar):

```
PID TTY          TIME CMD
2226 ?        00:00:00 esets_daemon
2229 ?        00:00:00 esets_daemon
```

donde al menos dos procesos *daemon* de *ESETS* deben estar activos en segundo plano. Uno de dichos procesos es el gestor de procesos y de hilos de ejecución del sistema. El otro constituye el proceso de análisis de *ESETS*.

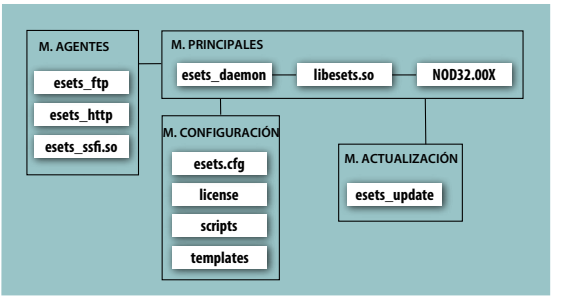
Capítulo 4:

Estructura del producto

Una vez que el paquete del producto se ha instalado exitosamente, llega el momento de familiarizarse con su contenido.

La estructura de ESET Gateway Security se muestra en la imagen 4-1. El sistema está formado por los siguientes componentes.

Imagen 4-1. Estructura de ESET Gateway Security



MÓDULOS PRINCIPALES

La parte principal de ESET Gateway Security consiste en el *daemon* de *ESETS* **esets_daemon.** El *daemon* utiliza la biblioteca de interfaz de programas de aplicación (*API*) **libesets.so** y los módulos ejecutables nod32.00X de *ESETS* para realizar las tareas básicas del sistema: análisis, mantenimiento de los procesos agentes *daemon*, mantenimiento del sistema de envío de muestras, registros, notificación, etc. Por favor, consulte la página del manual esets_daemon(8) para más detalles.

MÓDULOS AGENTES

El propósito de los módulos agentes de *ESETS* es integrar a *ESETS* con el entorno del servidor Linux/BSD. En este manual encontrará un capítulo especial dedicado al tema.

MÓDULOS DE ACTUALIZACIÓN

La utilidad de actualización es una parte importante del sistema. Fue desarrollada para actualizar los módulos ejecutables de *ESETS* que contienen, por ejemplo, bases de datos con firmas de virus, soporte de ficheros, soporte de heurística avanzada, etc. En este documento encontrará un capítulo especial dedicado al tema.

MÓDULOS DE CONFIGURACIÓN

La correcta configuración es la condición principal para el buen funcionamiento del sistema. Es por eso que en el resto de este capítulo describiremos todos los componentes relacionados a la configuración. También recomendamos la página del manual esets.cfg(5), una fuente de información esencial sobre la configuración de *ESETS*. Una vez que el producto se encuentra correctamente instalado, todos sus componentes para la configuración se guardan en el *directorio de configuración* de *ESETS*. El directorio está formado por los siguientes archivos:

***@ETCDIR*@/esets.cfg**

Éste es el archivo de configuración más importante ya que preserva la mayor parte del funcionamiento del producto. Luego de explorar el archivo, notará que está creado por varios parámetros distribuidos dentro de secciones. Los nombres de las secciones aparecen entre corchetes.

En el *archivo de configuración* de *ESETS* siempre hay una sección global y varias secciones agentes. Los parámetros en la sección global se usan para definir las opciones de configuración del *daemon* de *ESETS* así como los valores predeterminados de las opciones de configuración del motor de análisis de *ESETS*. Los parámetros de las secciones agentes se utilizan para definir las opciones de configuración de los agentes, es decir, módulos usados para interceptar diversos tipos de flujo de datos en la computadora y/o su entorno y preparar dichos datos para su análisis. Recuerde que, además del número de parámetros usados para la configuración del sistema, también existe una serie de reglas que determinan la organización del archivo. Para familiarizarse con esta información, consulte las páginas del manual esets.cfg(5), esets_daemon(8) así como otras páginas sobre agentes relevantes.

@*ETCDIR*@/certs

Este directorio se utiliza para guardar los certificados usados por la Interfaz WWW de *ESETS* para la autenticación (ver la página esets_wwwi(8) para más detalles).

@*ETCDIR*@/license

Este directorio se utiliza para guardar la/s clave/s de licencia que Ud. ha adquirido de su vendedor. El residente *daemon* de ESETS siempre se dirigirá sólo a este directorio para confirmar la validez de la clave de licencia, a menos que sea redefinido desde el parámetro 'lic_dir' en el *archivo de configuración* de *ESETS*.

@*ETCDIR*@/scripts/license_warning_script

Este *script*, si se habilita desde el parámetro 'license_warn_enabled' en el *archivo de configuración* de *ESETS,* se ejecuta durante los 30 días anteriores al vencimiento de la licencia del producto. Se utiliza para enviar notificaciones por correo electrónico sobre la fecha de vencimiento al administrador del sistema.

@*ETCDIR*@/scripts/daemon_notification_script

Este *script*, si se habilita desde el parámetro 'exec_script' en el *archivo de configuración* de *ESETS*, se ejecuta en caso de que el sistema anti-virus haya detectado una infiltración. Se utiliza para enviar notificaciones por correo electrónico sobre la detección al administrador del sistema.

