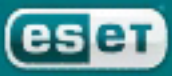


protegemos su mundo digital

ESET Mail Security

Manual de instalación y documentación para el usuario

Contenidos

ESET Mail Security, Primera Edición
Fecha de publicación13 de marzo de 2007

Capítulo 1:

Introducción

Estimado usuario, Ud. acaba de adquirir ESET Mail Security - probablemente el mejor sistema de seguridad ejecutable 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 NOD32 incluido en este producto proveen la mayor tasa de detección de virus y las búsquedas más veloces.

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

• Incluye una heurística única y avanzada para la detección de gusanos y troyanos 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 Mail 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.

• El sistema contiene mecanismos de control de correo basura (*spam*).

• Se puede configurar la información sobre infiltraciones para que aparezca en el encabezado, el pie o el asunto del correo electrónico.

Para un funcionamiento eficiente, ESET Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 las bibliotecas relevantes de ESET Mail 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*.

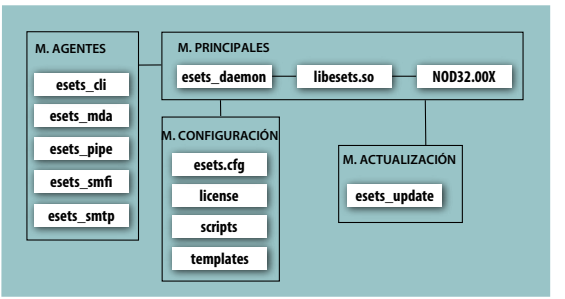
Capítulo 4:

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 Mail Security se muestra en la imagen 4-1. El sistema está formado por los siguientes componentes.

*Imagen **4-1.** Estructura de **ESET** Mail Security.*



MÓDULOS PRINCIPALES

La parte principal de ESET Mail 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 fun-

cionamiento 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 el o los archivos 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@/anti-spam

Este directorio contiene el archivo de configuración utilizado para ajustar y perfeccionar el funcionamiento del motor contra correo basura.

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

Estos archivos son plantillas html utilizadas para definir los textos de los mensajes insertados como notas al pie en los correos electrónicos analizados. Para habilitar estas planillas html, hará falta eliminar el sufijo 'example' de todos los nombres de los archivos de plantillas. También recuerde que la apariencia de los mensajes en notas al pie en los correos electrónicos es establecida por el parámetro 'write_to_footnote' del *archivo de configuración de ESETS*. A continuación se especifica el significado de cada archivo de plantillas individual:

Las siguientes plantillas para mensajes en notas al pie son utilizadas en los correos infectados:

encabezado del correo	De:
.	Para:
---	---
cuerpo del correo	texto del cuerpo del correo electrónico
.	contenido de lms_sig_header_infected.html
.	lista de infiltraciones detectadas por el análisis
.	contenido de lms_sig_footer_infected.html

Las siguientes plantillas para mensajes en notas al pie son utilizadas en los correos limpios:

encabezado del correo	Para:
.	De:
cuerpo del correo	texto del cuerpo del correo electrónico
.	contenido de lms_sig_header_clean.html
.	lista de objetos analizados
.	contenido de lms_sig_footer_clean.html

Las siguientes plantillas para mensajes en notas al pie son utilizadas en los correos que no pudieron ser analizados:

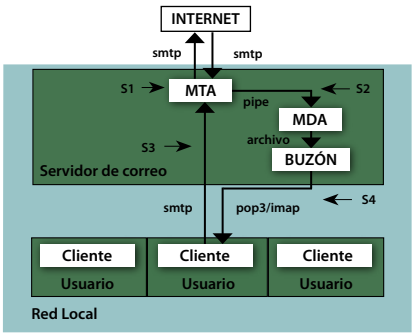
encabezado del correo	Para:
.	De:
cuerpo del correo	texto del cuerpo del correo electrónico
.	contenido de lms_sig_header_not_scanned.html
.	lista de objetos analizados
.	contenido de lms_sig_footer_not_scanned.html

Capítulo 5:

Integración con el Sistema de Mensajería de Correo Electrónico

Este capítulo describe la integración de ESET Mail Security con los diversos sistemas conocidos de mensajería para correo electrónico. El conocimiento de los principios básicos del sistema de mensajería para correo electrónico (imagen 5-1) es imprescindible para comprender el funcionamiento de *ESETS*.

*Imagen **5-1.** Esquema del sistema de mensajería para correo electrónico del SO **UNIX.***



MTA - Agente de transporte de correos (según siglas en inglés)

Es un programa (por ejemplo, sendmail, postfix, qmail, exim, etc.) que transfiere mensajes de correo electrónico entre dominios locales y remotos.

MDA - Agente de reparto de correos (según siglas en inglés)

Es un programa (por ejemplo, maildrop, procmail, deliver, local.mail, etc.) que distribuye los mensajes entrantes enviados a direcciones locales en buzones de correo específicos.

MUA - Cliente de correo electrónico (según siglas en inglés)

Es un programa (por ejemplo, MS Outlook, Mozilla Mail, Eudora, etc.) que permite el acceso y manejo de los mensajes guardados en buzones de correo (leer, escribir, imprimir, etc.).

