ESET
Mail Security

Руководство по установке
и документация для пользователя

we protect your digital worlds

Содержание

ESET Mail Security

REV.20071112-003

1. Введение

Позвольте поздравить вас с приобретением ESET Mail Security – одной из лучших систем безопасности, работающих под управлением операционных систем Linux и BSD. Благодаря ультрасовременному ядру сканирования ESET система достигает непревзойденной скорости сканирования и уровня обнаружения при минимальном использовании системных ресурсов, что делает ее идеальной для серверных операционных систем Linux и BSD.

В этой главе рассматриваются основные характеристики системы.

- Алгоритм работы антивирусного ядра сканирования ESET обеспечивает высочайший уровень обнаружения и скорость сканирования.
- Система ESET Mail Security разработана для использования как в однопроцессорных, так и в многопроцессорных системах.
- Предоставляет уникальную расширенную эвристику для обнаружения червей и «бэкдоров» в Win32.
- Встроенные архиваторы распаковывают заархивированные объекты без использования сторонних программ.
- Архитектура решения основана на использовании демона (резидентной программы), к которому отправляются все запросы на сканирование. Благодаря такому решению повышается скорость и эффективность работы системы.
- Система позволяет выполнять настройку как для индивидуальных пользователей, так и для пользователей клиент-серверного уровня.
- Для получения информации о работе системы и проникших вирусах могут быть настроены шесть уровней ведения журналов.
- Для установки ESET Mail Security не требуются внешние библиотеки или программы, кроме LIBC.
- Система может направлять предупреждение о проникновении угрозы любому сотруднику, в зависимости от настроек.
- Система содержит механизм управления защитой от спама.
- Возможность настройки для добавления информации о проникновениях в заголовок, нижний колонтитул или тему сообщения электронной почты.

Для эффективной работы приложению ESET Mail Security требуется всего 16 МБ пространства на жестком диске и 32 МБ оперативной памяти.

Программа без помех работает с версиями ядра Linux 2.2.x, 2.4.x и 2.6.x, а также с версиями 5.x и 6.x ядра операционной системы FreeBSD.

Как для маломощных серверов небольших офисов, так и для ISP-серверов корпоративного класса с тысячами пользователей система обеспечивает работоспособность и масштабируемость, свойственные UNIX-решениям, наряду с непревзойденной безопасностью продуктов ESET.

2. Терминология и сокращения

Далее рассматриваются термины и сокращения, используемые в настоящей документации. Обратите внимание, что в этой документации (только для PDF-формата) полужирный шрифт используется для выделения названий компонентов продукта, а в этой главе – также для выделения новых терминов и сокращений. Также обратите внимание, что термины и сокращения, описанные в данной главе, будут выделяться и в других главах данной документации (только в PDF-формате).

ESETS

ESET Security – распространенное сокращение для всех продуктов, разрабатываемых под маркой ESET spol. s r.o. для операционной системы Linux (и для операционной системы BSD). Также это название (или часть названия) пакета программного обеспечения, в состав которого включены наши продукты.

RSR

Сокращение для **RedHat/Novell(SuSE) Ready**. Обратите внимание, что реализована поддержка вариантов продукта RedHat Ready и Novell(SuSE) Ready. Отличие от «стандартной» версии Linux в том, что пакет RSR соответствует критериям описанным в FHS (стандарт иерархии файловой системы (File-system Hierarchy Standard), который определяется как часть базы стандартов Linux) – документе, который требуется для сертификации RedHat Ready и Novell(SuSE) Ready. Это означает, к примеру, что RSR-пакет устанавливается как приложение-надстройка, то есть основным каталогом установки является **/opt/eset/esets**.

Демон ESETS

Основной демон управления и сканирования системы ESETS – esets_daemon.

Основной каталог ESETS

Каталог, в котором хранятся загружаемые модули ESETS, в том числе, например, база данных вирусных сигнатур. Далее в документации для данного каталога используется сокращение @BASEDIR@. Путь каталога:

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

Каталог настроек ESETS

Каталог для хранения всех файлов, связанных с настройками ESET Mail Security. Далее в документации для данного каталога используется сокращение @ETCDIR@. Путь каталога:

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

Файл настроек ESETS

Основной файл настроек ESET Mail Security. Полный путь к файлу:

@ETCDIR@/esets.cfg

Каталог двоичных файлов ESETS

Каталог, в котором хранятся двоичные файлы, относящиеся к ESET Mail Security. Далее в документации для данного каталога используется сокращение @BINDIR@. Путь каталога:

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

Каталог системных двоичных файлов ESETS

Каталог, в котором хранятся двоичные файлы, относящиеся к ESET Mail Security. Далее в документации для данного каталога используется сокращение @SBINDIR@. Путь каталога:

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

Каталог объектных файлов ESETS

Каталог, в котором хранятся объектные файлы и библиотеки, относящиеся к ESET Mail Security. Далее в документации для данного каталога используется сокращение @LIBDIR@. Путь каталога:

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

3. Установка

Настоящий продукт распространяется в виде двоичного файла

esets.i386.ext.bin

При этом **ext** – суффикс, зависящий от дистрибутива операционной системы Linux или BSD, то есть, **deb** для Debian, **rpm** для RedHat и SuSE, **tgz** для других дистрибутивов Linux, **fbs5.tgz** для FreeBSD 5.xx и **fbs6.tgz** для FreeBSD 6.xx.

Обратите внимание, что формат двоичного файла для Linux RSR выглядит следующим образом:

esets-rsr.i386.rpm.bin

Для установки или обновления продукта используйте оператор

sh ./esets.i386.ext.bin

Соответственно, для версии продукта для Linux RSR используйте оператор

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

В результате выполнения оператора на экране будет отображено приглашение о принятии условий лицензионного соглашения для данного продукта. После подтверждения принятия условий лицензионного соглашения установочный пакет сохраняется в текущий рабочий каталог и на терминал выводится информация, относящаяся к установке, удалению или обновлению программного обеспечения.

Сразу после установки пакета и запуска основной службы ESETS работу приложения в операционной системе Linux можно проверить при помощи команды

ps -C esets_daemon

Для операционной системы BSD используется похожая команда

ps -ax esets_daemon | grep esets_daemon

В результате выводится следующее (или сходное с ним) сообщение.

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

То есть должны быть представлены как минимум два процесса демона ESETS, выполняющиеся в фоновом режиме. Один из этих процессов – так называемый диспетчер процессов и потоков системы. Второй – процесс сканирования ESETS.

4. План продукта

После успешной установки пакета продукта следует ознакомиться с его содержимым.

Структура ESET Mail Security показана на рисунке 4–1. Система состоит из представленных далее компонентов.

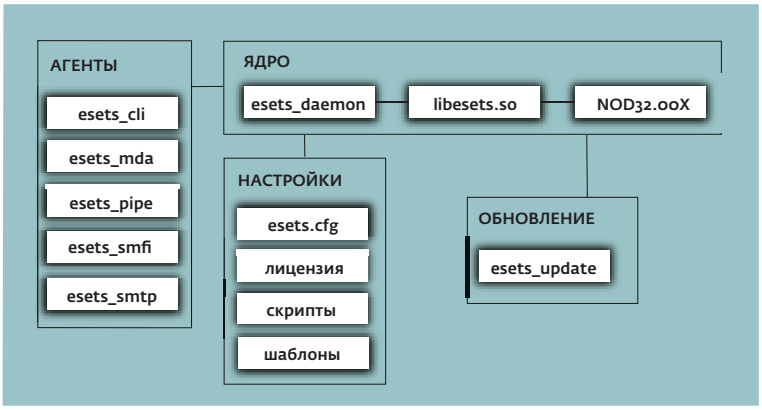

Рис. 4–1. Структура ESET Mail Security

ЯДРО

Ядро ESET Mail Security включает демон ESETS – esets_daemon. Этот демон использует библиотеку ESETS libesets.so и загружаемые модули ESETS nod32.00X для обеспечения основных системных задач: сканирования, обслуживания агентских процессов демона, обслуживания системы предоставления образцов, ведения журналов, уведомлений и так далее. Для получения дополнительных сведений обратитесь к странице руководства esets_daemon(8).

