

# ESET

# Gateway Security

## Manual de instalación y guía del usuario

Versión 3.0 - Mayo de 2009



Protegemos su mundo digital



[www.eset.es](http://www.eset.es)

# ESET Gateway Security

**Copyright © 2009 por ESET, spol. s r.o.**

ESET Gateway Security ha sido desarrollado por ESET, spol. s r.o.  
Para más información, visite [www.eset.es](http://www.eset.es).

Todos los derechos reservados.

Este documento no puede ser reproducido, guardado en un sistema automatizado de obtención de documentos, ni transmitido, total o parcialmente, bajo ningún formato ni medio electrónico o mecánico, para ningún propósito sin el consentimiento escrito del autor.

La información de este documento está sujeta a cambios sin previa advertencia.

Esta guía se actualiza frecuentemente para reflejar modificaciones en el producto.

Este producto ha sido desarrollado con PHP. Esta aplicación gratuita está disponible en <http://php.net/software/>.

Última revisión en inglés: febrero de 2009.

Traducción y adaptación al español: Ontinet.com, S.L., mayo de 2009.

<b>1. Introducción</b>	<b>5</b>
1.1 Requisitos del sistema	6
<b>2. Instalación de ESET Gateway Security</b>	<b>7</b>
<b>3. Arquitectura de ESET Gateway Security</b>	<b>9</b>
<b>4. Integración con los servicios de Internet Gateway</b>	<b>12</b>
4.1 Configuración de un servidor proxy transparente HTTP / FTP	12
4.2 Configuración de un servidor proxy manual HTTP / FTP	14
4.2.1 Configuración del proxy manual de Mozilla Firefox	15
4.2.2 Configuración del proxy manual Squid Web	17
4.3 Configuración del protocolo de adaptación de contenidos de Internet	19
4.4 Tratamiento de objetos HTTP de gran tamaño	21
4.4.1 Método de análisis diferido	21
4.3.3 Técnica de análisis parcial	22
4.5 Filtro ESET para SafeSquid	23
4.5.1 Principio operativo	23
4.5.2 Instalación y configuración	23
<b>5. Mecanismos principales de ESET Gateway Security</b>	<b>26</b>
5.1 Directivas de manejo de objetos	26
5.2 Configuración específica del usuario	27
5.3 Lista negra y lista blanca	29
5.4 Sistema de envío de muestras	30
5.5 Interfaz web	31
5.6 Administración remota	32
<b>6. Sistema de actualización de ESET File Security</b>	<b>33</b>
6.1 Herramienta de actualización de ESET File Security	33
6.2 Descripción del proceso de actualización	34
6.3 Proceso demonio del servidor local de actualizaciones HTTP	35
<b>7. Glosario</b>	<b>36</b>
<b>8. Contacto</b>	<b>38</b>

<b>Apéndice A: Descripción del proceso de configuración de ESET Gateway Security</b>	<b>39</b>
A.1 Configuración de ESET Gateway Security para analizar las comunicaciones HTTP en modo transparente	39
A.2 Configuración de ESET Gateway Security para analizar las comunicaciones FTP en modo transparente	40
A.3 Configuración de ESET Gateway Security para analizar los mensajes ICAP HTTP encapsulados	41
<b>Apéndice B: Licencia PHP</b>	<b>42</b>

# 1. Introducción

Apreciado usuario, gracias por adquirir **ESET Gateway Security**, la mejor solución de seguridad para los sistemas operativos Linux, BSD y Solaris.

Pronto comprobará que la tecnología avanzada del motor de análisis **ESET**, proporciona una velocidad de exploración y tasas de detección insuperables, con un consumo de recursos mínimo. Esto convierte a **ESET Gateway Security** en la elección ideal para los servidores en entornos de trabajo Linux, BSD o Solaris.

Características principales de **ESET Gateway Security**:

- Elevada tasa de detección y máxima velocidad de análisis, gracias a los algoritmos del motor antivirus **ESET**.
- Diseño especialmente desarrollado para ejecutarse en ordenadores con uno o varios procesadores.
- Heurística avanzada única para detectar gusanos y puertas traseras de sistemas Windows de 32 bits.
- Sistema de descompresión de archivos integrado, que permite examinar objetos empaquetados sin la necesidad de recurrir a una aplicación externa.
- Arquitectura basada sobre un proceso demonio que permanece siempre activo (programa residente), y que recibe todas las solicitudes de análisis.
- Ejecución de procesos demonio limitada exclusivamente a cuentas de usuario con privilegios (excepto **esets\_dac**), con el fin de mejorar aún más la seguridad.
- Personalización de configuraciones para cada usuario, equipo cliente o servidor.
- Opción para configurar varios niveles de registro, para obtener información detallada sobre la actividad del sistema y las infiltraciones.
- Interfaz web, intuitiva y simple, que permite configurar y administrar fácilmente el programa y sus licencias.
- Compatibilidad con **ESET Remote Administrator**. Esto permite administrar fácilmente su implementación en redes extensas.
- No es necesario recurrir a librerías o programas externos, excepto **libc**.
- Sistema de configuración de alertas, para enviar avisos a ciertos usuarios específicos, comunicando la detección de una infiltración u otro suceso importante.

## 1.1. Requisitos de sistema

- **Procesador**
  - Arquitectura i386 (Intel® 80386) o AMD64 (x86-64).
  
- **Sistemas operativos**
  - **Linux**  
Con Kernel 2.2.x, 2.4.x o 2.6.x, glibc 2.2.5 o superior.  
Módulo Dazuko kernel 2.0.0 o superior (opcional).
  
  - **FreeBSD**  
Versión 5.x, 6.x o 7.x.  
Módulo Dazuko kernel 2.0.0 o superior (opcional).
  
  - **NetBSD**  
Versión 4.x.
  
  - **Sun Solaris**  
Versión 10 o superior.
  
- **Memoria operativa**
  - 32 MB
  
- **Espacio en disco duro**
  - 25 MB para la instalación.  
Espacio adicional para los archivos temporales

**ESET Gateway Security** tiene el desempeño y la versatilidad que usted espera de una solución basada sobre UNIX.

Cuenta también con la seguridad incomparable de los productos **ESET**, tanto para servidores de oficina pequeños, como para grandes servidores corporativos con miles de usuarios, como los que utilizan los proveedores de Internet (ISP, *Internet Service Provider*).

## 2. Instalación de *ESET Gateway Security*

Al adquirir la licencia de uso de **ESET Gateway Security**, el usuario recibirá un mensaje de correo electrónico que contiene sus datos de autenticación —nombre de usuario y contraseña— y un archivo adjunto con la clave de licencia.

Esta información le permitirá identificarse como cliente, y también acceder a los servidores de **ESET** para descargar el paquete inicial del programa y sus actualizaciones.

**ESET Gateway Security** se distribuye como archivo binario:

**esets.i386.ext.bin**

Donde **ext** es un sufijo que dependerá de la distribución del sistema operativo: **deb** corresponderá a la distribución Debian; **rpm** a las distribuciones Red Hat y SuSE; **tgz** a otras distribuciones de Linux; **fbs5.tgz** corresponderá a FreeBSD 5.xx; **fbs6.tgz** a FreeBSD 6.xx; **nbs4.tgz** a NetBSD 4.xx y **sol10.pkg.gz** corresponderá a Solaris 10.


El formato del nombre del archivo binario para Linux **RSR** es:

**esets-rsr.i386.rpm.bin**

Para instalar o actualizar el producto, siga las instrucciones detalladas a continuación:

1. En la interfaz de comandos, introduzca la instrucción:

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

 En la versión de **ESET Gateway Security** para Linux **RSR**, el comando a utilizar es el siguiente:

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

2. Después de ejecutar el comando correspondiente a la versión de Linux instalada, aparecerá en pantalla el **Contrato de licencia** solicitando la conformidad del usuario para continuar el proceso.
3. Una vez leído y aceptado el **Contrato de licencia**, se visualizará información relevante sobre el proceso de instalación, desinstalación o actualización, y el paquete de instalación se ubicará en el directorio en el que se esté trabajando en ese momento.
4. Cuando finaliza la instalación del producto, podrá verificar que el servicio principal de **ESET Gateway Security** está activo, mediante el comando correspondiente al sistema operativo del equipo:
  - o En sistemas operativos Linux:  
**ps -C esets\_daemon**
  - o En sistemas operativos BSD:  
**ps -ax | grep esets\_daemon**
  - o En sistemas operativos Solaris:  
**ps -A | grep esets\_daemon**

Al presionar la tecla **Intro** (*Enter*), se visualizarán los procesos **esets** activos. Si el servicio se está ejecutando correctamente, el mensaje debería mostrar al menos dos procesos demonio (*daemon*), con el siguiente formato:

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

El primero de ellos representa al gestor de procesos e hilos de ejecución del sistema. El segundo representa el proceso de análisis de **esets**.

### 3. Arquitectura de ESET Gateway Security

Una vez instalado **ESET Gateway Security**, es conveniente conocer su estructura para comprender mejor su funcionamiento.