@*ETCDIR*@/templates/http_*.html.example

Estos archivos son plantillas html que el módulo **esets_http** utiliza cuando el análisis no tuvo éxito por diversos motivos. El significado de cada archivo individual es el siguiente:

Las siguientes plantillas se usan al detectar que el objeto descargado está infectado.

```
content of http_header_infected.html
list of infiltrations found by the scanner
content of http_footer_infected.html
```

Las siguientes plantillas se usan cuando el objeto descargado no pudo ser analizado.

```
content of http_header_not_scanned.html
list of object scanned by the scanner
content of http_footer_not_scanned.html
```

Capítulo 5:

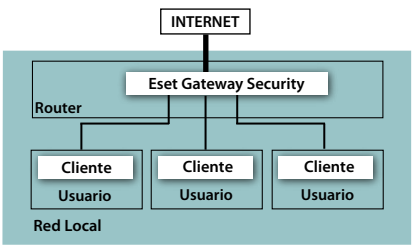
Integración con los servicios de Puerta de Enlace de Internet

ESET Gateway Security protege los servicios HTTP y FTP de las organizaciones contra virus, gusanos, troyanos, *spyware* (programas espía), *phishing* (suplantación de identidad) y otras amenazas en el nivel de los Servidores de Puerta de Enlace de Internet. Con el término "Servidor de Puerta de Enlace" nos referimos a la capa de red (capa 3) del modelo ISO/OSI, es decir, los *routers*. En este capítulo describimos los procesos de integración del producto con los servicios mencionados.

5.1. Configuración transparente de proxy HTTP/FTP

La configuración transparente de proxy se basa en el mecanismo estándar de enrutamiento como se muestra en la siguiente imagen:

Imagen 5-1. Esquema de ESET Gateway Security con un proxy transparente.



La configuración se lleva a cabo automáticamente cuando se definen las tablas de enrutamiento IP del núcleo para cada usuario local de red. Estas tablas de enrutamiento se utilizan para establecer rutas estáticas para el servidor de puerta de enlace de red predeterminado (*router*). Recuerde que esta acción se realiza automáticamente en redes DHCP. Si se usa este mecanismo, todas las comunicaciones HTTP (o FTP) con servidores externos serán enrutadas a través del servidor de puerta de enlace de red donde deberá estar instalado ESET Gateway Security para que pueda analizar dichas comunicaciones y detectar posibles infiltraciones. Con este propósito se ha desarrollado un filtrador genérico de *ESETS* para HTTP (o FTP): **esets_http** (o **esets_ftp** respectivamente).

Si desea configurar ESET Gateway Security para analizar los mensajes HTTP (o FTP) enrutados a través del servidor de puerta de enlace de red, ingrese el siguiente comando:

```
esets_setup
```

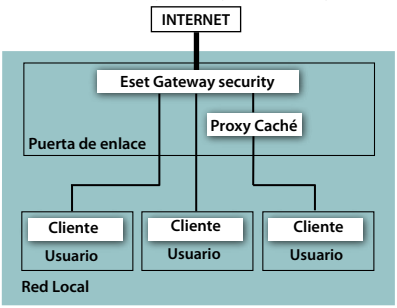
Siga las instrucciones suministradas por el *script*. Cuando aparezca la sección de instalaciones y desinstalaciones disponibles 'Available installations/un-installations', elija la opción 'HTTP' (o FTP) para que le muestre las opciones de instalación y desinstalación 'install/uninstall' apropiadas para el módulo. Seleccione la opción 'install'. De esta forma se configurará automáticamente el módulo para que atienda un puerto predeterminado y redirija los paquetes IP originados en la red seleccionada y con el puerto de destino HTTP (o FTP) hacia el puerto atendido por **esets_http** (o **esets_ftp** respectivamente). Esto significa que sólo serán analizados los pedidos enviados originalmente al puerto de destino HTTP (o FTP). Si también le interesa analizar otros puertos, habrá que asignar reglas equivalentes para redirigir los paquetes respectivos.

Recuerde que el instalador muestra por defecto todos los pasos que va a realizar y también crea una copia de seguridad de la configuración existente para que pueda ser restaurada más adelante si llega a ser necesario. Los pasos detallados de la utilidad de instalación para todos los escenarios posibles se describen en el apéndice A de este documento.

5.2. Configuración manual de proxy HTTP

La configuración manual de proxy (ver imagen 5-2) se caracteriza por especificar en forma explícita la dirección y el puerto atendidos por el proxy padre en la configuración del cliente que utiliza el proxy.

Imagen 5-2. Esquema de ESET Gateway Security con un proxy configurado manualmente.



En este caso, el servidor proxy en general modifica los pedidos y/o respuestas transmitidos, es decir, actúa de manera no transparente. El soporte para proxy de configuración manual de **esets_http** fue probado con una amplia variedad de los clientes más comunes, por ejemplo, los proxy caché (Squid Proxy Cache, SafeSquid), y los navegadores web (Mozilla Firefox, Opera, Netscape, Konqueror). En líneas generales, cada cliente HTTP que utiliza la configuración manual del proxy padre colaborará con el módulo **esets_http**. En la sección siguiente describimos la configuración manual de proxy de **esets_http** para Mozilla Firefox y para Squid Web Proxy Cache, que son las aplicaciones más comunes para clientes HTTP.