BUZÓN DE CORREO

Es un archivo o estructura de archivo en un disco que sirve como lugar de almacenamiento de mensajes de correo electrónico. Existen diversos formatos de buzones de correo en los sistemas operativos Linux/BSD: MAILBOX es un formato antiguo donde los correos electrónicos para cada usuario se almacenan cronológicamente en el archivo correspondiente del usuario, ubicado en el directorio '/var/spool/mail'; MBOX sigue siendo un formato antiguo (aunque un poco más actual) donde los correos electrónicos se almacenan cronológicamente en un archivo ubicado dentro del directorio local del usuario; MAILDIR almacena correos electrónicos en archivos separados dentro de una estructura jerárquica de directorios.

El servidor de correo electrónico en general usa el SMTP (protocolo de transferencia simple de correo) para recibir las comunicaciones de datos. El MTA transfiere el mensaje recibido ya sea a otro sistema de mensajería de correo electrónico remoto o al MDA local, que lo enviará al buzón de correo específico (se asume que cada usuario de la red local posee un buzón de correo ubicado en el disco del servidor). Recuerde que la tarea de descargar e interpretar correctamente los mensajes en la computadora del usuario es responsabilidad del MUA local. Cuando el MUA recupera datos del buzón de correo del usuario, en general utiliza el POP3 (protocolo de oficina de correo) o el IMAP

(protocolo de acceso a mensajes de Internet) para comunicarse con el MTA. Para enviar información a Internet se utiliza el protocolo de comunicación SMTP.

El principio de funcionamiento de *ESETS* se basa en la intercepción del intercambio de datos y el análisis en las diversas etapas de su transferencia. Los lugares de intercepción están indicados en la imagen 5-1 por los símbolos S1, S2, S3 y S4.

S1

Análisis de mensajes de correo electrónico bidireccionales, es decir, se filtra el contenido en el MTA.

S2

Análisis de mensajes de correo electrónico entrantes, es decir, mensajes cuyo destinatario corresponde a una dirección ubicada dentro del dominio local.

S3

Análisis de mensajes de correo electrónico salientes, es decir, mensajes dirigidos a un dominio de Internet remoto especificado en el destinatario.

S4

Análisis de mensajes de correo electrónico descargados desde el servidor POP3/IMAP.

En el resto de este capítulo se analizan los métodos de integración de *ESETS* con varios de los sistemas de mensajería soportados.

5.1. Análisis de mensajes de correo bidireccionales en el MTA

La ventaja del modo de análisis de mensajes de correo electrónico bidireccionales nos permite analizar mensajes de entrada y salida en el mismo algoritmo de implementación. Por otra parte, el método bidireccional (filtrador de contenidos) depende del MTA. El sistema de ESET incluye cuatro filtradores de contenido preparados para los MTA más comunes: Sendmail, Postfix, Exim y QMail.

Para configurar ESET Mail Security para el análisis de mensajes de correo bidireccionales, debe asegurarse de que su MTA esté bien configurado y activo. Luego ejecute el siguiente *script*:

```
esets_setup
```

Seleccione las opciones de instalación del MTA y filtrador de contenido. También se visualizará el módulo de *ESETS* utilizado.

Recuerde que el instalador hace una copia de seguridad de todos los archivos de configuración modificados y puede mostrar todos los comandos que ejecutará luego de que Ud. confirme la operación. Úselo también para desinstalar. Los pasos detallados de configuración para todos los posibles escenarios se describen en el apéndice A de este documento.

5.2. Análisis de mensajes de correo entrantes

El análisis de mensajes de correo electrónico entrantes se lleva a cabo durante la transferencia de los mensajes entre el MTA y el MDA. El correo electrónico entrante es interceptado por el módulo **esets_mda**, analizado por el *daemon de ESETS* y distribuido al buzón de correo usando el MDA

original. Como se muestra en la imagen, el análisis de virus puede habilitarse con la configuración adecuada del MTA y del módulo **esets_mda**. Recuerde que ESET Mail Security soporta la mayoría de los MTA más comunes: Sendmail, Postfix, Exim y QMail. *ESETS* soporta todos los MDA. Específicamente se probaron los siguientes MDA: procmail, maildrop, deliver y local.mail.

Para configurar ESET Mail Security para analizar mensajes de correo entrantes, debe asegurarse de que su MTA esté configurado como corresponde utilizando el MDA original y que esté ejecutándose. Luego ejecute el siguiente *script*:

```
esets_setup
```

Seleccione las opciones de instalación del MDA y de correo entrante. También se visualizará el módulo de *ESETS* utilizado.

Recuerde que el instalador hace una copia de seguridad de todos los archivos de configuración modificados y puede mostrar todos los comandos que ejecutará luego de que Ud. confirme la operación. Úselo también para desinstalar. Los pasos detallados de configuración para todos los posibles escenarios se describen en el apéndice A de este documento.

5.3. Análisis de mensajes de correo salientes

El análisis de mensajes de correo electrónico salientes se lleva a cabo durante la transferencia de los mensajes entre el MUA local y el MTA.