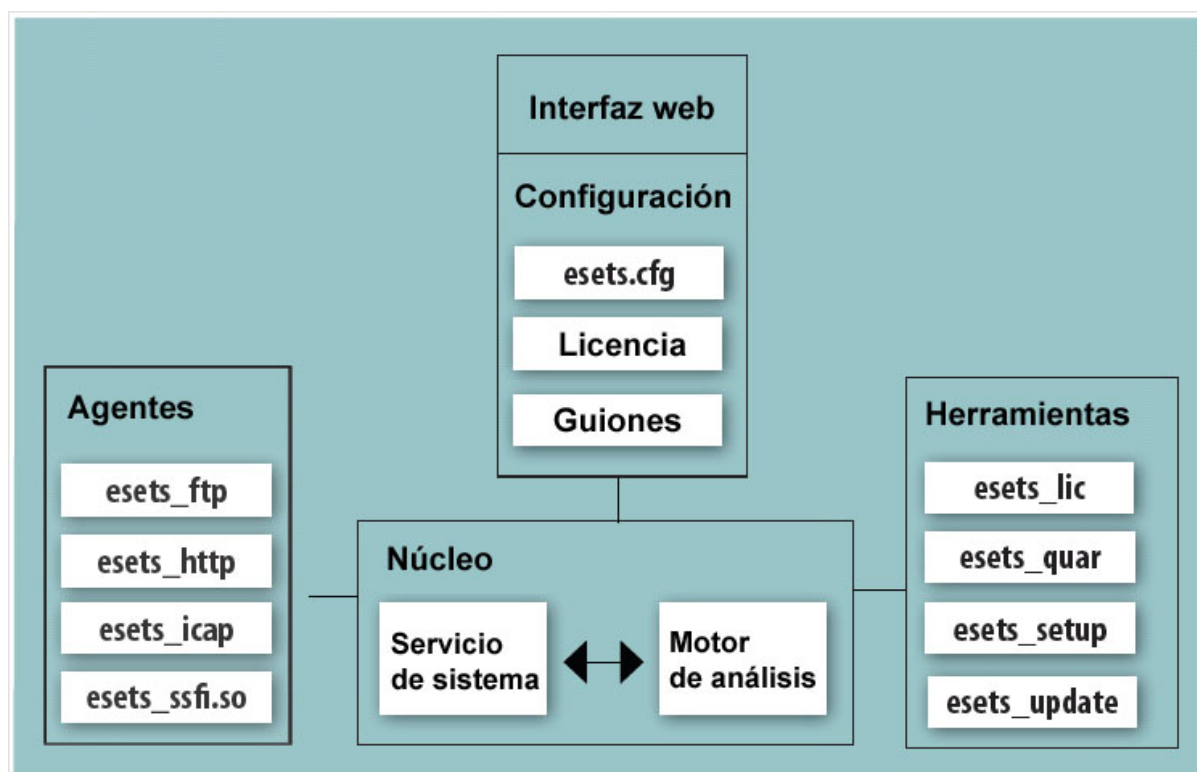


Figura 3.1 - Estructura de *ESET Gateway Security*

El sistema está formado por los siguientes componentes:

- **Núcleo**

El corazón de **ESET Gateway Security** reside en el proceso demonio **esets\_daemon**. Este, utiliza la librería **libesets.so** y los módulos **em00X\_xx.dat** para efectuar tareas básicas del sistema, tales como análisis, mantenimiento del agente de procesos demonio y del sistema de envío de muestras, registros, avisos, etcétera. Para obtener mayor información, consulte la página de manual **esets\_daemon(8)**.

- **Agentes**

El propósito de los módulos agente, es integrar **ESET Gateway Security** a los entornos Linux, BSD y Solaris.

- **Herramientas**

Los módulos de herramientas, permiten una administración simple y efectiva del sistema. Son los responsables de realizar las tareas principales, tales como la administración de licencias, la gestión de la carpeta de cuarentena, y la configuración y actualización del sistema.

- **Configuración**

Para obtener un funcionamiento óptimo del sistema, es fundamental determinar la configuración apropiada.

El resto de este capítulo, está dedicado a explicar todos los componentes relacionados con este punto.

Asimismo, se recomienda estudiar los parámetros del archivo **esets.cfg**, el cual contiene información esencial para la configuración correcta de **ESET Gateway Security**.

Una vez que el producto se ha instalado exitosamente, todos sus componentes de configuración se guardarán en el directorio **@ETCDIR@**, que contiene los siguientes archivos:

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

El archivo de configuración **esets.cfg** es el más importante, ya que controla los aspectos principales del funcionamiento del producto. Está constituido por varias secciones y cada una de ellas presenta diversos parámetros configurables.

Hay una sección global y varias secciones **agente**, cuyos nombres aparecen entre corchetes. Los parámetros de la sección global se utilizan para definir las opciones de configuración del proceso demonio, así como también los valores predeterminados para la configuración del motor de análisis de **ESET Gateway Security**.

En las secciones **agente**, los parámetros definen la configuración de los módulos dedicados a interceptar y preparar los flujos de datos para el análisis.

Es necesario destacar que, más allá de los distintos parámetros utilizados para la configuración del sistema, existen también reglas que rigen la organización del archivo. Para obtener información detallada sobre la manera más efectiva de organizar este archivo, consulte las páginas de manual **esets.cfg(5)** y **esets\_daemon(8)**, así como las páginas de manual de los agentes pertinentes.

- **@ETCDIR@/certs**

En este directorio se guardan los certificados de autenticación utilizados por la interfaz web de **ESET Gateway Security**.

Consulte la página de manual **esets\_wwwi(8)** para más detalles.

- **@ETCDIR@/license**

En este directorio se guardan las claves de licencia de los productos adquiridos por el cliente. Al buscar una clave de licencia válida, el proceso demonio de **ESET Gateway Security** registrará solamente este directorio, a menos que se redefina el parámetro **license\_dir** en el archivo de configuración **esets.cfg**.

- **@ETCDIR@/scripts/license\_warning\_script**

Si en el archivo de configuración **esets.cfg**, se habilita el guión **license\_warning\_script** con el parámetro **license\_warn\_enabled**, este se ejecutará diariamente durante los 30 días anteriores a la expiración de la licencia del producto, enviando un mensaje de correo electrónico al administrador del sistema, advirtiéndole la situación.

- @ETCDIR@/scripts/daemon\_notification\_script

Si en el archivo de configuración **esets.cfg**, se habilita el guión **daemon\_notification\_script** con el parámetro **exec\_script**, este se ejecutará cuando el sistema antivirus detecte una infiltración, enviando un mensaje de correo electrónico al administrador del sistema para darle aviso del acontecimiento.

## 4. Integración con los servicios de Internet Gateway

**ESET Gateway Security** protege los servicios HTTP y FTP de la empresa, contra todo tipo de amenaza informática: virus, gusanos, troyanos, programas espía, falsificación de sitios y demás códigos maliciosos. La expresión **Gateway Server** (Servidor de enlace) se refiere a la capa 3 del modelo OSI (*Open System Interconnect*, Interconexión de sistemas abiertos), correspondiente al nivel de enlace y dirección de datos.

En este capítulo se describe el proceso de integración de **ESET Gateway Security** con los distintos servicios del sistema.

### 4.1 Configuración de un servidor *proxy* transparente HTTP / FTP

La configuración de un *proxy* transparente se basa sobre un mecanismo de dirección estándar.

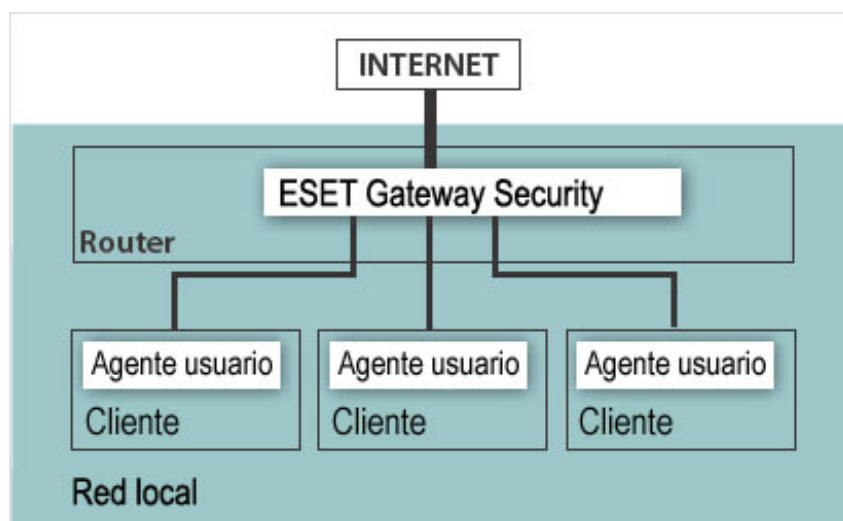


Figura 4.1: Esquema de funcionamiento de **ESET Gateway Security** como *proxy* transparente.

La configuración se va creando progresivamente, a medida que se determinan las tablas de dirección IP en cada equipo cliente de la red local.