5.2.1. Configuración manual de proxy para Mozilla Firefox

La configuración manual de proxy HTTP para **esets_http** con Mozilla Firefox corresponde, en líneas generales, al sector izquierdo de la imagen 5-2.

Recuerde que esta configuración le permite instalar ESET Gateway Security en cualquier lugar dentro de la red local incluyendo el servidor de puerta de enlace así como la computadora del cliente.

En el siguiente ejemplo configuraremos **esets_http** para que atienda el puerto 8080 de la computadora cuya dirección IP de red local es 192.168.1.10, especificando los siguientes parámetros dentro de la sección [http] del *archivo de configuración* principal de *ESETS:*

```
agent_enabled = yes
listen_addr = ”192.168.1.10”
listen_port = 8080
```

Recuerde que el parámetro 'listen_addr' también puede configurarse como el nombre del host visible desde la red local.

Si desea configurar Mozilla para que utilice **esets_http**, deberá seleccionar el menú de edición 'Edit' en la barra del menú y luego las preferencias 'Preferences' (en versiones anteriores de Mozilla, habrá que seleccionar el menú de herramientas 'Tools' y luego las opciones 'Options'). Luego seleccione la configuración de conexión 'Connection settings', que encontrará bajo la sección de configuración general 'General', y elija la opción de configuración manual de proxy 'Manual Proxy

Configuration'. Finalmente habrá que completar los campos de 'HTTP Proxy' con el nombre del host (o su dirección IP) y el puerto 'Port' correspondiente con el puerto atendido por **esets_http** (en este ejemplo se especificará la dirección IP '192.168.1.10' y el puerto 8080). Para que se active la configuración recién creada, reinicie el *daemon* de *ESETS*.

Es importante tener en cuenta que esta configuración no es la más apropiada para redes con un gran número de computadoras de usuarios. La razón es que en este caso el caché HTTP (si hay uno) está presente sólo en el cliente, por lo que el mismo objeto inicial se analiza varias veces si es solicitado por diferentes clientes.

5.2.2. Configuración manual de proxy para Squid Web Proxy Cache

La configuración manual de proxy HTTP para **esets_http** con Squid Web Proxy Cache corresponde, en líneas generales, al sector derecho de la imagen 5-2.

La diferencia más significativa con las demás configuraciones descriptas hasta el momento es que ESET Gateway Security se instala en el puerto de enlace HTTP entre el proxy caché (Squid Web Proxy, en este ejemplo) e Internet. Por lo tanto, todas las respuestas HTTP que ingresan a la red primero son analizadas para detectar infiltraciones y luego son almacenadas en el caché correspondiente de red, es decir, todos los objetos iniciales que fueron solicitados una vez y que están presentes dentro de un proxy caché ya fueron analizados contra virus y no requieren análisis adicionales cuando son solicitados nuevamente.

En el siguiente ejemplo configuraremos **esets_http** para que atienda el puerto 8080 del servidor de puerta de enlace cuya dirección IP de red local es 192.168.1.10, especificando los siguientes parámetros dentro de la sección [http] del *archivo de configuración* de *ESETS:*

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8080
```

Recuerde que el parámetro 'listen_addr' puede configurarse como el nombre del host visible desde la red local o también puede usarse la dirección 0.0.0.0 para permitir que **esets_http** atienda todas las interfaces. En el último caso hay que tomar precauciones ya que los usuarios ajenos a la red local también tienen acceso al analizador de virus HTTP a menos que se tomen medidas de seguridad adicionales para prevenirlo.

Si desea configurar Squid para que utilice **esets_http** como proxy padre, deberá insertar las siguientes líneas en el archivo de configuración de Squid (/etc/squid/squid.conf):

```
cache_peer 192.168.1.10 parent 8080 0 no-query default
acl all src 0.0.0.0/0.0.0.0
never_direct allow all
```

Al agregar estas líneas a la configuración, Squid usará HTTP proxy para atender la dirección IP 192.168.1.10 en el puerto 8080 como proxy padre. Todos los pedidos procesados por Squid serán enviados a este destino. Las demás líneas de comando definen el comportamiento de Squid para enviar notificaciones de error en caso de que el proxy padre no esté funcionando o no se pueda localizar. Existe una configuración alternativa de Squid para que intente realizar conexiones directas cuando el proxy padre no se puede encontrar. En este caso, los parámetros que habrá que insertar en el archivo de configuración de Squid son los siguientes:

```
cache_peer 192.168.1.10 parent 8080 0 no-query
prefer_direct off
```

Para que se active la configuración recién creada, reinicie el *daemon* de *ESETS*.

5.3. Manejo de Grandes Objetos HTTP

Bajo condiciones normales, **esets_http** maneja cada objeto transferido de manera que el objeto primero se envía desde el servidor HTTP (o usuario) a **esets_http**, en segundo lugar se analiza para detectar infiltraciones y por último se transfiere al usuario HTTP (o servidor, respectivamente). En cuanto a los archivos grandes (grandes objetos cuyo tiempo de transferencia excede el tiempo de espera definido por el parámetro lo_timeout), éste no es un escenario adecuado, ya que el tiempo de espera del cliente e incluso la impaciencia del usuario pueden provocar la interrupción o cancelación de la transferencia del objeto. En consecuencia, deben implementarse otros métodos para procesar los grandes objetos.

5.3.1. Método de análisis diferido

El sistema **esets_http** implementa el método de análisis diferido estándar para el manejo de archivos grandes. Esto significa que, si el objeto transferido es demasiado grande, **esets_http** empieza a enviar el objeto en forma transparente a un punto de llegada HTTP disponible (usuario o servidor). Cuando la última parte del objeto llega a **esets_http**, el objeto es analizado para detectar infiltraciones. Si se detecta que el objeto está infectado, la última parte de él (para la versión actual de ESET Gateway Security, la última parte son los últimos 4KB de los datos del objeto) no será enviada al punto de llegada disponible y la conexión con dicho punto de llegada será interrumpida. Al mismo tiempo se enviará una notificación al administrador de la Puerta de Enlace con la información relevante sobre la transferencia de un archivo peligroso. Recuerde que la notificación sólo será enviada en el caso de que la transferencia de datos se realice desde el servidor al usuario. En este caso, el URL del objeto inicial se almacena en el caché de **esets_http** para bloquear nuevas transferencias si se vuelve a solicitar.

En este punto nos gustaría destacar que la técnica de análisis diferido explicada arriba presenta un riesgo potencial para la computadora cuyo cliente solicitó el archivo de tamaño grande por primera vez. El riesgo se debe a que, a pesar de que la transferencia de datos del objeto infectado no se haya completado, ciertas partes de los datos transferidos pueden contener código malicioso ejecutable. Por eso ESET desarrolló una reforma para el método de análisis diferido llamada técnica de análisis parcial.

5.3.2. Técnica de análisis parcial

La técnica de análisis parcial fue desarrollada para salvaguardar el método de análisis diferido. El funcionamiento básico de la técnica de análisis parcial se basa en la noción de que el tiempo requerido para analizar objetos grandes es insignificante comparado con el tiempo total para procesar el objeto. Esta condición se cumple en el caso de la transferencia HTTP de grandes objetos, donde el tiempo requerido para la transferencia es considerablemente mayor que el del análisis para detectar infiltraciones. Esta apreciación nos permite realizar más de un análisis durante la transferencia de grandes objetos.

Una vez que se habilita el parámetro `lo_partscan_enabled` en la sección [http] del *archivo de configuración* de *ESETS*, los objetos grandes son analizados para detectar infiltraciones durante su transferencia en intervalos predefinidos y los datos analizados son enviados al punto de llegada disponible (es decir, al usuario o al servidor). Con este método no es posible que lleguen infiltraciones a la computadora cuyo usuario solicitó el objeto infectado de gran tamaño porque se garantiza que cada porción de los datos enviados es segura.

Se ha comprobado que en circunstancias normales (cuando la velocidad de conexión de la Puerta de Enlace de red local es mayor que la velocidad de conexión de la Puerta de Enlace a Internet) el tiempo requerido para procesar la transferencia de grandes objetos con la técnica de análisis parcial es aproximadamente el mismo que el requerido al usar sólo el método de análisis diferido estándar.

5.4. Filtro *plugin* de *ESETS* para SafeSquid Proxy Cache

En las secciones anteriores hemos descripto la integración de ESET Gateway Security con los servicios HTTP y FTP de Puerta de Enlace de Internet usando **esets_http** y **esets_ftp.** Aunque los métodos mencionados se pueden aplicar para los clientes más comunes, entre los que se encuentra el conocido programa proxy para filtrar contenidos de Internet - SafeSquid (http://www.safesquid.com), para este caso en particular, ESET Gateway Security ofrece una forma alternativa para proteger los servicios de Puerta de Enlace usando el módulo **esets_ssfi.so**, desarrollado con este propósito.

5.4.1. Pautas generales de uso

El módulo **esets_ssfi.so** es un *plugin* cuyo objetivo es acceder a todos los objetos procesados por el proxy caché SafeSquid usando una interfaz especial desarrollada por el personal de SafeSquid con dicha finalidad. Cuando el *plugin* accede al objeto, éste es analizado por el *daemon* de *ESETS*. Si el objeto está infectado, SafeSquid lo bloquea y a cambio envía un página con una plantilla predeterminada. Recuerde que **esets_ssfi.so** es soportado por las versiones 4.0.4.2 y superiores de SafeSquid Advanced.

5.4.2. Instalación y configuración

En la siguiente explicación suponemos que SafeSquid está instalado en el directorio '/opt/safesquid'. Para integrar el módulo, deberá crear accesos desde el directorio de módulos de SafeSquid a las ubicaciones de instalación apropiadas del paquete de ESET Gateway Security.