Para configurar ESET Mail Security para analizar mensajes de correo salientes, ejecute el siguiente *script*:

```
esets_setup
```

Seleccione la opción de instalación SMTP. Se configurará el módulo **esets_smtp** para que atienda un puerto predefinido y redirija los paquetes IP relevantes. Verifique la regla de *firewall* (cortafuego) agregada y elimínela o modifíquela según sus necesidades.

Recuerde que el instalador hace una copia de seguridad de todos los archivos de configuración modificados y puede mostrar todos los comandos que ejecutará luego de que Ud. confirme la operación. Úselo también para desinstalar. Los pasos detallados de configuración para todos los posibles escenarios se describen en el apéndice A de este documento.

5.4. Análisis de mensajes de correo descargados desde el servidor POP3/IMAP

Para configurar ESET Mail Security para analizar mensajes de correo descargados desde el servidor POP3 (o IMAP), ingrese el siguiente *script*:

```
esets_setup
```

Seleccione la opción de instalación POP3 o IMAP. Se configurará el módulo *ESETS* visualizado para que atienda un puerto predefinido y redirija los paquetes IP relevantes. Verifique la regla de *firewall* agregada y elimínela o modifíquela según sus necesidades.

Recuerde que el instalador hace una copia de seguridad de todos los archivos de configuración modificados y puede mostrar todos los comandos que ejecutará luego de que Ud. confirme la operación. Úselo también para desinstalar. Los pasos detallados de configuración para todos los posibles escenarios se describen en el apéndice A de este documento.

5.5. Métodos alternativos para filtrar contenidos

5.5.1. Análisis de mensajes de correo usando AMaViS

AMaViS (un analizador de virus de correo, según sus siglas en inglés) es una herramienta que crea una interfaz entre el MTA del usuario y varios programas anti-virus. Soporta diversos MTA y existe en tres versiones: **amavis, amavisd** y **amavisd-new**. Amavis colabora con ESET Mail Security utilizando **esets_cli**. Sin embargo, antes de entrar en detalles con la explicación de las configuraciones de Amavis, nos gustaría discutir el impacto que tiene la implementación de este método en el funcionamiento de ESET Mail Security.

Primero, recuerde que Amavis no permite modificar los mensajes de correo electrónico analizados. En consecuencia, ningún archivo adjunto de un mensaje infectado podrá ser desinfectado o eliminado por *ESETS*. La segunda consecuencia es que no serán escritos en el correo electrónico la notificación al pie con el registro de eventos ni los campos del encabezado que dependan del estado de análisis. Por otra parte, Amavis no proporciona el campo remitente/destinatario del correo, por lo que tampoco se pueden utilizar configuraciones específicas de usuario. El manejo avanzado del correo (aceptar, ignorar, descartar, rechazar) también es limitado para **esets_cli**. Finalmente, como Amavis analiza archivos, no se puede utilizar el motor de análisis de correo basura de *ESETS*.

Teniendo en cuenta los inconvenientes mencionados, esta configuración será útil sólo si las características del producto explicadas arriba no son necesarias para el usuario.

5.5.1.1. amavis

La configuración de Amavis se lleva a cabo durante la instalación de Amavis. Luego de descomprimir el archivo original amavis-0.x.y.tgz, cree el archivo amavis/av/esets_cli con el contenido:

```
#
# ESET Software ESETS Command Line Interface
#
if ($esets_cli) {
  do_log(2,"Using $esets_cli");
  chop($output = `$esets_cli --subdir $TEMPDIR/parts`);
  $errval = retcode($?);
  do_log(2,$output);
if ($errval == 0) {
  $scanner_errors = 0;
} elsif ($errval == 1 || $errval == 2 || $errval == 3) {
  $scanner_errors = 0;
  @virusname = ($output =~ /virus="([^"]+)"/g);
  do_virus();
} else {
do_log(0,"Virus scanner failure: $esets_cli (error code: $errval)");
   }
}
```

Tenga en cuenta que este *script* acepta el correo electrónico sólo en caso de que haya sido aceptado previamente por la Política para el Manejo de Objetos de esets_cli. De lo contrario, el correo se bloquea. Si se detectó un virus, se extrae su nombre del correo resultante.

A continuación, si Ud. está utilizando el paquete Linux *RSR*, debe actualizar su variable de entorno PATH con el siguiente comando:

```
export PATH="$PATH:/opt/eset/esets/bin"
```

Para una instalación exitosa, quizá necesite instalar programas adicionales como arc, unarj, unrar, zoo. También deberá hacer un enlace simbólico (*symlink*) en /usr/bin desde uncompress a gzip y crear el usuario amavis en el grupo amavis con el directorio /var/amavis. Ahora prosiga con el proceso de instalación normal (./configure, make, make install) y siga los pasos que aparecen en README.mta según su servidor de correo.

5.5.1.2. amavisd

La configuración de Amavisd se lleva a cabo durante el proceso de instalación de Amavisd. Descomprima el archivo original amavisd-0.x.tgz y siga las instrucciones para la configuración de amavis ya explicadas en la sección 5.5.1.1 de esta guía. Luego de ejecutar 'make install', es posible que sea necesario mover '/usr/etc/amavisd.conf' a '/etc' y ejecutar nuevamente 'make install'.