Estas tablas se utilizan para definir rutas estáticas hacia el servidor de enlace predeterminado para la red. En una red DHCP (*Dynamic Host Configuration Protocol*, Protocolo de configuración dinámica del equipo anfitrión), esta tarea se realiza automáticamente.

Por lo tanto, todas las comunicaciones HTTP o FTP con servidores externos, son dirigidas por el servidor de enlace de la red, donde debe ser instalado **ESET Gateway Security** con el fin de analizar las comunicaciones en busca de infiltraciones.

Con este propósito, **ESET** ha desarrollado un filtro HTTP o FTP genérico, llamado **esets\_http** o **esets\_ftp**, respectivamente.

Para configurar **ESET Gateway Security** con el objetivo de analizar los mensajes HTTP o FTP distribuidos por el servidor de enlace:

1. Introduzca el comando:

```
/usr/sbin/esets_setup
```

2. Siga las instrucciones del guión.
3. Cuando aparezca la opción **Available installations/un-installations** (Instalaciones / Desinstalaciones disponibles), seleccione **HTTP** o **FTP**.
4. Se activarán las opciones **install/uninstall** (Instalar / Desinstalar). Seleccione **Install** (instalar).

Dicho proceso configurará automáticamente el módulo para permanecer a la escucha, en un puerto predefinido.

También dirigirá los paquetes IP con destino HTTP o FTP originados en la red seleccionada, hacia el puerto analizado por **esets\_http** o **esets\_ftp**.

Esto significa que solo serán analizadas las solicitudes originalmente enviadas hacia un puerto HTTP o FTP. Si desea controlar otros puertos, debe asignar reglas de dirección equivalentes.

De modo predeterminado, el instalador muestra todos los pasos que se llevarán a cabo. También crea una copia de seguridad de la configuración actual, que podrá ser restaurada en cualquier momento.

En el **Apéndice A** encontrará los pasos detallados de la herramienta de instalación, para los distintos escenarios posibles.

## 4.2. Configuración de un servidor *proxy* manual HTTP / FTP

Esta configuración permite definir de forma explícita el agente usuario, para permanecer a la escucha en un puerto y dirección específicos del servidor *proxy* superior.

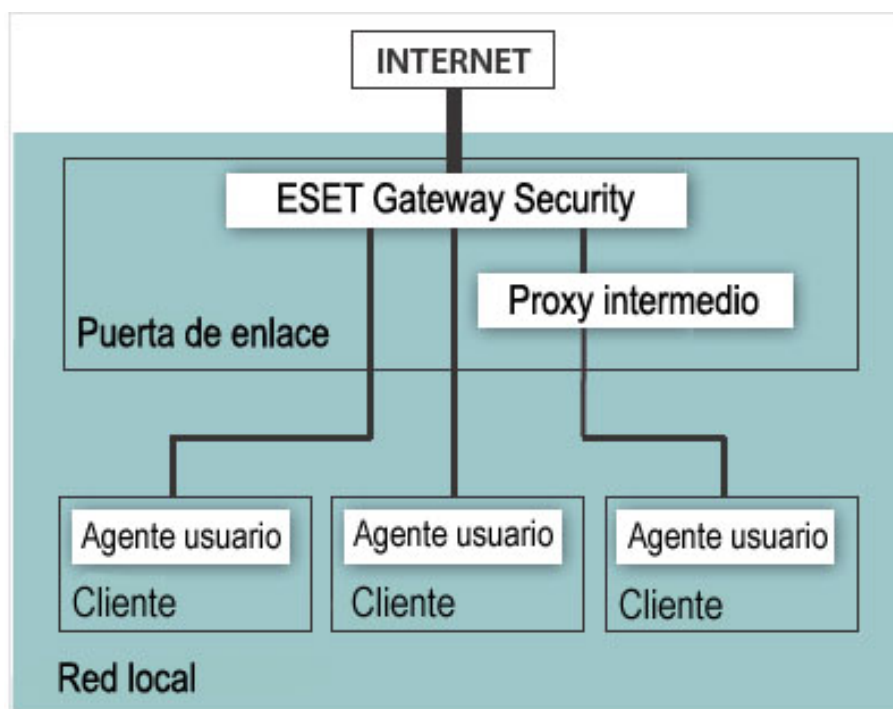


Figura 4.2: Esquema de funcionamiento de ESET Gateway Security como *proxy* manual.

Mediante esta configuración, el servidor *proxy* generalmente modifica las solicitudes o respuestas transferidas, por ejemplo, de forma no transparente.

El *proxy* manual de `esets_http` ha sido probado con una gran variedad de agentes de usuario comunes (por ejemplo, *proxy* intermedios), como Squid Proxy Cache y SafeSquid. También se verificó su funcionamiento con navegadores de red, como Mozilla Firefox, Opera, Netscape y Konqueror.

Por lo general, cualquier agente de usuario HTTP que permita la configuración de un *proxy* manual superior, será compatible con el módulo `esets_http`.

A continuación se describe la configuración de `esets_http` con Mozilla Firefox y Squid Web, dos de los agente de usuario HTTP más comunes.

#### 4.2.1. Configuración del *proxy* manual de Mozilla Firefox

La configuración del *proxy* manual HTTP / FTP de **esets\_http** con Mozilla Firefox, permite instalar **ESET Gateway Security** en cualquier equipo de la red local, incluyendo el servidor de enlace y el ordenador del agente de usuario.

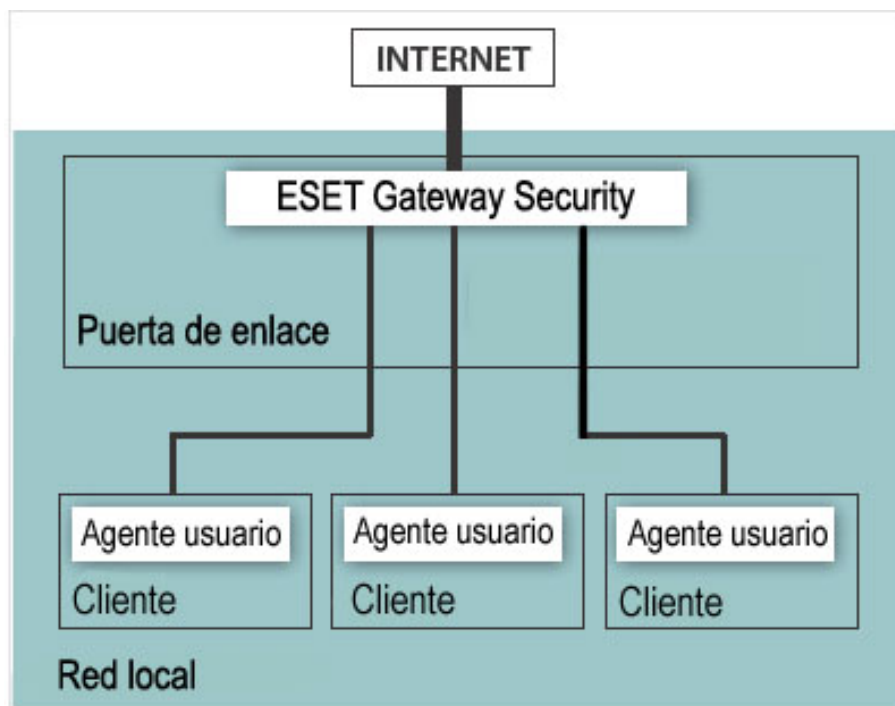


Figura 4.2.1: Configuración de **esets\_http** con Mozilla Firefox.

Como ejemplo, se muestra la configuración de **esets\_http** para permanecer a la escucha en el puerto 8080 de un ordenador, cuya IP local es **192.168.1.10**.

Para ello, en la sección **[http]** del archivo **esets.cfg** se determinaron los siguientes parámetros:

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

El valor del parámetro **listen\_addr** también puede ser el nombre del ordenador anfitrión. Este es visible desde la red local.

Para configurar Firefox con el fin de utilizar **esets\_http**:

1. Abra Mozilla Firefox. En el menú principal, presione **Herramientas** y seleccione **Opciones**.
2. En el menú de la ventana **Opciones**, pulse **Avanzado**.
3. Seleccione la pestaña **Red** y, en la sección **Conexión**, pulse **Configuración....**  
En la ventana **Configuración de conexión**, presione **Configuración manual del proxy**.
4. En el campo **Proxy HTTP**, introduzca el nombre o dirección IP del ordenador anfitrión.  
Complete el campo **Puerto** con el valor que utilizará **esets\_http**.  
En el ejemplo dado, la dirección IP es 192.168.1.10 y el puerto, 8080.
5. Para releer la configuración nueva, debe cargar nuevamente el proceso demonio de **ESET Gateway Security**.

## 4.2.2. Configuración del *proxy* manual Squid Web

En esta sección se describe la configuración del *proxy* manual HTTP / FTP de **esets\_http**, con Squid Web.