```
ln -s @LIBDIR@/ssfi/esets_ssfi.so /opt/safesquid/modules/esets_ssfi.so
ln -s @LIBDIR@/ssfi/esets_ssfi.xml /opt/safesquid/modules/esets_ssfi.xml
```

No obstante, una vez que la instalación del *plugin* SafeSquid esté lista, todavía habrá que hacer ciertos retoques finales en la configuración de SafeSquid. A continuación configuraremos SafeSquid para utilizar las plantillas predeterminadas de *ESETS,* que bloquearán los objetos en caso de que estén infectados (o no puedan ser analizados).

Ingrese a la interfaz de administración de red de SafeSquid (SafeSquid Web Administration Interface), seleccione el menú 'Config' de la página principal de la interfaz y vaya leyendo las secciones que aparecen en 'Select a Section to Configure' hasta encontrar la sección 'ESET Gateway Security'. Luego ingrese las definiciones nuevas de las plantillas, presione 'Add' en la parte inferior de la sección 'ESET Gateway Security' y defina los siguientes parámetros en la lista emergente:

```
Comment: ESET Gateway Security blocking templates
Profiles: antivirus
Infected template: esets_infected
Not scanned template: esets_not_scanned
```

Después de haber completado y confirmado la lista de plantillas, abra la página 'Templates' del menú 'Config'. Allí encontrará el parámetro 'Path' que define la ruta al directorio de plantillas de SafeSquid (de ahora en más, daremos por sentado que el parámetro es '/opt/safesquid/templates'). Verifique que exista el directorio apropiado, de lo contrario, créelo. Para acceder a las plantillas predeterminadas de *ESETS* desde este directorio, deberá crear los accesos correspondientes usando las siguientes líneas de comando *shell*:

```
ln -s @LIBDIR/ssfi/templates/ssfi_infected.html /opt/safesquid/ssfi_infected.html
ln -s @LIBDIR/ssfi/templates/ssfi_not_scanned.html /opt/safesquid/ssfi_not_scanned.html
```

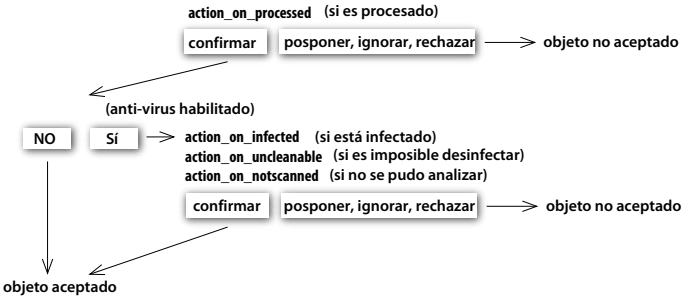
Capítulo 6:

Mecanismos importantes de ESET Gateway Security

6.1. Política para el manejo de Objetos

La Política para el Manejo de Objetos (ver imagen 6-1) es un mecanismo que permite tomar decisiones sobre los objetos analizados según el estado de su análisis. El mecanismo se basa en las opciones de configuración de las acciones que se deberán realizar ('action_on_processed': si es procesado, 'action_on_infected': si está infectado, 'action_on_uncleanable': si es imposible desinfectar, 'action_on_notscanned': si no se pudo analizar), además de la opción de configuración que habilita el Anti-Virus ('av_enabled').
Para mayor información sobre las opciones, consulte la página del manual esets.cfg(5).

Imagen 6-1. Esquema del mecanismo de la Política para el Manejo de Objetos.



Cada objeto primero se maneja según la opción de configuración 'action_on_processed' (si es procesado). Si se elige 'accept' (confirmar), el destino del objeto dependerá del estado de la opción de configuración 'av_enabled' (anti-virus habilitado). Cuando se habilita 'av_enabled', se procede al análisis del objeto para detectar infiltraciones y se toman en cuenta las opciones de configuración 'action_on_infected' (si está infectado), 'action_on_uncleanable' (si es imposible desinfectar) y 'action_on_notscanned' (si no se pudo analizar) para realizar las acciones pertinentes. Si se elige la acción 'accept' (confirmar) como respuesta a cualquiera de las tres opciones anteriores o la opción 'av_enabled' está deshabilitada, se permite el acceso al objeto; de lo contrario, el objeto se bloquea.

6.2. Configuración Específica de Usuario

El producto implementa el mecanismo de Configuración Específica de Usuario para otorgarle practicidad al administrador por medio de una mayor libertad de configuración. El mecanismo permite definir los parámetros de los análisis efectuados por el anti-virus *ESETS* en forma selectiva para la identificación del usuario/servidor.

Recuerde que podrá encontrar una descripción más detallada de esta función en la página del manual esets.cfg(5) y en las demás páginas a las que allí se hace referencia. Por lo tanto, en esta sección sólo daremos un ejemplo conciso sobre la configuración específica de usuario.

En el caso de que usemos **esets_http** para controlar el tráfico HTTP en el puerto 8080 del servidor de puerta de enlace con la dirección IP local de red 192.168.1.10, la configuración del módulo depende de la sección de configuración [http] en el *archivo de configuración* de *ESETS*. La sección es la siguiente:

```
[http]
agent_enabled = yes
listen_addr = "192.168.1.10"
```

```
listen_port = 8080
action_on_processed = accept
```

Para establecer la configuración de los parámetros individuales hay que definir el parámetro 'user_config' ingresando la ruta al archivo de configuración especial donde se guardará la configuración individual. En el siguiente ejemplo hacemos referencia al archivo de configuración especial 'esets_http_spec.cfg' ubicado dentro del *directorio de configuración* de *ESETS*.