5.5.1.3. amavisd-new

Para instalar el producto con Amavisd-new, descomprima e instale el archivo original amavisd-new-2.x.y.tgz en el directorio de instalación. Para configurar el producto con el Amavisd-new recién instalado, borre la cláusula para 'ESET Software *ESETS*' y reemplace la cláusula para 'ESET Software *ESETS* - Client/Server Version' en el archivo 'amavisd.conf' por la siguiente:

```
### http://www.eset.com/
['ESET Software ESETS Command Line Interface',
'@BINDIR@/esets_cli', '--subdir {}',
[0], [1], qr/virus="([^"]+)"/ ],
```

Es posible que necesite instalar algunos módulos Perl adicionales como Archive-Tar, Archive-Zip, BerkeleyDB, Compress-Zlib, Convert-TNEF, Convert-UUlib, IO-stringy, MailTools, MIME-Base64, MIME-tools, Net-Server y Unix-Syslog desde www.cpan.org/modules. El procedimiento para la instalación de cada uno de ellos es el siguiente: rl Makefile.PL; make; make install.

Luego de la configuración, por favor, siga las recomendaciones para la configuración de Amavisd-new en README.mta ubicado en el directorio Amavisd-new según su servidor de correo.

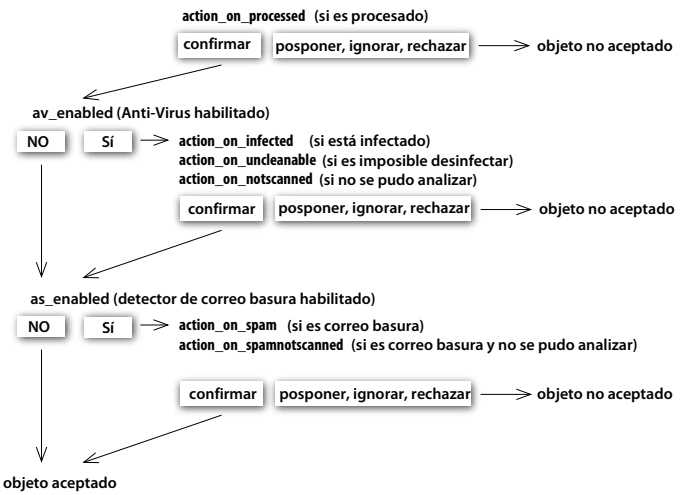
Capítulo 6:

Mecanismos importantes de ESET Mail 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, 'action_on_spam': si es correo basura, 'action_on_spamnotscanned': si es correo basura y no se pudo analizar), además de las opciones de configuración que habilitan el Anti-Virus ('av_enabled') y el detector de correo basura ('as_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 de virus 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, el objeto será analizado para detectar si es correo basura.

Recuerde que el objeto será analizado para detectar si es correo basura sólo si la opción 'as_enabled' está habilitada. En este caso se toman en cuenta las opciones 'action_on_spam' (si es correo basura) y 'action_on_spamnotscanned' (si es correo basura y no se pudo analizar). Si se elige la acción 'accept' (confirmar) como respuesta a cualquiera de las dos opciones anteriores o la opción 'as_enabled' está desabilitada, se acepta el objeto para proceder con su distribución, en caso contrario, se bloquea el objeto y se procede según la acción específica seleccionada.

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 definición de la configuración específica de usuario.

En el caso que utilicemos el módulo **esets_smtp** como filtrador de contenido para el MTA Postfix, el módulo está sujeto a la sección de configuración [smtp] en el *archivo de configuración* de *ESETS*. La sección es la siguiente:

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
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_smtp_spec.cfg' ubicado dentro del *directorio de configuración* de *ESETS*.

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
action_on_processed = accept
user_config = "esets_smtp_spec.cfg"
```

Una vez que se realizó la configuración especial a la que se hace referencia dentro de la sección [smtp], 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 destinatario rcptuser@rcptdomain.com.

```
[rcptuser@rcptdomain.com]
action_on_processed = reject
```

El nombre del encabezado de la sección contiene la identificación del usuario 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, los correos electrónicos serán procesados, es decir, analizados para detectar infiltraciones, con excepción de los correos electrónicos enviados a rcptuser@rcptdomain.com, que serán rechazados sin analizar.

6.3. Lista negra y lista blanca

En el siguiente ejemplo mostramos cómo crear la lista negra y la lista blanca para **esets_smtp** configurado como filtrador de contenido para el MTA Postfix. Recuerde que para este propósito utilizaremos el archivo de configuración especial mencionado anteriormente.

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

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

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