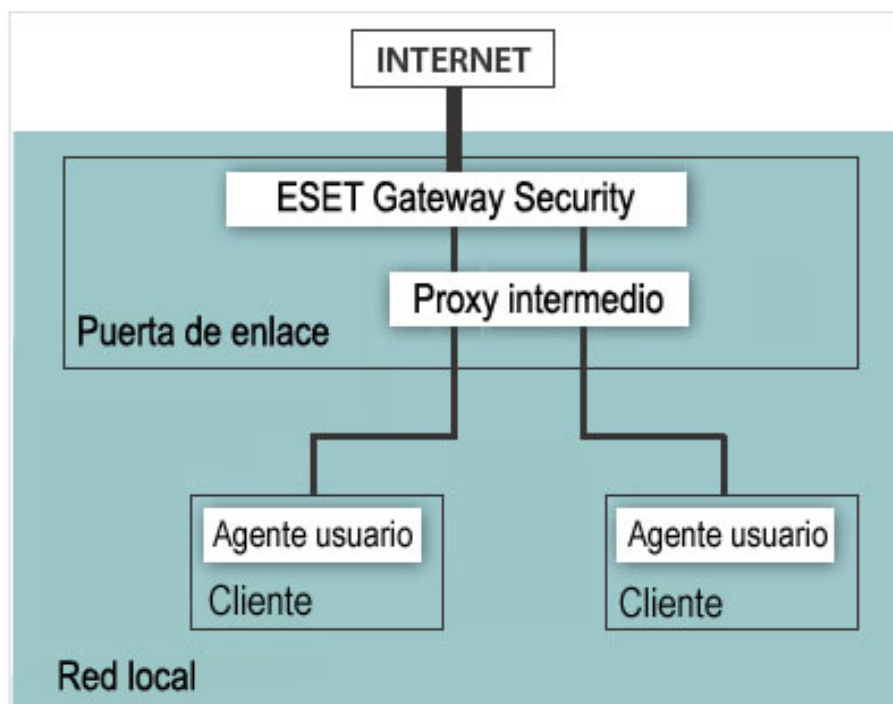


Figura 4.2.2: Configuración de **esets\_http** con Squid Web.

La diferencia principal de este esquema con la configuración detallada anteriormente, es que **ESET Gateway Security** está instalado en la puerta de enlace HTTP / FTP, entre el *proxy* intermedio (en este caso, Squid Web) e Internet.

De esta manera todas las comunicaciones HTTP / FTP entrantes, son analizadas en primer lugar y posteriormente almacenadas en la memoria intermedia específica de la red.

En otras palabras, todos los objetos fuente presentes en *proxy* intermedio, ya fueron analizados y no es necesario verificarlos cuando son solicitados nuevamente.

Como ejemplo, se muestra la configuración de **esets\_http** para permanecer a la escucha en el puerto 8080 del servidor de enlace, cuya IP local es **192.168.1.10**.

Para ello, en la sección **[http]** del archivo **esets.cfg** se determinaron los siguientes parámetros:

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

El valor del parámetro **listen\_addr** también puede ser el nombre del ordenador anfitrión. Este es visible desde la red local.

También puede ser configurado para permitir que **esets\_http** analice todas las interfaces, introduciendo el valor **0.0.0.0**.

Para utilizar la última opción, es necesario aplicar medidas de seguridad adicionales, ya que los usuarios que se encuentran fuera de la red local podrían utilizar el análisis HTTP / FTP.

Para configurar Squid con el fin de utilizar **esets\_http** como *proxy* superior:

- En el archivo de configuración de Squid (/etc/squid/squid.conf), agregue las siguientes líneas:

```
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
```

En el ejemplo, Squid ha sido configurado para utilizar el *proxy* HTTP a la escucha en la dirección IP 192.168.1.10, puerto 8080, como *proxy* superior.

Todas las solicitudes procesadas por Squid serán derivadas a este destino.

El resto de las líneas se utilizan para configurar mensajes de error, si el *proxy* superior estuviera caído o inaccesible.

Si desea configurar Squid para que intente realizar una conexión directa cuando el *proxy* superior esté inaccesible:

- En el archivo de configuración de Squid (/etc/squid/squid.conf), agregue las siguientes líneas:

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

Para releer la configuración nueva, debe cargar nuevamente el proceso demonio (*daemon*) de **ESET Gateway Security**.

### 4.3. Configuración del protocolo de adaptación de contenidos de Internet

La adaptación de contenidos de Internet es un método ampliamente conocido, destinado a proporcionar dirección de contenido basada sobre objetos para los servicios HTTP.

Este método utiliza el protocolo de adaptación de contenidos de Internet (ICAP, *Internet Content Adaptation Protocol*), descrito en el memorándum RFC-3507.

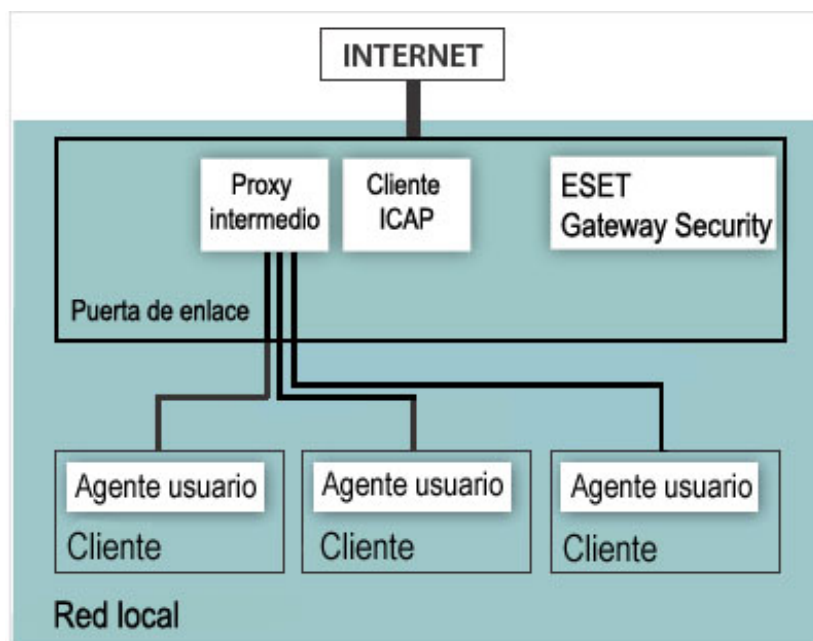


Figura 4.3: Esquema del funcionamiento de ESET Gateway Security como servidor ICAP.

El *proxy* intermedio recibe una solicitud HTTP del agente de usuario o una respuesta del servidor HTTP, y encapsula el mensaje en una solicitud ICAP.

En este caso, el *proxy* intermedio también debe actuar como cliente ICAP, y enviar la solicitud de adaptación del mensaje a ESET Gateway Security, es decir a un servidor de seguridad genérico ESET ICAP denominado *esets\_icap*.

Este módulo analiza el cuerpo del mensaje encapsulado, en busca de infiltraciones.

Sobre la base de los resultados de la verificación, ESET Gateway Security proporciona una respuesta ICAP adecuada, que es devuelta al cliente ICAP, o al *proxy* intermedio para su posterior envío hacia su correspondiente destino.

Si desea configurar **ESET Gateway Security**, para que realice el análisis de los mensajes HTTP encapsulados en solicitudes ICAP:

1. Introduzca la siguiente línea de comando:

```
/usr/sbin/esets_setup
```

2. Siga las instrucciones proporcionadas por la secuencia de comandos.
3. Cuando aparezca la opción **Available installations/un-installations** (Instalaciones / Desinstalaciones disponibles), seleccione **ICAP** para visualizar las opciones **install/uninstall** (Instalar / Desinstalar).
4. Seleccione **install** (Instalar).  
Automáticamente, esta opción configurará el módulo para permanecer a la escucha en un puerto predefinido y cargará nuevamente el servicio del proceso demonio de **ESET Gateway Security**.

De forma predeterminada, el instalador muestra todos los pasos que se realizarán. También crea una copia de seguridad de la configuración, que podrá ser restaurada más adelante, en caso de ser necesario.

En el [Apéndice A](#) encontrará los pasos detallados de la herramienta de instalación, para los distintos escenarios posibles.

5. A continuación, hay que activar la función de cliente ICAP en el *proxy* intermedio. El cliente ICAP debe ser configurado de forma apropiada, para que solicite adecuadamente el servicio de análisis de infiltraciones del módulo **esets\_icap**.

La línea de petición inicial de la solicitud ICAP debe ser introducida siguiendo este orden:

```
METHOD icap://servidor/av_scan ICAP/1.0
```

donde **METHOD** es el método ICAP utilizado, **servidores** el nombre o dirección IP del servidor y **av\_scanes** el identificador del servicio de análisis de infiltraciones de **esets\_icap**.

## 4.4. Tratamiento de objetos HTTP de gran tamaño

En condiciones normales, los objetos son transferidos, en primer término, del servidor o cliente HTTP al módulo **esets\_http**.

Allí son analizados en busca de infiltraciones y, una vez finalizada la verificación, son transferidos a su destino definitivo: el servidor o cliente HTTP, según corresponda.