```
[http]
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8080
action_on_processed = accept
user_config = "esets_http_spec.cfg"
```

Ona vez que se realizó la configuración especial a la que se hace referencia dentro de la sección [http], debemos crear el archivo en el *directorio de configuración de ESETS* y proporcionarle una configuración individual apropiada. El siguiente ejemplo muestra la configuración individual del parámetro 'action_on_processed' para el usuario cuya dirección de IP es 192.168.1.40.

```
[|192.168.1.40]
action_on_processed = reject
```

El nombre de la sección del encabezado contiene la identificación del usuario HTTP para el cual se ha creado una configuración individual. A continuación, el cuerpo de la sección contiene parámetros individuales específicos para ese usuario. De esta manera, con la configuración personalizada, el tráfico HTTP de todos los usuarios de la red local será procesado, es decir, analizado para detectar infiltraciones, con excepción del usuario cuya dirección de IP es 192.168.1.40, que será rechazado, es decir, estará bloqueado.

6.3. Lista negra y lista blanca

En el siguiente ejemplo mostramos cómo crear la lista negra y la lista blanca para **esets_http** configurado para analizar el proxy HTTP. Recuerde que para este propósito utilizaremos el archivo de configuración especial mencionado anteriormente.

Para crear una lista negra que pueda ser utilizada por **esets_http** , debemos crear la siguiente sección grupal dentro del archivo de configuración especial 'esets_http_spec.cfg' presentado en la sección anterior.

```
[black-list]
action_on_processed = reject
```

El próximo paso consiste en agregar un servidor HTTP al grupo de la lista negra 'black-list'. Para ello debemos crear la sección especial

```
[aaa.bbb.ccc.ddd]
parent_id = "black-list"
```

donde 'aaa.bbb.ccc.ddd' es la dirección IP del servidor agregado a la lista negra 'black-list'. Recuerde que con esta configuración todo el tráfico HTTP referente al servidor especificado será rechazado, es decir, el servidor estará bloqueado.

Si queremos crear la lista blanca 'white-list' que pueda ser utilizada por **esets_http**, debemos crear la siguiente sección grupal dentro del archivo de configuración especial 'esets_http_spec.cfg' presentado en la sección anterior.

```
[white-list]
action_on_processed = accept
av_enabled = no
```

Como es de esperar, se aceptarán los servidores HTTP agregados a esta lista.

6.4. Sistema de Envío de Muestras

El sistema de envío de muestras es una tecnología inteligente ThreatSense.NET que permite detectar los objetos infectados descubiertos por el método de heurística avanzada y enviarlos al servidor del sistema de envío de muestras. Todas las muestras de virus que ingresan en el sistema de envío de muestras serán procesadas por el equipo del departamento de laboratorio de virus de ESET y, si es necesario, agregadas a la base de datos de virus de ESET.

NOTA: DE ACUERDO A NUESTRO CONTRATO DE LICENCIA, AL HABILITAR EL SISTEMA DE ENVÍO DE MUESTRAS UD. ACCEDE A QUE LA COMPUTADORA Y/O PLATAFORMA SOBRE LA QUE ESETS_DAEMON ESTÁ INSTALADO RECOPILE INFORMACIÓN (QUE PUEDE INCLUIR INFORMACIÓN PERSONAL SOBRE UD. Y/O EL USUSARIO DE LA COMPUTADORA) Y MUESTRAS DE VIRUS U OTRAS AMENAZAS DETECTADAS Y LAS ENVÍE A NUESTRO LABORATORIO DE VIRUS. ESTA OPCIÓN SE ENCUENTRA POR DEFECTO DESABILITADA. SÓLO USAREMOS LA INFORMACIÓN Y DATOS RECIBIDOS PARA ESTUDIAR LA AMENAZA Y DAREMOS PASOS RAZONABLES PARA PRESERVAR LA CONFIDENCIALIDAD DE DICHA INFORMACIÓN.

Para activar el sistema de envío de muestras, debe iniciarse el caché del sistema de envío de muestras. Esto se logra habilitando la opción de configuración 'samples_enabled' en la sección [global] del *archivo de configuración* de *ESETS*. Para activar el proceso de envío de muestras a los servidores del laboratorio de virus de ESET también es necesario habilitar el parámetro 'samples_send_enabled' en la misma sección.

El usuario decidirá si desea enviar información suplementaria opcional al equipo del laboratorio de virus de ESET, usando las opciones de configuración 'samples_provider_mail' y/o 'samples_provider_country'. Esta información nos resultará útil para formarnos una visión global sobre la propagación de infiltraciones a través de Internet.

Para obtener información detallada sobre el Sistema de Envío de Muestras, consulte la página del manual esets_daemon(8).

Capítulo 7:

Actualización del sistema de Seguridad de ESET

7.1. Utilidad de actualización de *ESETS*

Para que ESET Gateway Security permanezca efectivo, es necesario mantener al día la base de datos de virus. La utilidad de actualización **esets_update** fue desarrollada con dicho propósito (consulte la página del manual esets_update(8) para más detalles). Si desea activar la actualización, debe definir las opciones de configuración 'username' (nombre de usuario) y 'password' (contraseña) en la sección [update] del *archivo de configuración* de *ESETS*. Recuerde que, en caso de que su acceso a Internet se realice por intermedio de un HTTP proxy, además deberá especificar las opciones de configuración adicionales de dirección: 'proxy_addr', puerto: 'proxy_port' y, en forma opcional, el nombre de usuario: 'proxy_username' y la contraseña: 'proxy_password' correspondientes. Para realizar una actualización, ingrese el comando:

```
@SBINDIR@/esets_update
```

Para otorgarle al usuario la mayor seguridad, el equipo de ESET recopila las definiciones de virus en forma continua de todas partes del mundo. Como los patrones nuevos pueden ser agregados a la base de datos en intervalos muy reducidos, se recomienda realizar las actualizaciones con regularidad. Recuerde que el *daemon* de *ESETS* es capaz de llevar a cabo la actualización periódica del sistema una vez que la opción de configuración 'av_update_period' especificada en la sección [update] del *archivo de configuración* de *ESETS y* el *daemon* se hayan habilitado y estén ejecutándose.

7.2. Descripción del proceso de actualización de *ESETS*

El proceso de actualización consiste en dos partes. Primero se replican todos los módulos relevantes de compilación previa desde el servidor ESET. Los módulos de compilación previa son descargados por defecto dentro del directorio

```
@BASEDIR@/mirror
```

Recuerde que la ruta del directorio de replicación puede modificarse usando la opción de configuración 'mirror_dir' en la sección [update] del *archivo de configuración* de *ESETS*.

Los módulos de *ESETS* se dividen en dos categorías: la categoría motor y la categoría componente. Los módulos de la categoría componente en la actualidad sólo pueden utilizarse con el SO MS Windows. Hoy en día son soportados los siguientes tipos de módulos correspondientes a la categoría motor: módulos de análisis básicos (prefix engine) que contienen bases de datos con firmas de virus, módulos de soporte de ficheros (prefix archs) que soportan varios formatos de ficheros del sistema de archivos, módulos de heurística avanzada (prefix advheur) que contienen la implementación del método de heurística avanzada para detección de virus y gusanos, módulos de análisis de gusanos en archivos comprimidos (prefix pwscan) utilizados en el SO MS Windows, módulos para utilidades (prefix utilmod) utilizados en el SO MS Windows y módulos para soporte de tecnología ThreatSense.NET (prefix charon). Estos módulos son imprescindibles, en consecuencia todos ellos son descargados automáticamente durante cada proceso de descarga. Por el contrario, los módulos de la categoría componente dependen de la plataforma y de la configuración del idioma, por lo tanto la descarga de los módulos de la categoría componente es opcional.

Luego de la descarga de los módulos de compilación previa, también se crea el archivo 'update.ver' en el directorio de réplica. Este archivo contiene la información sobre los módulos guardados actualmente en la réplica recién creada. La réplica recién creada sirve entonces como servidor completamente funcional de descarga de módulos y se puede utilizar para crear nuevas réplicas subordinadas; sin embargo, para ello será necesario cumplir con algunas condiciones adicionales. En primer lugar, debe haber un servidor HTTP instalado en la computadora desde donde los módulos puedan ser descargados. En segundo lugar, los módulos que sean descargados por otras computadoras deberán ser ubicados en la ruta de directorio:

```
/http-serv-base-path/nod_upd
```

donde 'http-serv-base-path' es una ruta al directorio del servidor HTTP básica, ya que constituye el primer lugar donde la utilidad de actualización busca los módulos.

La segunda parte del proceso de actualización consiste en la compilación de módulos que el programa de análisis de ESET Gateway Security carga desde los módulos que se encuentran guardados en la réplica local. Los módulos de *ESETS* que suelen crearse son los siguientes: un módulo base (nod32.000), un módulo para soporte de archivos (nod32.002), un módulo de heurística avanzada (nod32.003), un módulo de análisis de gusanos en archivos comprimidos (nod32.004), un módulo para utilidades de Windows (nod32.005) y un módulo para soporte de la tecnología ThreatSense.NET (nod32.006). Todos los módulos mencionados son creados en el directorio:

```
@BASEDIR@
```

Recuerde que éste es exactamente el mismo directorio desde donde el *daemon* de *ESETS* carga los módulos, por lo tanto puede redefinirse usando la opción de configuración 'base_dir' en la sección [global] (o [update]) del *archivo de configuración* de *ESETS*.

Capítulo 8:

Contáctenos

Estimado usuario, el propósito de esta guía es brindarle la información necesaria sobre la instalación, configuración y mantenimiento de ESET Gateway Security. No obstante, la tarea de redactar un manual es un proceso que nunca se finaliza. Siempre quedarán temas que podrían haber sido explicados con mayor detalle o que directamente se han excluido. Por lo tanto, si encuentra omisiones o inconsistencias en este documento, por favor, informe el problema a nuestro centro de atención:

http://www.eset.com/support

Deseamos poder ayudarlo a resolver cualquier tipo de problema sobre el producto.

Apéndice A.
Descripción del proceso de configuración de *ESETS*

A.1. Configuración de *ESETS* para analizar comunicaciones HTTP - modo transparente

El análisis de la comunicación HTTP se lleva a cabo usando el *daemon* **esets_http**. En la sección [http] del *archivo de configuración* de *ESETS* ingrese los siguientes parámetros:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8080
```

donde 'listen_addr' es la dirección de la interfaz de red local llamada if0. Luego reinicie el *daemon* de *ESETS*. El siguiente paso consiste en redirigir todos los pedidos HTTP a **esets_http**. En el caso del filtrador del protocolo IP provisto por ipchains, la regla apropiada es:

```
ipchains -A INPUT -p tcp -i if0 --dport 80 -j REDIRECT 8080
```