АГЕНТЫ

Модули-агенты ESETS предназначены для интеграции ESETS в серверную среду Linux/BSD. Обратите внимание, что в настоящей документации данной теме посвящена отдельная глава.

ОБНОВЛЕНИЕ

Служебная программа обновления является особой частью системы. Она была разработана для обновления загружаемых модулей ESETS, например, базы данных вирусных сигнатур, поддержки архивов, поддержки расширенной эвристики и так далее. Обратите внимание, что в настоящей документации данной теме посвящена отдельная глава.

НАСТРОЙКИ

Правильная настройка является важнейшим условием работы системы. Поэтому далее в этой главе будут рассмотрены все соответствующие компоненты. Настоятельно рекомендуется также ознакомиться со страницей руководства esets.cfg(5), на которой представлена важная информация относительно настроек ESETS.

После успешной установки продукта все компоненты настроек сохраняются в каталоге настроек ESETS. Этот каталог содержит следующие файлы.

@ETCDIR@/esets.cfg

Это наиболее важный файл настроек, так как он обслуживает большую часть выполняемых продуктом функций. Просмотрев файл, вы заметите, что он составляется из различных параметров, распределенных по разделам. Обратите внимание, что названия разделов всегда заключены в квадратные скобки. В файле настроек ESETS всегда присутствует один глобальный и несколько так называемых агентских разделов. Параметры глобального раздела предназначены для определения опций настройки демона ESETS, а также значений, используемых по умолчанию для опций настроек ядра сканирования ESETS. Параметры в агентских разделах используются для определения опций настройки так называемых агентов, то есть модулей, используемых для перехвата различных потоков данных в компьютере или его окружении и для подготовки этих данных к сканированию. Обратите внимание, что кроме множества параметров, используемых для настройки системы, существует также некоторое количество правил, определяющих организацию файла. Чтобы получить дополнительные сведения, см. страницы руководства esets.cfg(5), esets_daemon(8), а также страницы, посвященные соответствующим агентам.

@ETCDIR@/certs

В данном каталоге хранятся сертификаты, используемые веб-интерфейсом ESETS в целях аутентификации (подробные сведения см. веб-интерфейс на странице esets_wwwi(8)).

@ETCDIR@/license

В этом каталоге хранятся лицензионные ключи продуктов, полученные от поставщика. Обратите внимание, что для проверки валидности лицензионных ключей демон ESETS всегда проверяет только этот каталог, если это не переопределено параметром **lic_dir** в файле настроек ESETS.

@ETCDIR@/scripts/license_warning_script

Если в файле настроек ESETS установлен флажок параметра **license_warn_enabled**, этот скрипт начнет выполняться за 30 дней до истечения срока лицензии и будет выполняться ежедневно. Он предназначен для отправки системному администратору по электронной почте предупреждения об истечении срока лицензии.

@ETCDIR@/scripts/daemon_notification_script

Данный скрипт, если он включен параметром **exec_script** файла настроек ESETS, выполняется, если системой антивируса обнаружено проникновение. Он предназначен для отправки системному администратору по электронной почте уведомлений о событиях.

@ETCDIR@/anti-spam

В этом каталоге содержится файл настроек, необходимый для точной настройки работы ядра защиты от спама.

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

Эти файлы представлют собой HTML-шаблоны для определения текста сообщений, вставляемых в виде сноски в просканированные сообщения электронной почты. Чтобы активировать эти HTML-шаблоны, из всех имен файлов шаблонов следует удалить суффикс **example**. Обратите также внимание на то, что внешний вид сносок в сообщениях электронной почты определяется в файле настроек ESETS параметром **write_to_footnote.** Далее описаны значения отдельных файлов шаблонов.

Следующие шаблоны сносок используются в сообщениях электронной почты, определенных как зараженные.

Заголовок сообщения электронной почты	От (From):
.	Кому (To):
Тело сообщения электронной почты	текст сообщения электронной почты
.	содержимое файла lms_sig_header_infected.html
.	список проникновений, обнаруженных при сканировании
.	содержимое файла lms_sig_footer_infected.html

Следующие шаблоны сносок используются в сообщениях электронной почты, определенных как незараженные.

Заголовок сообщения электронной почты	От (From):
.	Кому (To):
Тело сообщения электронной почты	текст сообщения электронной почты
.	содержимое файла lms_sig_header_clean.html
.	список объектов, проверенных при сканировании
.	содержимое файла lms_sig_footer_clean.html

Следующие шаблоны сносок добавляются в сообщения электронной почты, которые не удалось проверить.

Заголовок сообщения электронной почты	От (From):
.	Кому (To):
Тело сообщения электронной почты	текст сообщения электронной почты
.	содержимое файла lms_sig_header_not_scanned.html
.	список объектов, проверенных при сканировании
.	содержимое файла lms_sig_footer_not_scanned.html

5. Интеграция с системами передачи сообщений по электронной почте

В данной главе описывается интеграция приложения ESET Mail Security с различными распространенными системами передачи сообщений по электронной почте. Общее представление об основных принципах работы систем, используемых для передачи сообщений по электронной почте (рисунок 5–1), особенно важно для понимания работы системы ESETS.

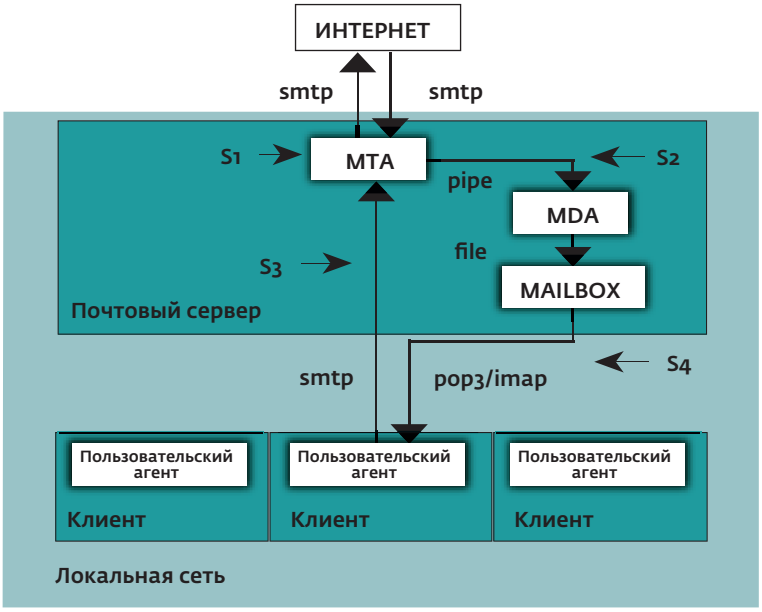

Рис. 5–1. Схема системы передачи сообщений по электронной почте в операционной системе UNIX

MTA – агент пересылки сообщений (Mail Transport Agent)

Программа (например, sendmail, postfix, qmail, exim и др.), обеспечивающая перенос сообщений электронной почты между локальными и удаленными доменами.

MDA – агент доставки электронной почты (Mail Delivery Agent)

Программа (например, maildrop, procmail, deliver, local.mail и др.), обеспечивающая доставку сообщений электронной почты с локальным адресом на почтовый ящик получателя.

MUA – клиент электронной почты (Mail User Agent)

Программа (например, MS Outlook, Mozilla Mail, Eudora и др.), обеспечивающая доступ к сообщениям электронной почты, сохраненным в электронном почтовом ящике, и управление этими сообщениями (чтение, создание нового сообщения, вывод на печать и т. д.).