Este no es un procedimiento óptimo para archivos de gran tamaño, es decir, para aquellos objetos cuyo tiempo de transferencia es mayor al tiempo de espera definido en el parámetro **lo\_timeout**.

En estos casos, la configuración del tiempo de espera del agente de usuario, o simplemente la impaciencia, pueden causar interrupciones en la transferencia del objeto, o incluso cancelarla.

Por este motivo, deben implementarse otros métodos para el procesamiento de objetos de gran tamaño. Estos métodos alternativos se describen en las dos secciones siguientes.

### 4.4.1. Método de análisis diferido

Con **esets\_http** puede emplearse la técnica conocida como **análisis diferido**. Este método utiliza el procedimiento que se describe a continuación.

Cuando el tamaño del objeto que recibe en la transferencia es demasiado grande, **esets\_http** comenzará a enviarlo hacia el destinatario HTTP, cliente o servidor.

Solo cuando **esets\_http** recibe la última parte del objeto, lo analizará en busca de infiltraciones.

Si encuentra una amenaza, no enviará la parte final del objeto y finalizará la conexión con el punto de destino.

Asimismo, se enviará un mensaje de correo electrónico al administrador de la puerta de enlace, detallando la infiltración detectada en el archivo. Este aviso se envía únicamente en un contexto de transferencia de datos de servidor a cliente.

Además, la URL de origen del objeto se guardará en el *proxy* intermedio **esets\_http**, para bloquear la transferencia del archivo si vuelve a ser solicitado.

Es importante mencionar que el método de **análisis diferido**, presenta un riesgo potencial para el ordenador que solicite por primera vez el archivo infectado. Esto se debe a que algunas partes de los datos que lograron ser transferidos pueden contener código ejecutable peligroso.

Por esta razón, **ESET** desarrolló una versión modificada de este método, conocida como la técnica de **análisis parcial**.

#### 4.4.2. Técnica de análisis parcial

La técnica de **análisis parcial** fue desarrollada como medida de seguridad adicional al método de **análisis diferido**.

Este método se basa sobre la idea de que el tiempo de análisis de un objeto de gran tamaño, es insignificante con respecto al tiempo total que lleva su procesamiento.

Este hecho es especialmente evidente en las transferencias HTTP de objetos de gran tamaño, en las que se necesita mucho más tiempo para transmitir el objeto que para analizarlo.

Esto permite realizar más de una verificación durante la transferencia de un objeto de este tipo.

Para activar esta técnica, en la sección [http] del archivo de configuración de ESET Gateway Security, hay que introducir el parámetro **lo\_partscan\_enabled**.

Con esta configuración, los objetos de gran tamaño serán analizados en busca de infiltraciones durante la transferencia, en intervalos de tiempo predefinidos. Simultáneamente, los datos que ya han sido analizados y no están infectados, son enviados al punto de destino, ya sea un cliente o un servidor HTTP.

Este método asegura que no se transmitirá ninguna infiltración al ordenador que ha solicitado el objeto infectado, pues solo se transferirán las porciones de datos que ya han sido analizadas y que están libres de código malicioso.

Está comprobado que en circunstancias normales, cuando la velocidad de la puerta de enlace de la red local es mayor que la de la conexión a Internet, el tiempo total de procesamiento de las transferencias de objetos de gran tamaño es aproximadamente el mismo utilizando la técnica de **análisis parcial**, que cuando se usa el método de **análisis diferido**.

## 4.5. Filtro ESET para SafeSquid

En las secciones anteriores hemos detallado la integración de **ESET Gateway Security** con servicios HTTP y FTP utilizando `esets_http` y `esets_ftp`. Los métodos descritos, son aplicables a la mayoría de los agentes de usuario más comunes, incluyendo el reconocido filtro de contenidos para Internet, [SafeSquid](#).

Sin embargo, **ESET Gateway Security** ofrece un método alternativo para la protección de servicios de la puerta de enlace, utilizando el módulo `esets_ssfi.so`.

### 4.5.1. Principio operativo

El módulo `esets_ssfi.so` es un complemento que permite el acceso a todos los objetos procesados por el *proxy* intermedio SafeSquid.

Una vez que el complemento accede al objeto, este es analizado en busca de infiltraciones, por el proceso demonio de **ESET Gateway Security**.

Si el objeto está infectado, SafeSquid bloquea el recurso correspondiente y envía la plantilla predeterminada en su lugar.

El módulo `esets_ssfi.so` es compatible con SafeSquid Advanced versión 4.0.4.2 y posteriores.

### 4.5.2. Instalación y configuración

Para integrar este complemento, en primer lugar deben crearse enlaces desde el directorio de módulos de SafeSquid, a la carpeta donde se encuentra instalado el paquete **ESET Gateway Security**.

Para el siguiente ejemplo se presupone que SafeSquid está instalado en un sistema operativo Linux, en el directorio `/opt/safesquid`.

- Si la versión de **SafeSquid** es 4.2 o posterior, introduzca los siguientes comandos:

```
mkdir /opt/safesquid/modules

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
```

- Si se trata de una versión de **SafeSquid** anterior a la versión 4.2, introduzca los siguientes comandos:

```
mkdir /opt/safesquid/modules

ln -s @LIBDIR@/ssfi/esets_ssfi.so /opt/safesquid/modules/
esets_ssfi.gcc295.so

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

/etc/init.d/safesquid restart
```

Para completar la instalación del complemento:

1. Inicie sesión en la interfaz de administración web de SafeSquid.
2. En el menú de la página principal de la interfaz, seleccione **Config**.
3. En la sección **Select a Section to Configure** (Seleccione una sección para configurar), busque el elemento **ESET Gateway Security**.  
Pulse **Submit** (Presentar).
4. En la parte inferior de la ventana, presione el botón **Add** (Agregar) para crear el perfil antivirus para **ESET Gateway Security**.
5. En la lista de parámetros que aparece, defina los siguientes valores:

```
Comment: ESET Gateway Security
Profiles: antivirus
```

6. Pulse **Submit** (Enviar).
7. Presione **Save settings** para guardar la configuración de SafeSquid.

El complemento para SafeSquid puede ser utilizado inmediatamente después de su instalación. Sin embargo, se recomienda realizar un pequeño ajuste adicional.

A continuación, se explica cómo configurar SafeSquid para que utilice las plantillas de bloqueo predeterminadas de **ESET Gateway Security**, cuando un objeto transferido esté infectado o no haya sido analizado.

1. Inicie sesión en la interfaz de administración web de SafeSquid.
2. En el menú de la página principal de la interfaz, seleccione **Config**.
3. En la sección **Select a Section to Configure** (Seleccione una sección para configurar), busque el elemento **ESET Gateway Security**.
4. A continuación, modifique el perfil de antivirus recientemente creado. Para ello, en la parte inferior de la sección **ESET Gateway Security** presione **Edit** (Modificar).
5. En la lista de parámetros que aparece, defina los siguientes valores:

```
Infected template: esets_infected
Not scanned template: esets_not_scanned
```

6. Pulse **Submit** (Enviar).
7. En el menú de la página principal de la interfaz, seleccione nuevamente **Config**.
8. Abra la página **Templates** (Plantillas).  
En esta sección, el parámetro **Path** define la ruta del directorio donde se encuentran las plantillas predeterminadas de SafeSquid.  
Generalmente, el valor de este parámetro es **/opt/safesquid/safesquid/templates**.  
Asegúrese de que dicho directorio exista realmente. En caso contrario, deberá crearlo.

Para acceder a las plantillas predeterminadas de **ESET Gateway Security** desde este directorio, agregue los enlaces apropiados mediante los siguientes comandos:

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

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

9. A continuación, en la sección **Templates** (Plantillas) presione **Add** (Agregar) para cargar las definiciones nuevas a la configuración de **SafeSquid**.
10. Seleccione la página de bloqueo de objetos infectados. En la lista que aparece allí, defina los siguientes parámetros:

```
Comment: ESET Gateway Security infected template  
Name: esets_infected  
File: ssfi_infected.html  
Mime type: text/html  
Response code: 200  
Type: File  
Parsable: Yes
```

11. Seleccione la página de bloqueo de objetos no analizados. En la lista que aparece allí, defina los siguientes parámetros:

```
Comment: ESET Gateway Security not scanned template  
Name: esets_not_scanned  
File: ssfi_not_scanned.html  
Mime type: text/html  
Response code: 200  
Type: File  
Parsable: Yes
```

12. Para forzar la lectura de la nueva configuración, debe cargar nuevamente SafeSquid y el proceso demonio de **ESET Gateway Security**.

## 5. Principales mecanismos de seguridad de ESET Gateway Security

### 5.1. Directivas para el manejo de objetos (*Handle Object Policy*)

El mecanismo de directivas para el manejo de objetos (*Handle Object Policy*), detallado en la figura 5.1, permite filtrar los objetos analizados según su estado.

Esta función se basa sobre las siguientes opciones de configuración: **action\_av**, **action\_av\_infected**, **action\_av\_notscanned**, y **action\_av\_deleted**.

Para obtener mayor información sobre estas opciones y sus características, consulte la página de manual `esets.cfg(5)`.