```
[|sndrname1@sndrdomain1.com]
parent_id = "black-list"
```

donde 'sndrname1@sndrdomain1.com' es la dirección de correo electrónico del remitente agregado a la lista negra 'black-list'. Recuerde que con esta configuración todos los correos electrónicos enviados desde esta dirección serán rechazados.
Si deseamos crear la lista blanca 'white-list' que pueda ser utilizada por **esets_smtp**, debemos crear la siguiente sección grupal dentro del archivo de configuración especial 'esets_smtp_spec.cfg' presentado en la sección anterior.

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

Como es de esperar, en este caso se acepta el remitente agregado a la lista blanca.

IMPORTANTE: Recuerde que la barra vertical '|' se coloca delante del nombre en el encabezado de la sección especial únicamente en el caso de la dirección del remitente y no del destinatario. Para más detalles sobre la sintaxis en los nombre de encabezados, consulte la página del manual correspondiente sobre módulos agentes de *ESETS*. Para más información sobre **esets_smtp**, consulte la página del manual esets_smtp(1).

6.4. Control de correo basura

El objetivo del sistema para detección de correo basura es filtrar los mensajes de correo no deseados por el remitente desde el flujo de datos del proceso de distribución de los mensajes.

Para deshacerse del correo basura, este producto implementa el mecanismo de control de correo basura. Dicha función se habilita usando el parámetro 'as_enabled' (para una descripción más detallada del parámetro, consulte la página esets.cfg(5) del manual). Recuerde que el análisis de correo basura sólo puede utilizarse para analizar objetos de correo electrónico, en consecuencia, esta función es relevante únicamente para los módulos **esets_imap, esets_mda, esets_pipe, esets_pop3, esets_smtp** y **esets_smfi**.

Una vez habilitada la opción para control de correo basura en cualquiera de las secciones de configuración, el motor de análisis de correo basura se activará durante el inicio del proceso *daemon* principal para análisis. Durante este proceso, desde el directorio caché de control de correo basura, se cargan los módulos de soporte apropiados para control de correo basura.

También es posible configurar esta opción de control usando el archivo de configuración:

```
@ETCDIR@/anti-spam/spamcatcher.conf
```

Existen varios archivos dentro de este directorio, cada uno de los cuales corresponde a una opción de configuración recomendada para el motor contra correo basura. Recuerde que el archivo de configuración predeterminado corresponde al archivo de configuración 'spamcatcher.conf.faster'. Para utilizar cualquiera de los demás archivos, sólo reemplace el archivo de configuración predeterminado para control de correo basura 'spamcatcher.conf' por el que Ud. eligió y vuelva a iniciar el *daemon* de *ESETS*.

6.5. 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 muetsras 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 ESET Mail Security

7.1. Utilidad de acualización de ESETS

Para que ESET Mail 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 Mail 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:

Trucos y consejos

8.1. Soporte de *ESETS* y TLS en el MTA

TLS (seguridad de la capa de transporte, según sus siglas en inglés) es un protocolo que garantiza la confidencialidad del intercambio de información entre cliente y servidor a través de Internet. TLS se basa en el cifrado de datos con el protocolo SSL para su transferencia entre el SMTP del cliente y el del servidor. Esto trae consecuencias a la hora de analizar dichos intercambios. De hecho, una vez que el soporte TLS está habilitado en el MTA, resulta imposible utilizar los métodos 'wrapping', ya que la comunicación completa SMTP interceptada en esta etapa ya se encuentra encriptada. Por otra parte, es posible usar el cifrado de datos en comunicaciones entre el MTA local e Internet y aún así seguir usando los métodos de filtrado de contenido 'content filtering'. En el MTA Sendmail no hay ningún inconveniente con el soporte TLS para SMTP porque el filtrado de contenido se lleva a cabo internamente usando el filtro de correo Milter. Por otro lado, el Postfix utiliza el protocolo SMTP para el intercambio de información entre el filtrador de contenidos y el MTA. Por lo tanto, una vez que el TLS está habilitado en Postfix, el método de filtrado de contenido fracasa debido al cifrado de la comunicación

Afortunadamente, este problema se puede solucionar en la configuración de TLS para Postfix desactivando el soporte de TLS para la comunicación entre el cliente y el usuario dentro del *localhost*. Agregue la siguiente línea en '/etc/postfix/main.cf':

```
smtp_tls_per_site = hash:/etc/postfix/smtp_tls_per_site
```

También deberá crear la carpeta '/etc/postfix/smtp_tls_per_site' con el siguiente contenido:

```
localhost       NONE
```

y asignarle la tabla *hash* adecuada ingresando el siguiente comando desde el directorio '/etc/postfix' :

```
postmap hash:smtp_tls_per_site
```

Al utilizar el comando mencionado arriba se crea el archivo '/etc/postfix/smtp_tls_per_site.db', que es utilizado por Postfix para habilitar TLS en cada uno de los sitios. En tanto hayamos deshabilitado TLS para el *localhost*, podrá usarse el filtrado de contenidos al mismo tiempo que se cifra la comunicación SMTP entre el MTA local e Internet.

Capítulo 9:

Contáctenos

Estimado usuario, el propósito de esta guía es brindarle la información necesaria sobre la instalación, configuración y mantenimiento de ESET Mail 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 el MTA Postfix

A.1.1. Análisis de mensajes de correo entrantes

Advertencia: Esta instalación no es compatible con SELinux. Deshabilite SELinux o prosiga a la siguiente sección.

El objetivo de esta instalación es insertar **esets_mda** antes del MDA original Postfix. El MDA utilizado (con argumentos) se configura en el parámetro 'mailbox_command' de Postfix.

NOTA: Si el valor está vacío es porque Postfix está enviando correos electrónicos por su cuenta. Deberá instalar y configurar un MDA real (por ejemplo, Procmail) y usarlo primero para 'mailbox_command' incluyendo los argumentos (por ejemplo, /usr/bin/procmail -d "$USER"). Reinicie Postfix y asegúrese de que esté enviando correos electrónicos de la forma que Ud. desea. Ahora puede proseguir con la instalación de *ESETS*.

Tome la ruta completa al MDA Postfix actual y modifique el parámetro 'mda_path' en la sección [mda] del *archivo de configuración* de *ESETS* con este valor, en nuestro ejemplo:

```
mda_path = "/usr/bin/procmail"
```

y reinicie el *daemon* de *ESETS*. Luego reemplace la ruta al MDA Postfix actual por la ruta a **esets_mda** agregando -- --recipient="$RECIPIENT" --sender="$SENDER" a los argumentos, en nuestro ejemplo:

```
mailbox_command = @BINDIR@/esets_mda -d "$USER"
-- --recipient="$RECIPIENT" --sender="$SENDER"
```

Para que se active la configuración recién creada, reinicie Postfix.

A.1.2. Análisis de mensajes de correo bidireccionales

El objetivo de esta instalación es desviar todos los correo electrónicos desde Postfix a **esets_smtp** y regresarlos a Postfix. En la sección [smtp] del *archivo de configuración* de *ESETS* ingrese:

```
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
```

y reinicie el *daemon* de *ESETS*. El *daemon* activará **esets_smtp**, hará que analice todas las comunicaciones SMTP aceptadas en 'listen_addr:listen_port' y las reenviará a 'server_addr:server_port'. Para desviar todos los correos electrónicos a **esets_smtp** ingrese en Postfix:

```
content_filter = smtp:[127.0.0.1]:2526
```

NOTA: En caso de que el parámetro 'content_filter' ya tenga un valor asignado, no siga estas instrucciones. En cambio, deberá insertar **esets_smtp** (u otro módulo para análisis de correo electrónico de *ESETS*) antes o después del filtrador de contenido actual 'content_filter'.

El último paso es lograr que Postfix acepte correos electrónicos en el puerto 2525 y continúe procesándolos. Ingrese las siguientes líneas en el archivo master.cf de Postfix:

```
localhost:2525 inet  n - n - - smtpd
  -o content_filter=
  -o myhostname=esets.yourdomain.com
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
```

simplemente reemplace yourdomain.com por el nombre de su propio *host*, luego del primer punto. Verifique que todas las líneas menos la primera tengan sangría. Para que se active la configuración recién creada, reinicie Postfix.

NOTA: En caso de que SELinux esté habilitado, lo que impide que Postfix atienda el puerto 2525 (por ejemplo, Fedora Code >=5), ejecute este comando: semanage -a -t smtp_port_t-p tcp 2525.

A.2. Configuración de *ESETS* para el MTA Sendmail

A.2.1. Análisis de mensajes de correo entrantes

Advertencia: Esta instalación no es compatible con SELinux. Deshabilite SELinux o prosiga a la siguiente sección.

El objetivo de esta instalación es insertar **esets_mda** antes del MDA original de Sendmail.

NOTA: En FreeBSD, Sendmail puede estar comunicándose con el MDA usando el protocolo LMTP. Sin embargo, **esets_mda** no entiende el protocolo LMTP. Por lo tanto, si en 'hostname'.mc aparece FEATURE(local_lmtp), elimínelo y vuelva a crear el archivo sendmail.cf.

El MDA actualmente en uso puede encontrarse en el archivo sendmail.cf en la sección Mlocal: parámetros 'P' (ejecutable) y 'A' (su nombre y sus argumentos).

Primero configure 'mda_path' en la sección [mda] del *archivo de configuración* de *ESETS* para el ejecutable del MDA en uso (parámetro 'P' de Sendmail) y reinicie el *daemon* de *ESETS*.

Luego agréguele al archivo sendmail.mc (o `hostname`.mc en FreeBSD) las siguientes líneas antes de todas las definiciones de MAILER:

```
define(`LOCAL_MAILER_PATH', `@BINDIR@/esets_mda')dnl
define(`LOCAL_MAILER_ARGS',
  `esets_mda original_arguments -- --sender $f --recipient $u@$j')dnl
```

donde original_arguments es el parámetro 'A' de Sendmail sin el nombre (primera palabra).

Por último, vuelva a crear el archivo sendmail.cf y reinicie Sendmail.

A.2.2. Análisis de mensajes de correo bidireccionales

El objetivo de esta instalación es analizar todos los correos electrónicos de Sendmail con el filtro **esets_smfi**. En la sección [smfi] del *archivo de configuración* de *ESETS* configure los parámetros:

```
agent_enabled = yes
smfi_sock_path = "/var/run/esets_smfi.sock"
```

y reinicie el *daemon* de *ESETS*. Luego agregue al archivo sendmail.mc (o `hostname`.mc en FreeBSD) la siguiente línea antes de todas las definiciones de MAILER:

```
INPUT_MAIL_FILTER(`esets_smfi',
  `S=local:/var/run/esets_smfi.sock, F=T, T=S:2m;R:2m;E:5m')dnl
```

Según esta configuración, Sendmail se comunicará con **esets_smfi** a través del *socket* de unix /var/run/esets_smfi.sock. La bandera F=T provocará una falla de conexión temporaria si el filtro no está disponible. El tiempo de espera S:2m indica 2 minutos de espera para el envío de información desde el MTA al filtrador, R:2m indica 2 minutos de espera para la lectura de la respuesta del filtrador y E:5m significa que el tiempo de espera total desde el envío del fin de mensaje al filtrador y la demora de la confirmación final es de 5 minutos.

Recuerde que si se configuran los tiempos de espera para el filtro **esets_smfi** con valores demasiado chicos, Sendmail puede desviar el mensaje temporariamente a la cola de espera para volver a intentar enviarlo más tarde. Esto puede ocasionar que se envíen a la cola los mismos mensajes en forma reiterada. Para evitar el problema, los tiempos de espera deben ser configurados apropiadamente. También se pueden configurar desde el parámetro de Sendmail 'confMAX_MESSAGE_SIZE', que corresponde al tamaño máximo aceptado del mensaje (en bytes). Teniendo en cuenta este valor y el tiempo máximo que tarda el MTA para procesar esa cantidad de datos (lo cual se puede medir), es posible evaluar los tiempos de espera apropiados para el filtro **esets_smfi**.

Al final, vuelva a crear el archivo sendmail.cf y reinicie Sendmail.

A.3. Configuración de *ESETS* para el MTA Qmail

A.3.1. Análisis de mensajes de correo entrantes

El objetivo de esta instalación es insertar **esets_mda** antes del agente de reparto local de Qmail. Si, por ejemplo, Qmail estuviera instalado en el directorio /var/qmail, en la sección [mda] del *archivo de configuración* de *ESETS* ingrese el siguiente parámetro:

```
mda_path = "/var/qmail/bin/qmail-esets_mda"
```

y reinicie el *daemon* de *ESETS*. Cree el archivo /var/qmail/bin/qmail-esets_mda con el siguiente contenido y ejecute chmod a+x:

```
#!/bin/sh
exec qmail-local -- "$USER" "$HOME" "$LOCAL" "" "$EXT" \
     "$HOST" "$SENDER" "$1"
```

Esto hará que **esets_mda** llame al agente de reparto local de Qmail. Ahora cree el archivo /var/qmail/bin/qmail-start.esets con el siguiente contenido y vuelva a ejecutar chmod a+x:

```
#!/bin/sh
A="$1"; shift
```

```
exec qmail-start.orig "|@BINDIR@/esets_mda '$A'"' \
     -- --sender="$SENDER" --recipient="$RECIPIENT"' "$@"
```

lo que iniciará Qmail usando **esets_mda** para repartos locales. No obstante, la especificación de reparto original será transmitida a qmail-local a través de **esets_mda**. Recuerde que en esta configuración **esets_mda** usará los códigos de salida de Qmail reconocidos (ver qmail-command(8)). Por último, reemplace qmail-start usando los comandos:

```
mv /var/qmail/bin/qmail-start /var/qmail/bin/qmail-start.orig
ln -s qmail-start.esets /var/qmail/bin/qmail-start
```

y reinicie Qmail.

A.3.2. Análisis de mensajes de correo bidireccionales

El objetivo de esta instalación es insertar **esets_mda** antes de qmail-queue, que pone en cola de espera todos los correos antes de su distribución. Si Qmail estuviera instalado en el directorio /var/qmail, en la sección [mda] del *archivo de configuración* de *ESETS* ingrese el parámetro:

```
mda_path = "/var/qmail/bin/qmail-queue.esets"
```

y reinicie el *daemon de ESETS*. Al final, reemplace qmail-queue usando los comandos:

```
mv /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.esets
ln -s @BINDIR@/esets_mda /var/qmail/bin/qmail-queue
```

No es necesario reiniciar Qmail. Todos los mensajes que a partir de este momento lleguen a la cola serán analizados por *ESETS*. Recuerde que en esta configuración **esets_mda** utilizará los códigos de salida de qmail-queue (ver qmail-queue(8)).

A.4. Configuración de *ESETS* para el MTA Exim versión 3

A.4.1. Análisis de mensajes de correo entrantes

El objetivo de esta instalación es crear un transporte Exim desde **esets_mda** para usuarios locales. En la sección [mda] del *archivo de configuración* de *ESETS* ingrese el parámetro:

```
mda_path = "/usr/sbin/exim"
```

donde /usr/sbin/exim es la ruta completa al archivo binario de Exim. Reinicie el *daemon* de ESETS. Luego agregue el siguiente transporte a la lista de transportes de Exim (en cualquier lugar):

```
esets_transport:
  driver = pipe
  command = @BINDIR@/esets_mda -oMr esets-scanned $local_part@$domain \
    -- --sender=$sender_address --recipient=$local_part@$domain
  user = mail
```

donde "mail" es un usuario de la categoría 'trusted_users' de Exim. Luego agregue el siguiente director a la lista de directores:

```
esets_director:
```

```
  driver = smartuser
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

lo que enviará todos los correos aún no analizados para usuarios locales a **esets_mda**, que los devolverá a Exim para seguir siendo procesados. Para activar la nueva configuración, reinicie Exim.