ПОЧТОВЫЙ ЯЩИК

Файл или файловая структура на диске, используемые в качестве хранилища для сообщений электронной почты. Обратите внимание, что в операционных системах Linux/BSD имеется несколько форматов почтовых ящиков: устаревший формат, при котором сообщения каждого пользователя сохраняются последовательно в одном соответствующем пользователю файле в каталоге **/var/ spool/mail**; формат MBOX (более новый по сравнению с предыдущим, но также устаревший), при котором сообщения сохраняются последовательно в одном файле, расположенном в домашнем каталоге пользователя; MAILDIR, при котором сообщения электронной почты сохраняются в отдельных файлах в иерархической структуре каталогов.

Передача данных на сервер электронной почты осуществляется, как правило, посредством протокола SMTP –(Simple Mail Transfer Protocol). Полученное сообщение либо передается агентом MTA в другую удаленную систему передачи сообщений по электронной почте, либо доставляется локальным агентом MDA на конкретный почтовый ящик (предполагается, что у каждого пользователя локальной сети имеется собственный почтовый ящик на жестком диске сервера). Обратите внимание, что загрузка и правильная интерпретация сообщения на пользовательском компьютере входят в задачи локального агента MUA пользователя. При извлечении данных из почтового ящика для взаимодействия с агентом MTA агенты MUA обычно используют протоколы POP3 (Post Office Protocol) или IMAP (Internet Message Access Protocol). Отправка данных через Интернет осуществляется по протоколу SMTP.

В основе принципов работы ESETS лежит перехват в процессе обмена данными и сканирование на различных стадиях их передачи. Точки перехвата обозначены на рисунке 4–1 символами S1, S2, S3 и S4.

S1
Двунаправленное сканирование сообщений электронной почты, то есть фильтрация содержимого в MTA.

S2
Сканирование входящих сообщений электронной почты, т. е. сообщений с таким адресом назначения, который соответствует назначению в области локального домена.

S3
Сканирование исходящих сообщений электронной почты, т. е. сообщений, связанных посредством адреса назначения с каким-либо удаленным интернет-доменом.

S4
Сканирование собщений электронной почты, загружаемых с сервера POP3/IMAP.

Далее в этой главе рассматриваются методы интеграции продуктов ESETS с различными поддерживаемыми системами передачи сообщений по электронной почте.

5.1. Двунаправленное сканирование сообщений электронной почты в MTA

Преимуществом режима двунаправленного сканирования сообщений электронной почты является возможность сканирования как входящих, так и исходящих сообщений по одному алгоритму действий. С другой стороны, двунаправленный метод (фильтр содержимого) зависит от агента MTA. В системе ESET реализовано четыре фильтра содержимого – для наиболее распространенных агентов MTA: Sendmail, Postfix, Exim и QMail.

Чтобы в приложении ESET Mail Security настроить двунаправленное сканирование сообщений электронной почты, необходимо убедиться в правильной настройке и функционировании самого агента MTA. Затем выполните следующий скрипт.

esets_setup

Выберите соответствующий MTA и опции установки фильтра содержимого. На экране будет также отображен используемый модуль ESETS.

Обратите внимание, что программа установки создает резервные копии всех изменяемых файлов настройки и может отобразить все команды, которые будут выполнены после подтверждения пользователем. Этот же скрипт позволяет удалить продукт с компьютера. Подробное описание этапов для всех возможных сценариев содержится в приложении A настоящей документации.

5.2. Сканирование входящих сообщений электронной почты

Сканирование входящих сообщений электронной почты выполняется во время передачи сообщения между агентами MTA и MDA. Входящее сообщение перехватывается модулем esets_mda, сканируется демоном ESETS и доставляется в почтовый ящик при помощи исходного агента MDA. Как представлено на рисунке, сканирование на наличие вирусов включается при установке соответствующей настройки агента MTA и модуля esets_mda. Обратите внимание, что в приложении ESET Mail Security реализована поддержка наиболее распространенных агентов MTA: Sendmail, Postfix, Exim и QMail. Система ESETS поддерживает любые агенты MDA. Были протестированы, в частности, следующие агенты MDA: procmail, maildrop, deliver и local.mail.

Чтобы в приложении ESET Mail Security настроить сканирование входящих сообщений электронной почты, необходимо убедиться, что агент MTA правильно настроен при помощи исходного агента MDA и запущен. Затем выполните следующий скрипт.

esets_setup

Выберите соответствующий MDA и опции установки входящих соединений. На экране также будет отображен используемый модуль ESETS.

Обратите внимание, что программа установки создает резервные копии всех изменяемых файлов настройки и может отобразить все команды, которые будут выполнены после подтверждения пользователем. Этот же скрипт позволяет удалить продукт с компьютера. Подробное описание этапов для всех возможных сценариев содержится в приложении A настоящей документации.

5.3. Сканирование исходящих сообщений электронной почты

Сканирование исходящих сообщений электронной почты выполняется во время передачи сообщений между локальным агентом MUA и агентом MTA.

Чтобы в приложении ESET Mail Security настроить сканирование исходящих сообщений электронной почты, выполните следующий скрипт.

esets_setup

Выберите опции установки протокола SMTP. Это приведет к настройке модуля esets_smtp на прослушивание предопределенного порта и перенаправление соответствующих IP-пакетов. Проверьте добавленное правило файервола и переместите или измените его по своему усмотрению.

Обратите внимание, что программа установки создает резервные копии всех изменяемых файлов настройки и может отобразить все команды, которые будут выполнены после подтверждения пользователем. Этот же скрипт позволяет удалить продукт с компьютера. Подробное описание этапов для всех возможных сценариев содержится в приложении A настоящей документации.

5.4. Сканирование собщений электронной почты, загружаемых с сервера POP3/IMAP

Чтобы в приложении ESET Mail Security настроить сканирование сообщений электронной почты, загружаемых с сервера POP3 (или, соответственно, IMAP), выполните следующий скрипт.

esets_setup

Выберите опции установки протокола POP3 или IMAP. Это приведет к настройке отображенного модуля ESETS на прослушивание предопределенного порта и перенаправление соответствующих IP-пакетов. Проверьте добавленное правило файервола и переместите или измените его по своему усмотрению.

Обратите внимание, что программа установки создает резервные копии всех изменяемых файлов настройки и может отобразить все команды, которые будут выполнены после подтверждения пользователем. Этот же скрипт позволяет удалить продукт с компьютера. Подробное описание этапов для всех возможных сценариев содержится в приложении A настоящей документации.

5.5. Другие методы фильтрации содержимого

5.5.1. Сканирование сообщений электронной почты при помощи AMaViS

AMaViS – сканер для поиска вирусов в почтовых вложениях – средство, служащее интерфейсом для агента MTA и различных антивирусных сканеров.

Этот сканер поддерживает различные агенты MTA и поставляется в трех вариантах: amavis, amavisd и amavisd-new. Взаимодействие сканера Amavis и приложения ESET Mail Security осуществляется посредством модуля esets_cli. Прежде чем перейти к подробному объяснению конфигурации Amavis, рассмотрим влияние этого метода на функциональность приложения ESET Mail Security.

Обратите внимание, что средство Amavis не допускает изменения просканированных сообщений электронной почты. В результате этого зараженные вложения электронной почты не могут быть очищены или удалены системой ESETS. В электронные сообщения не будут также добавлены сноски ESETS, в которых содержатся определяющиеся журналом и статусом поля заголовка. Кроме того, программа amavis не учитывает отправителей и получателей почты, что препятствует использованию особых пользовательских настроек. Для модуля esets_cli ограничены также возможности обработки сообщений (принять, отложить, сбросить, отклонить). И наконец, программа сканирует файлы и в результате этого не может использовать ядро защиты от спама ESETS.

Учитывая эти недостатки, данную конфигурацию целесообразно использовать только в том случае, если особенности продукта для пользователя несущественны.