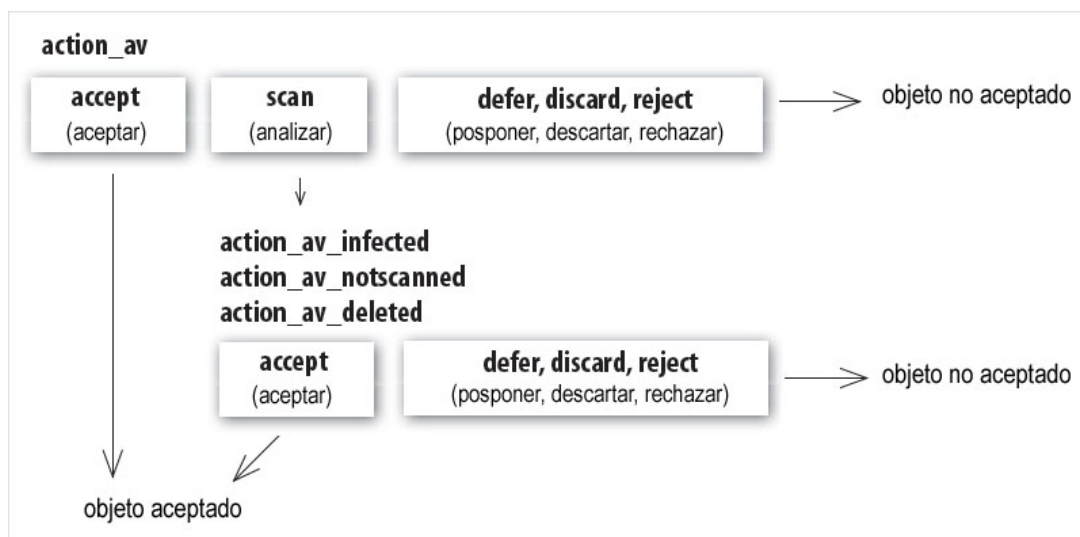


Figura 5-1. Esquema del mecanismo de directivas para el manejo de objetos (*Handle Object Policy*)

Inicialmente, cada objeto procesado se gestiona según la configuración de la opción **action\_av**.

De acuerdo con el valor determinado para dicha opción, el objeto se aceptará (**accept**), pospondrá (**defer**), descartará (**discard**), o rechazará (**reject**), según corresponda.

Si se le ha asignado el valor **scan** (analizar), el objeto será examinado en busca de infiltraciones de virus. Si la opción **av\_clean\_mode** tiene el valor **yes** (sí), al encontrar una amenaza, el objeto será desinfectado automáticamente.

Las opciones **action\_av\_infected**, **action\_av\_notscanned** y **action\_av\_deleted** sirven para determinar la acción que se aplicará sobre el objeto.

Si cada una de ellas tuvo como resultado el valor **accept** (aceptar), el objeto será admitido. En caso contrario, será bloqueado.

✍ Algunos módulos han sido desarrollados para integrar los productos de seguridad ESET en un entorno que no permite modificar los objetos analizados.

Por lo tanto, en dichos módulos, esta última opción está desactivada, y se ignora el valor del parámetro **av\_clean\_mode**.

Para obtener más información acerca de este tema, consulte las páginas de manual relacionadas con estos módulos.

## 5.2. Configuración específica del usuario (*User Specific Configuration*)

El propósito de la configuración específica del usuario (*User Specific Configuration*), es proporcionar un mayor nivel de personalización y funcionalidad al sistema.

Este mecanismo, le permite al administrador definir los parámetros del análisis antivirus de **ESET Gateway Security**, basándose sobre las necesidades de cada usuario que accede al sistema.

En esta sección, daremos un breve ejemplo de una configuración específica del usuario.

Para obtener una descripción más detallada sobre esta función, consulte la página del manual **esets.cfg(5)**.

En nuestro ejemplo, se utiliza el módulo **esets\_http** para controlar el tráfico HTTP a través del puerto 8080 del servidor de entrada, en una red local cuya dirección de IP es **192.168.1.10**.

En la sección **[http]** del archivo de configuración **esets.cfg**, se puede modificar este módulo, como se muestra a continuación:

```
[http]
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8080
action_av = "scan"
```

**ESET Gateway Security** permite asignar una configuración de análisis especial para un usuario en particular.

Para ello, hay que seguir los pasos descritos a continuación:

1. En la sección **[http]** del archivo de configuración de **ESETS**, hay que definir el parámetro **user\_config**, especificando el nombre del archivo donde se guardarán las reglas especiales.  
En el siguiente ejemplo, el archivo se llama **esets\_http\_spec.cfg** y está ubicado dentro del directorio de configuración de **ESET Gateway Security**.  
La ruta de este directorio varía según el sistema operativo utilizado (Ver [Glosario](#), [Directorio de configuración](#)).

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

2. Después de definir el archivo en el parámetro **user\_config**, en el directorio de configuración de **ESET Gateway Security** hay que crear el archivo **esets\_http\_spec.cfg**.
3. Por último, hay que agregar las reglas deseadas.  
Al comienzo de la sección especial, se debe introducir el nombre del usuario al cual se aplicará la configuración individual, y debajo especificar la lista de reglas.

La configuración determinada a continuación permitirá que se procesen normalmente los intentos de acceso al sistema de archivos realizados por los usuarios, excepto aquellos que provengan del cliente HTTP cuya dirección de IP sea **192.168.1.40**:

```
[ | 192.168.1.40]
action_av = "reject"
```

Es decir que, por ejemplo, todos los objetos del sistema de archivos a los cuales accedan los usuarios, serán analizados en busca de virus, excepto cuando la dirección de IP del cliente HTTP activo sea la que se ha especificado en la configuración, en cuyo caso se denegará el acceso.

### 5.3. Lista negra y lista blanca

La configuración descrita en la sección anterior permite crear una lista negra o una lista blanca para el módulo **esets\_http**, y controlar el tráfico HTTP de una forma más específica.

Para ello, hay que seguir los pasos descritos a continuación:

1. En el archivo de configuración especial **esets\_http\_spec.cfg**, hay que agregar una sección específica según el tipo de lista que desea crear.

- o Código para generar una lista negra:

```
[black-list]
action_av = "reject"
```

2. Código para generar una lista blanca:

```
[white-list]
action_av = "accept"
```

3. A continuación, hay que agregar a la lista negra o a la lista blanca los servidores HTTP que desea bloquear o aceptar, respectivamente.

Para ello, en el archivo de configuración **esets\_http\_spec.cfg**, es necesario crear una sección especial.

- o Código para agregar un servidor a la lista negra:

```
[200.191.93.52]
parent_id = "black-list"
```

Esta configuración, incluirá en la lista negra el servidor con dirección IP **200.191.93.52**. Todos los intentos de acceso al sistema de archivos provenientes del cliente HTTP con dirección IP **200.191.93.52**, serán rechazados.

4. Código para agregar un servidor a la lista blanca:


```
[200.198.90.101]
parent_id = "white-list"
```

Esta configuración, incluirá en la lista blanca el servidor con dirección IP **200.198.90.101**.

## 5.4. Sistema de envío de muestras

El sistema de envío de muestras, basado sobre la tecnología **ThreatSense.Net**, recolecta los objetos infectados que han sido detectados por la heurística avanzada, y los envía a un servidor especialmente dedicado.

Todas las muestras recibidas a través de este sistema, serán procesadas en el laboratorio de investigación de virus de **ESET**. Si es necesario, se agregarán a la base de datos de firmas de virus.

 **Nuestro acuerdo de licencia especifica que, al habilitar el sistema de envío de muestras, el usuario acepta que el ordenador o plataforma donde está instalado esets\_daemon recopile ciertos datos, que pueden incluir información personal y muestras de los virus u otras amenazas detectadas recientemente, para enviarlos posteriormente a nuestro laboratorio.**

**De forma predeterminada, esta característica está desactivada.**

**Toda la información recolectada se utilizará únicamente para analizar nuevas amenazas, y no se usará con ningún otro fin.**

Para activar el sistema de envío de muestras, en la sección **[global]** del archivo de configuración de **ESET Gateway Security**, hay que habilitar la opción **samples\_enabled**.

Para permitir el envío de las muestras a los servidores del laboratorio de análisis de virus de **ESET**, en la misma sección también se debe activar el parámetro **samples\_send\_enabled**.

Asimismo, el usuario tiene la posibilidad de proporcionar información complementaria al equipo del laboratorio de virus de **ESET**, si así lo desea.

Para esto puede utilizar las opciones de configuración **samples\_provider\_mail** y **samples\_provider\_country**.

La información recolectada mediante el uso de estas opciones, ayudará al equipo de **ESET** a tener una visión de conjunto sobre una infiltración específica, que podría estar diseminándose a través de Internet.

Para obtener más información acerca del sistema de envío de muestras, consulte la página de manual **esets\_daemon(8)**.

## 5.5. Interfaz web

La interfaz web simplifica las tareas de configuración, administración y gestión de licencias de los sistemas de seguridad **ESET**.

Este módulo, es un agente independiente y debe ser activado de forma explícita.

