we protect your digital worlds

ESET NOD32 Gateway Security

Руководство по установке
и документация пользователя

Содержание

1. Введение 3

2. Терминология и сокращения 5

3. Установка 9

4. Структура продукта 11

5. Интеграция со службами интернет-шлюзов 15

5.1. Настройка прозрачного HTTP- и FTP- прокси 16

5.2. Настройка HTTP/FTP-прокси вручную 17

5.2.1. Настройка прокси для Mozilla Firefox вручную 17

5.2.2. Настройка прокси для кэширующего прокси-сервера Squid вручную. 18

5.3. Обработка крупных HTTP-объектов 19

5.3.1. Метод отложенного сканирования 19

5.3.2. Метод частичного сканирования 19

5.4. Подключаемый фильтр ESETS для кэширующего прокси-сервера SafeSquid 20

5.4.1. Принцип работы 20

5.4.2. Установка и настройка 20

6. Основные механизмы ESET NOD32 Gateway Security 23

6.1. Политика обработки объектов 24

6.2. Настройки пользователя 24

6.3. «Черные» и «белые» списки 25

6.4. Система предоставления образцов 26

6.5. Веб-интерфейс 26

6.6. Удаленное администрирование 27

7. Обновление системы ESET Security 29

7.1. Служебная программа обновления ESETS 30

7.2. Описание процесса обновления ESETS 30

8. Обратная связь 31

A. Описание процесса настройки ESETS 33

A.1. Настройка ESETS для сканирования HTTP-соединений в прозрачном режиме 34

A.2. Настройка ESETS для сканирования FTP-соединений в прозрачном режиме 34

9. Приложение A. Лицензия PHP 35

ESET NOD32 Gateway Security

REV.20080307-004

Глава 1

Введение

Поздравляем вас с приобретением ESET NOD32 Gateway Security – одной из лучших систем безопасности, работающих под управлением операционных систем Linux и BSD. Используя ультрасовременное ядро сканирования ESET, система обеспечивает непревзойденные скорость сканирования и уровень обнаружения в сочетании с минимальным использованием системных ресурсов. Благодаря этому она идеально подходит для любого сервера Linux/BSD.

В данной главе будут рассмотрены ключевые характеристики системы.

- Алгоритмы ядра антивирусного сканирования ESET обеспечивают высочайший уровень обнаружения и максимальную скорость сканирования.
- Программный пакет ESET NOD32 Gateway Security разработан для использования как в однопроцессорных, так и в мультипроцессорных устройствах.
- В нем используется уникальная расширенная эвристика для обнаружения червей Win32 и бэкдоров.
- Встроенные архиваторы распаковывают заархивированные объекты без использования сторонних программ.
- Архитектура системы основана на использовании демона (резидентной программы), к которому отправляются все запросы на сканирование, что приводит к увеличению скорости и эффективности работы антивирусного продукта.
- Все исполняемые демоны (за исключением esets_dac) для повышения безопасности выполняются под учетной записью непривилегированного пользователя.
- Система позволяет выполнять избирательную настройку как для индивидуальных пользователей, так и для пользователей уровня клиент-сервер.
- Для получения информации о работе системы и угрозах могут быть настроены шесть уровней ведения журналов.
- Настройка, администрирование и управление лицензиями может выполняться при помощи интуитивно понятного удобного веб-интерфейса.
- В системе присутствует ESET Remote Administration для администрирования крупных компьютерных сетей.
- Для установки ESET NOD32 Gateway Security не требуются внешние программы или библиотеки, за исключением LIBC.
- Система может отсылать предупреждение о проникновении и прочих важных событиях любому лицу, в зависимости от настроек.

Для эффективной работы ESET NOD32 Gateway Security требуется всего 16 МБ пространства на жестком диске и 32 МБ оперативной памяти. Эффективная работа обеспечивается под управлением ядра Linux версий 2.2.x, 2.4.x и 2.6.x, а также под управлением ядра операционной системы FreeBSD версий 5.x, 6.x.

На всех серверах, от маломощных небольших офисных систем до ISP-серверов корпоративного класса с тысячами пользователей, система обеспечивает производительность и масштабируемость, присущие решениям на основе UNIX, а также непревзойденную безопасность продуктов ESET.

Глава 2

Терминология и сокращения

Далее рассматриваются термины и сокращения, используемые в настоящей документации. Обратите внимание, что в этой документации (только для PDF-формата) полужирным шрифтом выделены названия компонентов продукта, а в данной главе таким образом выделяются также новые термины и сокращения. Также обратите внимание, что термины и сокращения, определенные в этой главе, будут выделяться и в других главах данной документации (только в PDF-формате).