Si dicho mecanismo esá provisto por la herramienta administrativa de iptables, la regla es:

```
iptables -t nat -A PREROUTING -p tcp -i if0 \
  --dport 80 -j REDIRECT --to-ports 8080
```

y en caso de que se utilice la herramienta ipfw (con el SO BSD), la regla es la siguiente:

```
ipfw add fwd 192.168.1.10,8080 tcp from any to any 80 via if0 in
```

A.2. Configuración de *ESETS* para analizar comunicaciones FTP - modo transparente

El análisis de la comunicación FTP se lleva a cabo usando el *daemon* **esets_ftp**. En la sección [ftp] del *archivo de configuración* de *ESETS* ingrese los siguientes parámetros:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 2121
```

donde 'listen_addr' es la dirección de la interfaz de red local llamada if0. Luego reinicie el *daemon* de *ESETS*. El siguiente paso consiste en redirigir todos los pedidos FTP a **esets_ftp**. En el caso del filtrador del protocolo IP provisto por ipchains, la regla apropiada es:

```
ipchains -A INPUT -p tcp -i if0 --dport 21 -j REDIRECT 2121
```

Si dicho mecanismo esá provisto por la herramienta administrativa de iptables, la regla es:

```
iptables -t nat -A PREROUTING -p tcp -i if0 \
  --dport 21 -j REDIRECT --to-ports 2121
```

y en caso de que se utilice la herramienta ipfw (con el SO BSD), la regla es la siguiente:

```
ipfw add fwd 192.168.1.10,2121 tcp from any to any 21 via if0 in
```

Apéndice B. Licencia de PHP

La Licencia de PHP, versión 3.01 Copyright (c) 1999 - 2006 The PHP Group. Todos los derechos reservados. La redistribución y el uso en formas fuente y/o binaria, con o sin modificaciones, están permitidas siempre que se cumplan las siguientes condiciones:

1. Las redistribuciones de código fuente deben retener la advertencia de derechos de autor expresada arriba, esta lista de condiciones y el descargo expresado a continuación.

2. La redistribución en formato binario debe reproducir la advertencia de derechos de autor expresada arriba, esta lista de condiciones y el descargo expresado a continuación en la documentación y/u otros materiales que se proporcionen junto con la distribución.

3. El nombre "PHP" no debe utilizarse para respaldar o promocionar productos derivados de este programa sin el permiso previo por escrito. Para conseguir el permiso escrito, por favor, póngase en contacto con group@php.net.

4. Los productos derivados de este programa no podrán llamarse "PHP", ni contener las siglas "PHP" en su nombre, sin el permiso por escrito de group@php.net. Ud. podrá indicar que su programa funciona en conjunto con PHP llamándolo "X para PHP" en lugar de llamarlo "X de PHP" o "XPHP"

5. El grupo de PHP (PHP Group) puede publicar versiones nuevas o modificadas de la licencia con cierta frecuencia. Cada versión tendrá un número de versión diferente. Una vez que un código cubierto se haya publicado bajo una versión particular de la licencia, Ud. podrá continuar usándolo bajo los términos de dicha versión. También podrá optar por utilizar el código cubierto bajo los términos de cualquiera de las versiones posteriores de la licencia, publicadas por el grupo de PHP. Ninguna persona ajena al grupo PHP está autorizada a modificar los términos aplicables al código cubierto creados según esta Licencia.

6. Las redistribuciones en cualquier forma deben incluir la siguiente mención "Este producto utiliza el programa PHP, disponible en forma gratuita en la página web: <http://www.php.net/software/>".

ESTE PROGRAMA SE PROPORCIONA A TRAVÉS DEL EQUIPO DE DESARROLLO DE PHP "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA INCLUYENDO, PERO SIN LIMITACIÓN, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD Y ADECUACIÓN PARA UN PROPÓSITO EN PARTICULAR. EN NINGÚN CASO EL EQUIPO DE DESARROLLO DE PHP O SUS COLABORADORES SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO SIN LIMITACIÓN, LA PROCURACIÓN O SUSTITUCIÓN DE BIENES O SERVICIOS; PÉRDIDA DE USO, DATOS O BENEFICIOS; O INTERRUPCIÓN DE NEGOCIO) CAUSADO SIN EMBARGO Y EN CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA EN CONTRATO, RESPONSABILIDAD ESTRICTA O EXTRACONTRACTURAL (INCLUYENDO LA NEGLIGENCIA U OTRAS) EMERGENTES DEL USO DE ESTE PROGRAMA, INCLUSO SI SE ADVIERTE SOBRE LA POSIBILIDAD DE DICHOS DAÑOS.