Para configurar rápidamente la interfaz web:

1. Modifique las siguientes entradas en el archivo de configuración **esets.cfg**:

```
[wwi]
agent_enabled = yes
listen_addr = dirección de escucha
listen_port = puerto de escucha
username = nombre de usuario
password = contraseña
```

2. Reemplace los valores destacados por los datos correspondientes a su sistema, y abra su navegador en la página <https://address:port>.  
Para acceder al contenido, deberá introducir su nombre de usuario y contraseña.
3. A continuación, reinicie el proceso demonio de **ESET Gateway Security**.

En la página de ayuda encontrará instrucciones para el uso básico de esta característica. Si desea obtener más detalles técnicos, consulte la página de manual **esets\_wwi(1)**.

## 5.6. Administración remota

**ESET Gateway Security** es compatible con **ESET Remote Administrator**. Esto permite gestionar de forma remota la seguridad en redes extensas.

Para más información, consulte el [manual de ESET Remote Administrator](#).

El cliente de administración remota es parte del proceso demonio principal de **ESET Gateway Security**.

Para una configuración básica, en la sección **[global]** del archivo **esets\_cfg**, utilice el parámetro **racl\_server\_addr**.

Si se ha establecido una contraseña para el uso de la consola de **ESET Remote Administrator**, también deberá definir el parámetro **racl\_password**.

En la página de manual **esets\_daemon(8)**, encontrará una lista con todas las variables disponibles para configurar el cliente **ESET Remote Administrator**.

El cliente **ESET Remote Administrator** integrado en las soluciones de seguridad **ESET** para sistemas Unix, realiza las siguientes operaciones:

- Se comunica con el servidor de administración remota **ERAS** y proporciona información del sistema, configuración, estado de la protección y sus características.
- Permite ver y modificar las configuraciones cliente utilizando **ESET Configuration Editor** y aplicarlas mediante una tarea específica.
- Realiza análisis y actualizaciones a petición del usuario y envía los registros de análisis al servidor de administración remota **ERAS**.
- Envía al registro de amenazas los análisis más importantes realizados por el proceso demonio de **ESET Gateway Security**.
- Envía al registro de sucesos todos los mensajes que no contengan avisos de depuración de errores.

Funciones no compatibles:

- Registro de cortafuegos.
- Instalación remota.

## 6. Sistema de actualización de *ESET Gateway Security*

### 6.1. Herramienta de actualización de *ESET Gateway Security*

Para asegurar la eficacia de **ESET Gateway Security**, la base de firmas de virus debe mantenerse actualizada.

La herramienta **esets\_update** ha sido desarrollada con este propósito.

Para obtener más información sobre su funcionamiento, consulte la página de manual **esets\_update(8)**.

Antes de ejecutar una actualización, en la sección **[global]** del archivo de configuración de **ESET Gateway Security** deben estar definidas las opciones **av\_update\_username** y **av\_update\_password**.

Si el acceso a Internet se realiza a través de un servidor *proxy* HTTP, también hay que determinar las opciones **proxy\_addr** y **proxy\_port**.

Asimismo, si el servidor *proxy* solicita un nombre de usuario y una contraseña, será necesario definir las opciones **proxy\_username** y **proxy\_password** en dicha sección.

Para iniciar una actualización, introduzca el siguiente comando:

```
@SBINDIR@/esets_update
```

Con el objetivo de ofrecer la mayor seguridad posible al usuario final, el equipo de investigadores de **ESET** recolecta permanentemente definiciones de virus provenientes de todo el mundo.

Los patrones nuevos, se agregan a la base de firmas en intervalos breves. Por tal motivo, se recomienda realizar actualizaciones con frecuencia.

En la sección **[global]** del archivo de configuración de **ESET Gateway Security**, la opción **av\_update\_period** permite determinar la periodicidad de las actualizaciones.

Para que la actualización de la base de firmas de virus sea exitosa, el proceso demonio de **ESET Gateway Security** debe estar activo y en funcionamiento.

## 6.2. Descripción del proceso de actualización de *ESET Gateway Security*

El proceso de actualización consta de dos pasos:

1. En primer lugar, se descargan los módulos de actualización desde el servidor de **ESET**. Si en la sección **[global]** del archivo de configuración **esets.cfg** se encuentra presente la opción **av\_mirror\_enabled**, se crearán copias de dichos módulos. Estas, se guardarán de forma predefinida en el siguiente directorio:

**@BASEDIR@/mirror**

La ruta del directorio del servidor local de actualizaciones (*Mirror*) se puede redefinir en el archivo de configuración de **ESET Gateway Security**, en la sección **[update]** (actualización), utilizando la opción **av\_mirror\_dir**.

El servidor recientemente creado es completamente funcional y también puede ser copiado para crear otras imágenes de actualización, de menor jerarquía en la estructura de árbol de la red. Sin embargo, es necesario cumplir con las siguientes condiciones:

1. El ordenador donde se descargarán los módulos debe tener instalado un servidor HTTP.
2. Los módulos que serán descargados por otros ordenadores, deben ubicarse en el siguiente directorio:

**/http-serv-base-path/eset\_upd**

En el ejemplo anterior, **/http-serv-base-path/eset\_upd** es la ruta básica de un servidor HTTP. Este será el primer directorio donde la herramienta de actualización buscará los archivos con los datos nuevos.

2. En el segundo paso del proceso, se compilan los módulos guardados en el servidor local de actualizaciones (*Mirror*), que utilizará posteriormente el motor de análisis de **ESET Mail Security**. Normalmente, se crearán los siguientes módulos de carga (entre otros):
  - o Módulo cargador (*loader module*): em000.dat
  - o Módulo de análisis (*scanner module*): em001.dat
  - o Módulo de base de datos de firmas de virus (*virus signature database module*): em002.dat
  - o Módulos de compatibilidad para diferentes archivos (*archive support module*): em003.dat
  - o Módulos de heurística avanzada (*advanced heuristics module*): em004.dat

Todos ellos se crearán en el siguiente directorio:

**@BASEDIR@**

El proceso demonio de **ESET Gateway Security**, carga sus módulos desde dicho directorio. En la sección **[global]** del archivo de configuración **esets.cfg**, la opción **base\_dir** permite redefinir este valor, si fuera necesario hacerlo.

### 6.3. Proceso demonio del servidor local de actualizaciones HTTP de *ESET Gateway Security*

El proceso del servidor local de actualizaciones HTTP se instala automáticamente con **ESET Gateway Security**.

Este servicio se inicia si el servidor **Mirror** está habilitado y en la sección **[global]** del archivo **esets.cfg**, la opción **av\_mirror\_httpd\_enabled** tiene el valor **yes** (sí).

Las opciones **av\_mirror\_httpd\_port** y **av\_mirror\_httpd\_addr** definen el puerto (el valor predeterminado es 2221) y la dirección de escucha del servidor HTTP (las predeterminadas son todas las direcciones locales TCP).

La opción **av\_mirror\_httpd\_auth\_mode** permite cambiar al modo básico de autenticación de acceso. El valor predeterminado para esta opción es **none** (ninguno).

Las opciones **av\_mirror\_httpd\_username** y **av\_mirror\_httpd\_password** posibilitan que el administrador defina los parámetros de acceso al servidor local de actualizaciones.

## 7. Glosario

En esta sección, se detallarán algunos de los términos y abreviaciones que se utilizan a lo largo de este manual.

- **RSR**

Es la abreviatura de Red Hat / Novell (SuSE) Ready.

**ESET Gateway Security** es compatible con las variantes Red Hat Ready y Novell (SuSE) Ready. La diferencia del paquete **RSR** con la versión estándar de **ESET Gateway Security** para Linux, es que el primero cumple los requerimientos definidos por la norma FHS (*File-system Hierarchy Standard*, Estándar de jerarquía del sistema de archivos definido como parte de la base de Linux), exigidos por la certificación Red Hat Ready y Novell (SuSE) Ready.

El paquete **RSR** es un complemento de **ESET Gateway Security**, y su directorio principal de instalación es `/opt/eset/esets`.

- **Proceso demonio esets\_daemon**

El proceso `esets_daemon`, es el demonio principal de análisis y control del sistema.

- **Directorio base**

Es el directorio donde se guardan los módulos de **ESET Gateway Security** que contienen la base de firmas de virus.

Utilizaremos la variable `@BASEDIR@` para referirnos a dicho directorio. A continuación se presenta el valor de `@BASEDIR@` para los siguientes sistemas operativos:

- Linux: `/var/lib/esets`
- Linux RSR: `/var/opt/eset/esets/lib`
- FreeBSD: `/var/lib/esets`
- NetBSD: `/var/lib/esets`
- Solaris: `/var/opt/esets/lib`

- **Directorio de configuración de *ESET Gateway Security***

Es el directorio donde se guardan todos los archivos relacionados con la configuración de **ESET Gateway Security**.