5.5.1.1. amavis

Настройка средства Amavis выполняется во время его установки. После распаковки исходного файла **amavis-0.x.y.tgz** создайте файл **amavis/av/esets_cli** со следующим содержимым.

```
#
# Программное обеспечение ESET, интерфейс командной строки ESETS
#
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, «Ошибка при проверке на вирус: $esets_cli (код ошибки: $errval)»);
        }
}
```

Обратите внимание, что в приведенном выше скрипте сообщения электронной почты принимаются только в том случае, если они приняты политикой обработки объектов модуля esets_cli. Во всех других случаях сообщения блокируются. При обнаружении вируса его имя извлекается из результатов.

Затем при использовании пакета Linux RSR переменную среды PATH необходимо обновить при помощи команды

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

Для успешной установки может потребоваться дополнительное программное обеспечение (например, arc, unarj, unrar, zoo). Кроме того, в каталоге **/usr/bin** несжатую символьную ссылку необходимо сжать в формат gzip и создать пользователя amavis в группе amavis с домашним каталогом **/var/amavis**. После этого продолжите обычный процесс установки (./configure, make, make install) и следуйте правилам **README.mta**, соответствующим вашему почтовому серверу.

5.5.1.2. amavisd

Настройка средства Amavisd выполняется во время его установки. Распакуйте исходный файл **amavisd-0.x.tgz** и следуйте правилам для средства amavis, описанным в предыдущем разделе данного руководства. После выполнения команды make install каталог **/usr/etc/amavisd.conf** может потребоваться перенести в /etc, после чего выполнить команду make install повторно.

5.5.1.3. amavisd-new

Чтобы установить продукт в версии Amavisd-new, распакуйте и установите исходный файл **amavisd- new-2.x.y.tgz** в своем каталоге установки. После этого настройте продукт при помощи только что установленного компонента **Amavisd-new**, в файле **amavisd.conf** удалите выражение **ESET Software ESETS** и замените выражение **ESET Software ESETS – Client/Server Version** на следующее:

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

Может потребоваться установка дополнительных модулей Perl с веб-узла www.cpan.org/modules: Archive-Tar, Archive-Zip, BerkeleyDB, Compress-Zlib, Convert-TNEF, Convert-UUlib, IO-stringy, MailTools, MIME-Base64, MIME-tools, Net-Server и Unix-Syslog. В каждом случае процедура будет следующей. perl Makefile.PL; make; make install.

По завершении настройки следуйте рекомендациям по настройке компонента Amavisd-new, приведенным в файле README.mta, который находится в каталоге Amavisd-new, соответствующем используемому почтовому серверу.

5.5.2. Сканирование электронных сообщений в приложении KerioMailServer

- Установите пакет ESET Mail Security, импортируйте файл лицензии и убедитесь в проведении регулярного обновления программами esets_daemon или, например, cron.
- Подключитесь к серверу Kerio MailServer, используя консоль администрирования Kerio Administrator Console.
- Выбрав пункты меню **Настройка** – **Фильтр содержимого** – **Антивирус** (Configuration > Content Filter > Antivirus), установите флажок **Использовать внешний антивирус** (Use external antivirus) и отметьте вариант **NOD32 для Linux** (NOD32 for Linux).
- Нажмите кнопку **Параметры** (Options) и обновите пути версии, отличной от RSR, следующим образом:

```
LicenseDirectory: /etc/esets/license
NodDll: /usr/lib/libesets.so
NodModulesPath: /var/lib/esets
TmpDirectory: /tmp
```

Для RSR-версии:

```
LicenseDirectory: /etc/opt/eset/esets/license
NodDll: /opt/eset/esets/lib/libesets.so
NodModulesPath: /var/opt/eset/esets/lib
TmpDirectory: /tmp
```

- Подтвердите изменения, нажав кнопку **Применить** (Apply).

6. Важные механизмы работы ESET Mail Security

6.1. Политика обработки объектов

Политика обработки объектов (см. рисунок 5–1) – это механизм, обеспечивающий обработку просканированных объектов в соответствии с их статусом сканирования. Механизм основан на так называемых опциях настройки действий (**action_on_processed, action_on_infected, action_on_uncleanable, action_on_notscanned, action_on_spam, action_on_spamnotscanned**) в сочетании с опциями настройки запуска антивируса и антиспама (**av_enabled, as_enabled**). Подробные сведения об этих опциях см. на странице руководства esets.cfg(5).

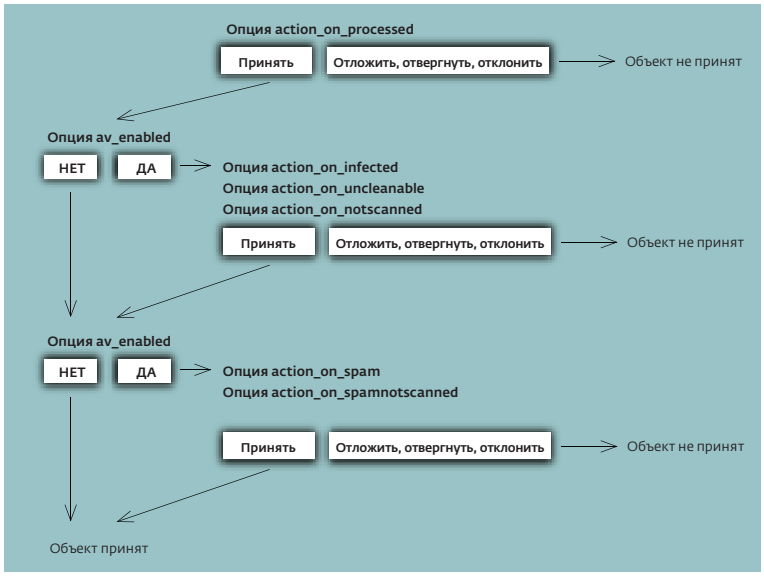

Рис. 6–1. Схема работы политики обработки объектов

Первоначально каждый объект обрабатывается в соответствии с установками опции настройки **action_on_processed**. Если выдается значение **принять** (accept), объект обрабатывается в соответствии со значением опции настройки **av_enabled**. Если опция **av_enabled** включена, объект сканируется на наличие вирусных проникновений и последующая его обработка зависит от значений, заданных в опциях настройки **action_on_infected, action_on_uncleanable** и **action_on_notscanned**. Если результатом вышеназванных опций будет значение **принять** (accept) или если опция **av_enabled** отключена, обрабатываемый объект будет просканирован на спам.Обратите внимание, что сканирование объекта на спам выполняется только при включенной опции настройки **as_enabled**. В этом случае учитываются опции настройки действия **action_on_spam** и **action_on_ spamnotscanned**. Если результатом этих действий будет значение **принять** (accept), либо если параметр **as_enabled** отключен, объект принимается для дальнейшей доставки; в противном случае объект блокируется и обрабатывается в соответствии с данной ситуацией.

6.2. Настройки пользователя

Механизм настроек пользователя введен в продукт для того, чтобы предоставить администратору более широкие возможности настройки. Благодаря этому параметры антивирусного сканера ESETS можно задавать выборочно для идентификации клиента/сервера.

Более подробное описание этих возможностей находится в разделе руководства, посвященном esets.cfg(5), а также в указанных там разделах. Поэтому здесь приводится только короткий пример настроек пользователя.

В данном примере модуль esets_smtp используется в качестве фильтра содержимого для агента MTA Postfix. Настройка модуля осуществляется в разделе [smtp] файла настроек ESETS. Раздел выглядит следующим образом.

```
[smtp]
agent_enabled = да
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
action_on_processed = reject
```

Для предоставления индивидуальных параметров настройки необходимо задать в параметре **user_config** путь к файлу специальных настроек, в котором хранятся индивидуальные настройки. В следующем примере создается ссылка на файл специальных настроек **esets_smtp_spec.cfg**, расположенный в каталоге настроек ESETS.