A.4.2. Análisis de mensajes de correo bidireccionales

El objetivo de esta instalación es crear un transporte Exim desde **esets_mda** para todos los correos. Realice todos los pasos de la sección anterior, pero además agregue el siguiente *router* como el primero de la lista de *routers* de Exim:

```
esets_router:
  driver = domainlist
  route_list = "* localhost byname"
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

A.5. Configuración de *ESETS* para el MTA Exim versión 4

A.5.1. Análisis de mensajes de correo entrantes

El objetivo de esta instalación es crear un transporte Exim desde **esets_mda** para los usuarios locales. En la sección [mda] del *archivo de configuración* de *ESETS* configure este parámetro:

```
  mda_path = "/usr/sbin/exim"
```

donde /usr/sbin/exim es la ruta completa al archivo binario de Exim. Reinicie el *daemon* de *ESETS*. Luego, agregue el siguiente *router* como el primero de la lista de *routers* de Exim:

```
esets_router:
  driver = accept
  domains = +local_domains
  condition = "${if eq {$received_protocol}{esets-scanned} {0}{1}}"
  transport = esets_transport
  verify = false
```

y el siguiente transporte (en cualquier lugar) a la lista de transportes de Exim:

```
esets_transport:
  driver = pipe
  command = @BINDIR@/esets_mda -oMr esets-scanned $local_part@$domain \
   -- --sender=$sender_address --recipient=$local_part@$domain
```

lo que enviará todos los correos aún no analizados para usuarios locales a **esets_mda**, que los devolverá a Exim para seguir siendo procesados. Para activar la nueva configuración, reinicie Exim.

A.5.2. Análisis de mensajes de correo bidireccionales

El objetivo de esta instalación es crear un transporte Exim desde **esets_mda** para todos los correos. Realice todos los pasos de la sección anterior (A.4.2), pero omita la siguiente línea en esets_router:

```
domains = +local_domains
```

A.6. Configuración de *ESETS* para análisis de mensajes salientes

El análisis de mensajes de correo electrónico salientes se realiza usando el *daemon* de **esets_smtp**. En la sección [smtp] del *archivo de configuración* de *ESETS* ingrese los siguientes parámetros:

```
agent_enabled = yes
listen_addr = ”192.168.1.0”
listen_port = 2525
```

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

```
ipchains -A INPUT -p tcp -i if0 --dport 25 -j REDIRECT 2525
```

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

```
iptables -t nat -A PREROUTING -p tcp -i if0 \
  --dport 25 -j REDIRECT --to-ports 2525
```

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

```
ipfw add fwd 192.168.1.10,2525 tcp from any to any 25 via if0 in
```

Advertencia: El MTA puede aceptar todas las conexiones sin un análisis extensivo de **esets_smtp** porque son locales. Al utilizar sus propias reglas de *firewall*, asegúrese de no crear un *open relay*, es decir, permitir la conexión de una persona a **esets_smtp** desde el exterior y usarlo como servidor SMTP *relay* enviando correo electrónico a través de él.

A.7. Configuración de *ESETS* para el análisis de comunicación POP3

El análisis de la comunicación en POP3 se lleva a cabo usando el *daemon* de **esets_pop3**. En la sección [pop3] del *archivo de configuración* de *ESETS* ingrese los siguientes parámetros:

```
agent_enabled = yes
listen_addr = ”192.168.1.10”
listen_port = 8110
```

donde 'listen_addr' es la dirección de la interfaz de red local llamada if0. Luego reinicie el *daemon* de *ESETS*. El siguiente paso es redirigir todos los pedidos POP3 a **esets_pop3**. En el caso del filtrador del protocolo IP provisto por la herramienta administrativa de ipchains, la regla apropiada es:

```
ipchains -A INPUT -p tcp -i if0 --dport 110 -j REDIRECT 8110
```

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

```
iptables -t nat -A PREROUTING -p tcp -i if0 \
--dport 110 -j REDIRECT --to-ports 8110
```

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

```
ipfw add fwd 192.168.1.10,8110 tcp from any to any 110 via if0 in
```

A.8. Configuración de *ESETS* para el análisis de comunicación IMAP

El análisis de comunicación IMAP se lleva a cabo usando el *daemon* de **esets_imap**. En la sección [imap] del *archivo de configuración de ESETS* ingrese estos parámetros:

```
agent_enabled = yes
listen_addr = ”192.168.1.10”
listen_port = 8143
```

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

```
ipchains -A INPUT -p tcp -i if0 --dport 143 -j REDIRECT 8143
```

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

```
iptables -t nat -A PREROUTING -p tcp -i if0 \
  --dport 143 -j REDIRECT --to-ports 8143
```

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

```
ipfw add fwd 192.168.1.10,8143 tcp from any to any 143 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.