Utilizaremos la variable `@ETCDIR@` para referirnos a dicho directorio. A continuación se presenta el valor de `@ETCDIR@` para los para los siguientes sistemas operativos:

- Linux: `/etc/esets`
- Linux RSR: `/etc/opt/eset/esets`
- FreeBSD: `/usr/local/etc/esets`
- NetBSD: `/usr/pkg/etc/esets`
- Solaris: `/etc/opt/esets`

- **Archivo de configuración de *ESET Gateway Security***

Es el archivo de configuración principal de **ESET Gateway Security**. La ruta absoluta de su ubicación es **@ETCDIR@/esets.cfg**.

- **Directorio de archivos binarios de *ESET Gateway Security***

Es el directorio donde se guardan los archivos binarios de **ESET Gateway Security**.

Utilizaremos la variable **@BINDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@BINDIR@** para los siguientes sistemas operativos:

- Linux: /usr/bin
- Linux RSR: /opt/eset/esets/bin
- FreeBSD: /usr/local/bin
- NetBSD: /usr/pkg/bin
- Solaris: /opt/esets/bin

- **Directorio de archivos binarios del sistema *ESET Gateway Security***

Es el directorio donde se guardan los archivos de sistema binarios de **ESET Gateway Security**.

Utilizaremos la variable **@SBINDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@SBINDIR@** para los siguientes sistemas operativos:

- Linux: /usr/sbin
- Linux RSR: /opt/eset/esets/sbin
- FreeBSD: /usr/local/sbin
- NetBSD: /usr/pkg/sbin
- Solaris: /opt/esets/sbin

- **Directorio de archivos objeto de *ESET Gateway Security***

Es el directorio donde se guardan los archivos objeto y bibliotecas de **ESET Gateway Security**.

Utilizaremos la variable **@LIBDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@LIBDIR@** para los siguientes sistemas operativos:

- Linux: /usr/lib/esets
- Linux RSR: /opt/eset/esets/lib
- FreeBSD: /usr/local/lib/esets
- NetBSD: /usr/pkg/lib/esets
- Solaris: /opt/esets/lib

## 8. Contacto

Apreciado usuario, esperamos que esta guía le haya permitido comprender cabalmente los requisitos para la instalación, configuración y mantenimiento de **ESET Gateway Security**.

Sin embargo, nuestro objetivo es mejorar continuamente la calidad de nuestra documentación. Si considera que alguna sección de esta guía no es clara o se encuentra incompleta, por favor comuníquese con nosotros.

Nos dedicamos a proporcionar un servicio de asistencia técnica de excelencia, y estamos disponibles para ayudarlo ante cualquier duda, problema o comentario acerca de este producto

### Soporte técnico:

[ayuda@eset.es](mailto:ayuda@eset.es)

### Ventas:

[ventas@eset.es](mailto:ventas@eset.es)

### Información general:

[info@eset.es](mailto:info@eset.es)

### Direcciones:

#### ESET NOD32 en España

**Ontinet.com, S.L.**,  
c/Martinez Valls 56 bajos  
46870 Ontinyent (Valencia)  
España

Teléfono: +34 902.33.48.33  
Fax: +34 96.191.03.21

#### ESET, Central

**ESET, LLC.**  
610 West Ash Street,  
Suite 1900  
San Diego, CA 92101  
USA

Teléfono: +1 (619) 876-5400  
Fax: +1 (619) 437-7045

# Apéndice A: Descripción del proceso de configuración de *ESET Gateway Security*

## A.1. Configuración de *ESET Gateway Security* para analizar las comunicaciones HTTP en modo transparente

El análisis HTTP se realiza utilizando el proceso demonio **esets\_http**.

1. En la sección **[http]** del archivo de configuración **esets.cfg**, introduzca los siguientes parámetros:

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

En el ejemplo, **listen\_addr** es la dirección de la interfaz de la red local, llamada **if0**.

2. Reinicie el proceso demonio de **ESET Gateway Security**.
3. El siguiente paso es redirigir todas las solicitudes HTTP hacia **esets\_http**.
  - o Si la filtración de direcciones IP se realiza mediante la herramienta de administración **ipchains**, una regla apropiada es:

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

4. Si la filtración de direcciones IP se realiza mediante la herramienta de administración **iptables**, la regla es:

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

 En FreeBSD, la regla es:

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

 En NetBSD y Solaris, la regla es:

```
echo 'rdr if0 0.0.0.0/0 port 80 -> 192.168.1.10 \
port 8080 tcp' | ipnat -f -
```

## A.2. Configuración de *ESET Gateway Security* para analizar las comunicaciones FTP, en modo transparente

El análisis FTP se realiza utilizando el proceso demonio **esets\_http**.

1. En la sección **[ftp]** del archivo de configuración **esets.cfg**, introduzca los siguientes parámetros:

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

En el ejemplo, **listen\_addr** es la dirección de la interfaz de la red local, llamada **if0**.

2. Reinicie el proceso demonio de **ESET Gateway Security**.
3. El siguiente paso es redirigir todas las solicitudes FTP hacia **esets\_ftp**.
  - o Si la filtración de direcciones IP se realiza mediante la herramienta de administración **ipchains**, una regla apropiada es:

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

4. Si la filtración de direcciones IP se realiza mediante la herramienta de administración **iptables**, la regla es:

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

 En FreeBSD, la regla es:

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

 En NetBSD y Solaris, la regla es:

```
echo 'rdr if0 0.0.0.0/0 port 21 -> 192.168.1.10 \
port 2121 tcp' | ipnat -f -
```

### A.3. Configuración de *ESET Gateway Security* para analizar los mensajes ICAP HTTP encapsulados

El análisis de los mensajes HTTP encapsulados del tipo ICAP, se realiza utilizando el proceso demonio `esets_icap`.

1. En la sección **[icap]** del archivo de configuración `esets.cfg`, introduzca los siguientes parámetros:

```
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 1344
```

En el ejemplo, **listen\_addr** es la dirección de interfaz de la red local, llamada **if0**.

2. A continuación, reinicie el proceso demonio de **ESET Gateway Security**.

## Apéndice B: Licencia PHP

Licencia PHP, versión 3.01 (*The PHP License, version 3.01*).

Copyright (c) 1999 - 2006, por The PHP Group.

Todos los derechos reservados. Se permite la redistribución y uso del código fuente o binario, con o sin modificación, siempre y cuando se cumplan las siguientes condiciones:

1. Las redistribuciones del código fuente deben mantener el aviso de *copyright* arriba detallado, la presente lista de condiciones y la exención de responsabilidad enunciada al final del documento.
2. Las redistribuciones del código binario deben reproducir el aviso de *copyright* arriba detallado, la presente lista de condiciones, la exención de responsabilidad enunciada al final de documento, y cualquier otro material incluido en esta distribución.
3. El nombre **PHP** no debe utilizarse para auspiciar o promover productos derivados de esta aplicación sin previo permiso escrito. Para obtener un permiso escrito, envíe un mensaje a [group@php.net](mailto:group@php.net).
4. Los productos derivados de esta aplicación no pueden denominarse **PHP**, como tampoco puede aparecer la sigla **PHP** en su nombre, sin haber obtenido el permiso escrito de [group@php.net](mailto:group@php.net). Está permitido destacar que su programa trabaja en conjunto con **PHP** indicando, por ejemplo, **Nombre\_del\_programa para PHP** en lugar de **PHP Nombre\_del\_programa** o **phpnombre\_del\_programa**.
5. The PHP Group puede publicar, regularmente, versiones corregidas o renovadas de esta licencia. Estas tendrán asignado un número de versión distintivo. Una vez que el código ha sido publicado con un número de versión determinado, el usuario puede seguir utilizándolo bajo la reglamentación que posea esa versión, o bien puede registrarse bajo los términos de cualquier versión de licencia publicada posteriormente. Solamente The PHP Group tiene el derecho de modificar los términos aplicables al código creado bajo esta licencia.
6. Las redistribuciones de código fuente o binario deben conservar y enunciar la siguiente certificación:  
"Este producto ha sido desarrollado con PHP. Esta aplicación gratuita está disponible en <http://php.net/software/>".

ESTE SOFTWARE ES DISTRIBUIDO POR EL EQUIPO DE DESARROLLO DE PHP EN UNA CONDICIÓN "TAL COMO ESTÁ". NO SE RECONOCE NINGUNA GARANTÍA EXPLÍCITA O IMPLÍCITA, INCLUYENDO GARANTÍA DE VENTA O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA. EL EQUIPO DE DESARROLLO DE PHP O SUS COLABORADORES NO SERÁN RESPONSABLES EN NINGÚN CASO POR DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES O PUNITIVOS DE NINGÚN TIPO (INCLUYENDO LA ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTOS, PÉRDIDA DE INFORMACIÓN O DE BENEFICIOS O INTERRUPCIÓN DEL NEGOCIO), CUALQUIERA SEA SU CAUSA; Y BAJO NINGUNA SUPOSICIÓN DE RESPONSABILIDAD, YA SEA CONTRACTUAL, ABSOLUTA O FRAUDULENTO (POR NEGLIGENCIA O DE FORMA VOLUNTARIA) OCASIONADOS POR LA UTILIZACIÓN DE ESTE SOFTWARE, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE DICHO DAÑO.