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

Создав в разделе [smtp] ссылку на файл специальных настроек, необходимо создать этот файл внутри каталога настроек ESETS и прописать в нем необходимые индивидуальные настройки. Следующий пример показывает индивидуальную настройку параметра **action_on_processed** для получателя rcptuser@rcptdomain.com.

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

Обратите внимание, что имя заголовка специального раздела содержит идентификацию получателя, для которого создаются индивидуальные настройки. Тело раздела содержит индивидуальные параметры, указанные для его идентификации. Таким образом, при помощи этой особой настройки обрабатываться (то есть сканироваться на наличие проникновений) будут все электронные сообщения, кроме адресованных rcptuser@rcptdomain.com – последние будут отклоняться без сканирования.

6.3. «Черный» и «белый» списки

На следующем примере демонстрируется создание «черного» и «белого» списков для агента esets_smtp, настроенного в качестве фильтра содержимого для агента MTA Postfix/ Обратите внимание, что для этих целей используется конфигурация, описанная в предыдущем разделе.

Таким образом, чтобы создать «черный» список для esets_smtp, в файле специальных настроек **esets_smtp_spec.cfg**, описанном в предыдущем разделе руководства, потребуется создать следующий раздел группы.

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

На следующем этапе в группу «черного» списка необходимо добавить несколько SMTP-серверов. Для этого нужно создать специальный раздел

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

где **sndrname1@sndrdomain1.com** – адрес отправителя электронных сообщений, добавленного в «черный» список. Обратите внимание, что при этой настройке отклоняются все электронные сообщения, отправленные с этого адреса.

Чтобы создать «белый» список для esets_smtp, в файле специальных настроек **esets_smtp_spec.cfg**, описанном в предыдущем разделе руководства, потребуется создать следующий раздел группы.

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

Добавление адреса отправителя электронной почты пояснений не требует.

Обратите внимание, что в имени заголовка особого раздела символ «|» помещается перед адресом отправителя, но отсутствует перед адресом получателя. Описание синтаксиса имен особых заголовков см. на страницах руководства, посвященных соответствующему агенту ESETS. Дополнительные сведения по агенту esets_smtp см. на странице руководства esets_smtp(1).

6.4. Управление антиспамом

Назначением антиспамовой системы является отсев всех спам-сообщений электронной почты (то есть сообщений, не востребованных получателем) из потока данных в процессе доставки электронных сообщений.

В целях избавления от спама в настоящем продукте реализован механизм управления антиспамом. Функцию антиспама можно включить при помощи параметра **as_enabled** (описание см. на странице руководства esets.cfg(5)). Обратите внимание на то, что антиспамовое сканирование можно применять только к объектам электронной почты, то есть данная функция относится только к модулям esets_imap, esets_mda, esets_pipe, esets_pop3, esets_smtp и esets_smfi.

Как только функция антиспама включена в каких-либо разделах настроек, во время основного запуска демона сканирования выполняется инициализация антиспамового механизма сканирования. Во время этого процесса из кэш-каталога антиспама загружаются соответствующие модули поддержки антиспама.

Функцию антиспама можно настроить и при помощи файла настроек:

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

Обратите внимание на количество файлов в этом каталоге: каждый соответствует отдельной рекомендуемой конфигурации антиспамового механизма. Обратите внимание, что файл настроек по умолчанию соответствует файлу настроек **spamcatcher.conf.faster**. Чтобы воспользоваться каким-либо из этих файлов, просто замените стандартный файл антиспамовых настроек **spamcatcher.conf** выбранным файлом и перезагрузите демон ESETS.

6.5. Система предоставления образцов

Система предоставления образцов представляет собой интеллектуальную технологию ThreatSense.NET, которая позволяет захватывать зараженные объекты, обнаруженные методом расширенных эвристик, и отправлять эти объекты на сервер системы отправки образцов. Все образцы вирусов, захваченные системой отправки образцов, обрабатываются в отделе вирусных лабораторий ESET и при необходимости добавляются в базу данных вирусов.

ПРИМЕЧАНИЕ. В СООТВЕТСТВИИ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ ВКЛЮЧЕНИЕМ СИСТЕМЫ ОТПРАВКИ ОБРАЗЦОВ ВЫ ПОДТВЕРЖДАЕТЕ СВОЕ СОГЛАСИЕ НА СБОР ДАННЫХ (КОТОРЫЕ МОГУТ СОДЕРЖАТЬ И ЛИЧНЫЕ СВЕДЕНИЯ О ПОЛЬЗОВАТЕЛЯХ КОМПЬЮТЕРА) И ОБРАЗЦОВ ПОСЛЕДНИХ ОБНАРУЖЕННЫХ ВИРУСОВ И ДРУГИХ УГРОЗ И ОТПРАВКУ ИХ В ВИРУСНУЮ ЛАБОРАТОРИЮ КОМПЬЮТЕРОМ И/ИЛИ ПЛАТФОРМОЙ, НА КОТОРЫХ УСТАНОВЛЕН МОДУЛЬ ESETS_DAEMON. ПО УМОЛЧАНИЮ ЭТА ФУНКЦИЯ ОТКЛЮЧЕНА. ЭТИ СВЕДЕНИЯ БУДУТ ИСПОЛЬЗОВАНЫ ИСКЛЮЧИТЕЛЬНО В ЦЕЛЯХ ИЗУЧЕНИЯ УГРОЗ. СОТРУДНИКИ ВИРУСНОЙ ЛАБОРАТОРИИ ПРЕДПРИНИМАЮТ СООТВЕТСТВУЮЩИЕ МЕРЫ ПО СОХРАНЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ТАКИХ ДАННЫХ.

Чтобы включить систему предоставления образцов, необходимо выполнить инициализацию кэша системы предоставления образцов. Достичь этого можно включением опции **samples_enabled** в разделе [global] файла настроек ESETS. Чтобы включить процесс доставки образцов на серверы вирусной лаборатории ESET, в этом же разделе необходимо включить параметр **samples_send_enabled**.

При помощи опций настройки **samples_provider_mail** и/или **samples_provider_ country** пользователи могут предоставить сотрудникам вирусной лаборатории ESET дополнительные необязательные сведения. Эти сведения позволяют получить обзор распространения проникновений в Интернете.

Подробные сведения о системе предоставления образцов см. на странице руководства esets_daemon(8).

6.6. Веб-интерфейс

Веб-интерфейс позволяет удобным для пользователя образом выполнять настройку ESETS, администрирование системы и управление лицензиями.

Этот модуль является отдельным агентом, и его необходимо явно включить. В целях быстрого запуска установите все перечисленные далее опции в файле настроек ESETS и перезапустите демон ESETS:

```
[wwwi]
agent_enabled = yes
listen_addr = адрес
listen_port = порт
username = имя
password = пароль
```

(для всех четырех значений введите свои собственные); введите в веб-браузере адрес https://address:port (обратите внимание на префикс «https») и зарегистрируйтесь в системе со своим именем и паролем. На странице справки приведены основные указания действий. Более подробные технические сведения о модуле esets_wwwi см. на странице руководства esets_wwwi(1).

7. Обновление системы ESET Mail Security

7.1. Программа обновления ESETS

В целях сохранения эффективности программы ESET Mail Security необходимо поддерживать актуальность базы данных вирусных сигнатур. Для этих целей была разработана программа esets_update (подробности см. на странице руководства esets_ update(8)). Чтобы запустить обновление, в разделе [update] файла настроек ESETS необходимо определить опции настройки **username** и **password**. Обратите внимание, что при организации доступа к Интернету через прокси-сервер HTTP здесь же необходимо задать дополнительные опции настройки: **proxy_addr**, **proxy_ port** и **proxy_username** (последний параметр необязателен). Чтобы запустить обновление, введите команду:

@SBINDIR@/esets_update

В целях обеспечения высочайшей безопасности пользователей сотрудники ESET постоянно собирают информацию о детектировании вредоносного ПО со всего мира. За очень небольшие промежутки времени в базе данных могут появиться новые образцы. Поэтому обновление рекомендуется запускать регулярно. Необходимо отметить, что периодическое обновление системы при помощи демона ESETS возможно только при наличии заданной опции настройки **av_update_period** в разделе [update] файла настроек и при запуске и работе самого демона.

7.2. Описание процесса обновления ESETS

Процесс обновления состоит из двух этапов. Сначала с исходного сервера ESET создается зеркало всех соответствующих так называемых предварительно скомпилированных модулей. Эти предварительно скомпилированные модули по умолчанию загружаются в каталог

@BASEDIR@/mirror

Обратите внимание, что путь к каталогу зеркала можно переопределить при помощи опции настройки **mirror_dir** в разделе [update] файла настроек ESETS.

Модули ESETS можно подразделить на две категории: категорию механизмов и категорию компонентов. Модули из категории компонентов в настоящий момент используются только в операционных системах MS Windows. В данное время поддерживаются следующие типы модулей из категории механизмов: модули базового сканирования (с префиксом «engine», содержат базу данных вирусных сигнатур), модули поддержки архивов (с префиксом «archs», поддерживают архивные форматы различных файловых систем), модули расширенных эвристик (с префиксом «advheur», содержат реализацию так называемого метода расширенных эвристик для обнаружения вирусов и червей), модули сканирования для обнаружения упакованных червей (с префиксом «pwscan», используются в ОС MS Windows) и модули поддержки технологии ThreatSense.NET (с префиксом «charon»). Поскольку эти модули всегда необходимы, все они загружаются при каждой операции загрузки по умолчанию. С другой стороны, модули из категории компонентов зависимы от платформы и языка локализации, поэтому загрузка таких модулей необязательна.

После загрузки предварительно скомпилированных модулей в директории зеркала создается файл **update.ver**. В этом файле содержатся сведения о модулях, сохраненных на данный момент в только что созданном зеркале. Таким образом, это вновь созданное зеркало служит в качестве полнофункционального сервера загрузки модулей и может использоваться для создания второстепенных зеркал, при условии, однако, соблюдения некоторых дополнительных условий. Во-первых, на компьютере, с которого планируется загружать модули, должен быть установлен HTTP-сервер. Во-вторых, модули, предназначенные для загрузки на другие компьютеры, должны быть размещены по пути каталога

/http-serv-base-path/nod_upd
где **http-serv-base-path** – это путь к каталогу базового HTTP-сервера, поскольку именно с этого каталога программа обновления начинает поиск модулей.

На втором этапе процесса обновления осуществляется компиляция модулей, загружаемых сканером ESET Mail Security из сохраненных на локальном зеркале. Как правило, создаются следующие загрузочные модули ESETS: базовый модуль (nod32.000), модуль поддержки архивации (nod32.002), модуль расширенных эвристик (nod32.003), модуль сканирования для обнаружения упакованных червей (nod32.004), модуль программ под Windows (nod32.005) и модуль поддержки технологии ThreatSense.NET (nod32.006), – которые располагаются в каталоге:

@BASEDIR@

Обратите внимание, что это именно тот каталог, из которого демон ESETS загружает модули, и поэтому его можно переопределить при помощи опции настройки **base_dir** в разделе [global] (соотв. [update]) файла настроек ESETS.

8. Советы и рекомендации

8.1. ESETS и поддержка TLS в MTA

Безопасность транспортного уровня (TLS< Transport Layer Security) –это протокол, обеспечивающий конфиденциальность данных при клиент-серверном обмене по сети Интернет. Принцип TLS основан на SSL-шифровании данных, передаваемых между SMTP-клиентом и сервером, и это имеет определенные последствия в отношении сканирования передачи данных. В самом деле, как только в агенте MTA включена поддержка TLS, методы «оболочки» становятся невозможными, поскольку все данные, перехваченные на SMTP-обмене, на этом этапе зашифрованы. С другой стороны, имеется возможность использовать шифрование данных при обмене ими между локальным агентом и Интернетом и применять при этом методы «фильтрации содержимого». В агенте MTA Sendmail проблема с поддержкой TLS в SMTP отсутствует, поскольку здесь фильтрация содержимого выполняется внутренне при помощи Milter. С другой стороны, для обмена данными между фильтром содержимого и агентом MTA агент Postfix использует SMTP-протокол. Поэтому если поддержка TLS включена в Postfix, метод фильтрации содержимого становится невозможным, поскольку передаваемые данные зашифрованы.

Эту проблему можно решить на уровне настройки TLS в Postfix, отключив поддержку TLS для передачи данных между клиентом и сервером в пределах локального узла. Добавьте в файл **/etc/postfix/main.cf** следующую строку:
smtp_tls_per_site = hash:/etc/postfix/smtp_tls_per_site

Кроме того, необходимо создать файл **/etc/postfix/smtp_tls_per_site** со следующим содержимым:
localhost NONE

и указать соответствующую таблицу хэшей посредством ввода следующей команды из каталога **/etc/postfix**:
postmap hash:smtp_tls_per_site

При помощи приведенного выше оператора создается файл **'/etc/postfix/smtp_tls_per_site.db**, используемый агентом Postfix для включения поддержки TLS на основе узлов. Поскольку поддержка TLS для локального узла была отключена, возможно использование фильтрации содержимого, и в то же время передача данных между локальным агентом MTA и Интернетом по SMTP-протоколу остается зашифрованной.

9. Сообщите нам

Уважаемый пользователь, настоящее руководство содержит исчерпывающие сведения об установке, настройке и обслуживании системы ESET File Security. Тем не менее, написание документации – процесс бесконечный. Всегда найдутся моменты, объяснение которых было недостаточно подробным или совсем не было предоставлено. Поэтому при наличии вопросов или замечаний, связанных с данным документом, просим сообщить их в наш центр поддержки:

http://www.eset.com/support

Мы рады будем помочь вам в решении любых проблем, возникших в связи с данным продуктом.

Приложение A. Описание процесса установки ESETS

A1. Настройка ESETS для MTA-агента Postfix

A.1.1. Сканирование входящих сообщений электронной почты

Внимание! Эта установка несовместима с SELinux. Отключите SELinux или перейдите к следующему разделу.

Цель данной установки – вставить модуль esets_mda перед исходным MDA-агентом Postfix. Используемый MDA-агент (включая параметры) задается в параметре Postfix **mailbox_command**.

ПРИМЕЧАНИЕ. Если это значение пусто, Postfix самостоятельно осуществляет доставку почты. Необходимо установить и настроить фактический MDA-агент (например, procmail) и в первую очередь использовать его для параметра **mailbox_command**, включая аргументы (например, **/usr/bin/ procmail -d "$USER"**). Перезагрузите Postfix и убедитесь, что доставка почты осуществляется в соответствии с вашими требованиями. Теперь установку ESETS можно продолжить.

Скопируйте полный путь к текущему MDA-агенту Postfix и присвойте это значение параметру **mda_path** в разделе [mda] файла настроек ESETS. В рассматриваемом примере результат этого действия выглядит следующим образом:

mda_path = "/usr/bin/procmail"
и перезагрузите демон ESETS. Затем замените путь к текущему MDA-агенту Postfix на путь модуля esets_mda и добавьте к аргументам -- --recipient="$RECIPIENT" --sender="$SENDER"; в рассматриваемом примере это выглядит следующим образом:

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

Чтобы произвести считывание обновленной конфигурации, перезагрузите Postfix.

A.1.2. Двунаправленное сканирование сообщений электронной почты

Целью данной установки является перенаправление всех сообщений электронной почты из Postfix в модуль esets_smtp и получение их обратно. В разделе [smtp] файла настроек ESETS задайте следующие параметры:

agent_enabled = да
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
и перезагрузите демон ESETS. Это приведет к запуску модуля esets_smtp, сканированию всех данных, передаваемых по SMTP-протоколу и полученных на порт **listen_addr:listen_port**, и передаче этих данных на порт **server_addr:server_port**. Чтобы перенаправить все сообщения электронной почты из модуля esets_smtp в Postfix:

content_filter = smtp:[127.0.0.1]:2526

ПРИМЕЧАНИЕ. Если параметр **content_filter** уже установлен, пропустите эти указания. Вместо этого модуль esets_smtp (или другой модуль ESETS по сканированию почты) потребуется вставить перед текущим фильтром **content_filter** или после него.

В заключение необходимо настроить Postfix на прием почты на порт 2525 и дальнейшую ее обработку. Добавьте в файл master.cf модуля Postfix следующую запись:

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

В выражении с yourdomain.com просто замените часть после первой точки именем своего хоста. Убедитесь в наличии отступов во всех строках, кроме первой. Чтобы произвести новое считывание только что созданной настройки, перезагрузите Postfix.

ПРИМЕЧАНИЕ. Если включена функция SELinux, предотвращающая прослушивание порта 2525 модулем Postfix (например, при Fedora Core >= 5), выполните следующую команду: semanage -a -t smtp_port_t -p tcp 2525

A.2. Настройка ESETS для MTA-агента Sendmail

A.2.1. Сканирование входящих сообщений электронной почты

Внимание! Эта установка несовместима с SELinux. Отключите SELinux либо перейдите к следующему разделу.

Цель данной установки – вставить модуль esets_mda перед исходным MDA-агентом Sendmail.

ПРИМЕЧАНИЕ. В ОС FreeBSD обмен данными между Sendmail и MDA-агентом может осуществляться по протоколу LMTP. Однако в модуле esets_mda поддержка протокола LMTP не предусмотрена. Таким образом, если в файле имя **хост-узла.mc** содержится запись FEATURE(local_lmtp), ее необходимо вынести в комментарий и повторно создать файл **sendmail.cf**.

MDA-агент, используемый в данный момент, можно найти в файле **sendmail.cf** в разделе Mlocal: в параметрах **P** (исполняемый) и **A** (его имя и аргументы).

Сначала в разделе [mda] файла настроек ESETS укажите путь **mda_path** к текущему используемому исполняемому MDA-агенту (параметр **P** в Sendmail) и перезагрузите демон ESETS.

Затем к файлу sendmail.mc (или имя **хост-узла.mc** в ОС FreeBSD) перед всеми определениями MAILER добавьте следующие строки:

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

где **original_arguments** – это параметр **A** модуля Sendmail без имени (первое слово). В завершение повторно создайте файл sendmail.cf и перезагрузите Sendmail.

A.2.2. Двунаправленное сканирование сообщений электронной почты

Назначением данной установки является сканирование всей электронной почты в Sendmail при помощи фильтра esets_smfi. В разделе [smfi] файла настроек ESETS задайте следующие параметры:

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

и перезагрузите демон ESETS. Затем к файлу sendmail.mc (или имя **хост-узла.mc** в ОС FreeBSD) перед всеми определениями MAILER добавьте следующую строку:

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

Эти настройки позволяют модулю Sendmail обмениваться данными с фильтром esets_smfi через unix-сокет **/var/run/esets_smfi.sock**. Значение флага F=T приводит к созданию временного сбоя соединения, если фильтр недоступен. Пределы времени имеют следующие значения: S:2m задает время ожидания, равное 2 минутам, для отправки информации фильтру от MTA-агента; R:2m задает время ожидания, равное 2 минутам, для считывания ответа фильтра, а E:5m обозначает общий 5-минутный срок ожидания между отправкой последнего фрагмента сообщения фильтру и получением окончательного подтверждения.

Обратите внимание, что если для фильтра esets_smfi заданы слишком короткие временные пределы, модуль Sendmail может временно отложить сообщение в очередь и через некоторое время повторить попытку его передачи. Это может привести к постоянной задержке одних и тех же сообщений. Во избежание этой проблемы следует установить соответствующие пределы времени. Кроме того, можно испытать различные значения параметра **confMAX_MESSAGE_SIZE** модуля Sendmail, устанавливающего максимально допустимый размер сообщения в байтах. Учитывая это значение и максимальное время обработки такого объема данных агентом MTA (данный показатель можно измерить), можно оценить соответствующие пределы времени для фильтра esets_smfi.

В завершение повторно создайте файл sendmail.cf и перезагрузите Sendmail.

A.3. Настройка ESETS для MTA-агента Qmail

A.3.1. Сканирование входящих сообщений электронной почты

Цель данной установки – вставить модуль esets_mda перед локальным агентом доставки модуля Qmail. Предполагается, что модуль Qmail установлен в каталог **/var/qmail**. В разделе [mda] файла настроек ESETS задайте следующий параметр:

mda_path = "/var/qmail/bin/qmail-esets_mda"
и перезагрузите демон ESETS. Создайте файл **/var/qmail/bin/qmail-esets_mda** со следующим содержимым и примените к нему команду chmod a+x:

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

Это позволит модулю esets_mda вызвать локальный агент доставки модуля Qmail. Теперь создайте файл **/var/qmail/bin/qmail-start.esets** со следующим содержимым и так же примените к нему команду chmod a+x:

```
#!/bin/sh
A="$1"; shift
exec qmail-start.orig "|@BINDIR@/esets_mda '$A'" \
    -- --sender="$SENDER" --recipient="$RECIPIENT"' "$@"
```

Это приведет к использованию модуля esets_mda при запуске Qmail для локальной доставки. Тем не менее, через esets_mda в qmail-local передается исходная спецификация доставки. Обратите внимание, что в этой конфигурации модуль esets_ mda будет использовать распозноваемые коды выхода Qmail (см. see qmail-command(8)). В завершение замените qmail-start при помощи команд:

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

A.3.2. Двунаправленное сканирование сообщений электронной почты

Целью этой установки является вставка модуля esets_mda перед функцией qmail-queue, в которой все сообщения электронной почты перед доставкой ставятся в очередь. Предполагается, что модуль Qmail установлен в каталог **/var/qmail**. В разделе [mda] файла настроек ESETS задайте следующий параметр:

mda_path = "/var/qmail/bin/qmail-queue.esets"
и перезагрузите демон ESETS. В завершение замените qmail-queue при помощи команд:

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

Перезагрузка Qmail не требуется. Теперь все поставленные в очередь сообщения будут сканироваться системой ESETS. Обратите внимание, что в этой настройке модуль esets_mda будет использовать коды выхода qmail-queue (см. qmail- queue(8)).

A.4. Настройка ESETS для MTA-агента Exim версии 3

A.4.1. Сканирование входящих сообщений электронной почты

Целью данной установки является создание Exim-передачи из модуля esets_mda для локальных пользователей. В разделе [mda] файла настроек ESETS задайте следующий параметр:

mda_path = "/usr/sbin/exim"
где **/usr/sbin/exim** – полный путь к двоичному файлу Exim. Затем перезагрузите демон ESETS. После этого добавьте данный механизм передачи в список механизмов передачи Exim (в любое место по своему усмотрению).

```
esets_transport:
    driver = pipe
    command = @BINDIR@/esets_mda -oi -oMr esets-scanned $local_part@$domain \
    -- --sender=$sender_address --recipient=$local_part@$domain user = mail
```
где **mail** – это один из доверенных пользователей агента Exim. Затем добавьте этот указатель на первую позицию в список указателей Exim:

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

Это приведет к отправке еще не просканированных сообщений электронной почты, предназначенных для локальных пользователей, на модуль esets_mda, который, в свою очередь, отправит их обратно в Exim для дальнейшей обработки. Чтобы заново считать только что созданную конфигурацию, перезагрузите Exim.

A.4.2. Двунаправленное сканирование сообщений электронной почты

Целью данной установки является создание Exim-передачи из модуля esets_mda для всех электронных сообщений. Выполните все шаги, описанные в предыдущем разделе, и в список маршрутизаторов Exim на первую позицию добавьте следующий маршрутизатор:

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

A.5. Настройка ESETS для MTA-агента Exim версии 4

A.5.1. Сканирование входящих сообщений электронной почты

Целью данной установки является создание передачи Exim из модуля esets_mda для локальных пользователей. В разделе [mda] файла настроек ESETS задайте следующий параметр:

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

где **/usr/sbin/exim** – полный путь к двоичному файлу Exim. Затем перезагрузите демон ESETS. Добавьте следующий маршрутизатор на первую позицию списка маршрутизаторов Exim:

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

Кроме того, добавьте следующий механизм передачи в список механизмов передачи Exim (на любую позицию):

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

Это приведет к отправке еще не просканированных сообщений электронной почты, предназначенных для локальных пользователей, на модуль esets_mda, который, в свою очередь, отправит их обратно в Exim для дальнейшей обработки. Чтобы заново считать только что созданную конфигурацию, перезагрузите Exim.

A.5.2. Двунаправленное сканирование сообщений электронной почты

Целью данной установки является создание Exim-передачи из модуля esets_mda для всех электронных сообщений. Выполните все шаги, описанные в предыдущем разделе, исключив следующую строку для esets_router:

```
domains = +local_domains
```

A.6. Настройка ESETS на сканирование исходящих сообщений электронной почты

Сканирование исходящих сообщений электронной почты выполняется при помощи демона esets_smtp. В разделе [smtp] файла настроек ESETS задайте следующие параметры:

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

где **listen_addr** – это адрес локального сетевого интерфейса с именем ifo. Затем перезагрузите демон ESETS. На следующем этапе все SMTP-запросы необходимо перенаправить на модуль esets_smtp. При наличии IP-фильтрации, обеспечиваемой средством администрирования ipchains, подходящим является правило:

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

Если механизм IP-фильтрации обеспечивается средством администрирования iptables, необходимо использовать правило:

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

Соответственно, при использовании средства ipfw (в ОС BSD) правило выглядит следующим образом:

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

Внимание! Используемый MTA-агент может принимать все подключения без подробной проверки со стороны esets_smtp, поскольку они локальны. Применяя правила персонального файервола, убедитесь, что вы не создали open relay, предоставляющий внешним пользователям возможность подключаться к модулю esets_smtp и использовать его в качестве SMTP-relay сервера.

A.7. Настройка ESETS на сканирование данных, передаваемых по протоколу POP3

Сканирование данных, передаваемых по протоколу POP3, осуществляется при помощи демона esets_pop3. В разделе [pop3] файла настроек ESETS задайте следующие параметры:

agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8110
где **listen_addr** – это адрес локального сетевого интерфейса с именем ifo. Затем перезагрузите демон ESETS. На следующем этапе все POP3-запросы необходимо перенаправить на модуль esets_pop3. При наличии IP-фильтрации, обеспечиваемой средством администрирования ipchains, подходящим является правило:

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

Если механизм IP-фильтрации обеспечивается средством администрирования iptables, необходимо использовать правило:

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

Соответственно, при использовании правила ipfw (при работе с ОС BSD) правило выглядит следующим образом:

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

A.8. Настройка ESETS на сканирование данных, передаваемых по протоколу IMAP

Сканирование данных, передаваемых по протоколу IMAP, осуществляется при помощи демона esets_imap. В разделе [imap] файла настроек ESETS задайте следующие параметры:

agent_enabled = yes listen_addr = "192.168.1.10" listen_port = 8143
где **listen_addr** – это адрес локального сетевого интерфейса с именем ifo. Затем перезагрузите демон ESETS. На следующем этапе все IMAP-запросы необходимо перенаправить на модуль esets_imap. При наличии IP-фильтрации, обеспечиваемой средством администрирования ipchains, применяется правило:

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

Если механизм IP-фильтрации обеспечивается средством администрирования iptables, необходимо использовать правило:

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

Соответственно, при использовании правила ipfw (при работе с ОС BSD) правило выглядит следующим образом:

ipfw add fwd 192.168.1.10,8143 tcp from any to any 143 via ifo in

Приложение В. Лицензия PHP

Лицензия PHP, версия 3.01, © PHP Group, 1999–2006. Все права защищены. Повторное воспроизведение в форме исходного кода или в двоичной форме допустимо при соблюдении следующих условий.

1. При повторном воспроизведении исходного кода должны сохраняться вышеприведенное уведомление об авторских правах, данный список условий и соответствующие оговорки.
2. При повторном воспроизведении в двоичной форме должны сохраняться вышеприведенное уведомление об авторских правах, данный список условий и соответствующие оговорки в документации, а также другие материалы, прилагаемые к данному дистрибутиву.
3. Имя PHP не должно использоваться при поддержке и продвижении продуктов, полученных из данного программного обеспечения, без предварительного письменного разрешения. Для получения письменного разрешения следует написать запрос по адресу group@ php.net.
4. Без получения предварительного письменного разрешения, запрашиваемого по адресу group@php.net, «PHP» не может быть названием или частью названий продуктов, созданных на основе данного программного обеспечения. Обозначить совместимость разработанного программного обеспечения с PHP можно выражением «Нечто для PHP», но не «PHP Нечто» или «phpнечто».
5. Компания PHP Group может периодически выпускать новые или пересмотренные версии данной лицензии. Каждая версия будет отличаться соответствующим номером. После публикации закрытого кода с определенной версией лицензии он может использоваться в соответствии с условиями этой лицензии. Также этот закрытый код может использоваться в рамках любой более поздней версии лицензии, опубликованной компанией PHP Group. Никто кроме компании PHP Group не имеет права изменять условия, относящиеся к закрытому коду, выпущенному в рамках данной лицензии.
6. Повторное воспроизведение, в какой бы форме оно ни проводилось, должно сопровождаться следующим подтверждением. «Данный продукт включает программное обеспечение PHP, находящееся в бесплатном доступе по адресу http://www.php.net/software/».

   ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО ГРУППОЙ РАЗРАБОТЧИКОВ PHP «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОСТИ ИЛИ ПРИГОДНОСТИ ДЛЯ КАКИХ-ЛИБО ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ГРУППА РАЗРАБОТКИ PHP И ЕЕ СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО ПРЯМЫЕ, КОСВЕННЫЕ, СЛУЧАЙНЫЕ, ОСОБЫЕ, ОПОСРЕДОВАННЫЕ ИЛИ ШТРАФНЫЕ УЩЕРБ ИЛИ УБЫТКИ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, УБЫТКИ, СВЯЗАННЫЕ С РАСХОДОВАНИЕМ СРЕДСТВ НА ЗАМЕНУ ПРОДУКТОВ ИЛИ УСЛУГ, УТРАТОЙ ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИИ, ПОТЕРЕЙ ДАННЫХ, УПУЩЕННОЙ ВЫГОДОЙ ИЛИ С ПЕРЕРЫВОМ В КОММЕРЧЕСКОЙ ИЛИ ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, КАКИМ БЫ ОБРАЗОМ ЭТОТ УЩЕРБ НИ БЫЛ ПРИЧИНЕН И КАКОЙ БЫ НИ БЫЛА ПРАВОВАЯ ОСНОВА ОТВЕТСТВЕННОСТИ ЗА УЩЕРБ, БУДЬ ТО НАРУШЕНИЕ ДОГОВОРНЫХ ОБЯЗАТЕЛЬСТВ, СТРОГАЯ ОТВЕТСТВЕННОСТЬ ИЛИ ГРАЖДАНСКОЕ ПРАВОНАРУШЕНИЕ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), ЕСЛИ ЭТОТ УЩЕРБ ВОЗНИКАЕТ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ГРУППА РАЗРАБОТЧИКОВ БЫЛА ЗАРАНЕЕ ПРЕДУПРЕЖДЕНА О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.