ESETS

ESET Security является общей аббревиатурой для всех продуктов обеспечения безопасности, разработанных компанией ESET, spol. s r.o. для ОС Linux (и, соответственно, для ОС BSD). Также это название (или часть названия) программного пакета, включающего соответствующие продукты.

RSR

Сокращение для RedHat/Novell(SuSE) Ready. Обратите внимание, что мы поддерживаем оба варианта продукта: RedHat Ready и Novell(SuSE) Ready. Отличие от «стандартной» версии Linux заключается в том, что пакет RSR соответствует критериям, представленным в документе 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 пакет *RSR* устанавливается как приложение-надстройка, то есть по умолчанию предлагается путь установки /opt/eset/esets.

Демон ESETS

Основной демон системы управления и сканирования *ESETS* – **esets_daemon**.

Базовый каталог ESETS

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

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

Каталог настроек ESETS

Каталог, в котором хранятся все файлы, связанные с настройками ESET NOD32 для защиты сервера. Далее в документации для этого каталога будет использоваться сокращение ***@ETCDIR@***. Путь каталога:

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

Файл конфигурации ESETS

Основной файл конфигурации ESET NOD32 для защиты сервера. Полный путь к файлу:

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

Каталог бинарных файлов ESETS

Каталог, в котором хранятся бинарные файлы, относящиеся к ESET NOD32 для защиты сервера. Далее в документации для этого каталога будет использоваться сокращение **@*BINDIR*@**. Путь каталога:

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

Каталог системных бинарных файлов ESETS

Каталог, в котором хранятся системные бинарные файлы, относящиеся к ESET NOD32 для защиты сервера. Далее в документации для этого каталога будет использоваться 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 NOD32 для защиты сервера. Далее в документации для этого каталога будет использоваться сокращение **@*LIBDIR*@**. Путь каталога:

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

Глава 3

Установка

Данный продукт распространяется в виде бинарного файла:

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

где **ext** представляет собой суффикс, зависящий от дистрибутива операционной системы Linux/BSD, то есть **deb** для Debian, **rpm** для RedHat и SuSE, **tgz** для других дистрибутивов ОС Linux, **fbs5.tgz** для FreeBSD 5.xx и **fbs6.tgz** для FreeBSD 6.xx.

Обратите внимание, что форматом бинарного 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 Linux *RSR* используйте оператор

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

В качестве ответа выводится 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.

Установив пакет программ и запустив основной сервис *ESETS*, вы можете проверить работу системы, используя в операционной системе LINUX следующую команду:

```
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
```

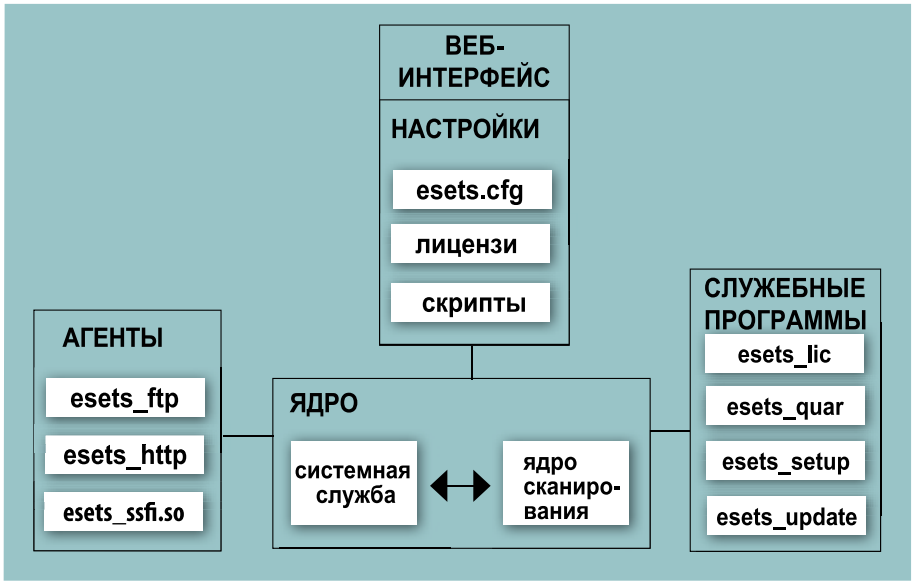
где должны быть представлены как минимум два процесса демона *ESETS*, выполняющиеся в фоновом режиме. Один из этих процессов – так называемый диспетчер процессов и потоков системы. Другой – процесс сканирования *ESETS*.

Глава 4

Структрура продукта

После успешной установки пакета продукта следует ознакомиться с его содержимым.

Рис. 4–1. Структура ESET NOD32 Gateway Security



Структура программного пакета ESET NOD32 Gateway Security показана на рисунке 4–1. Система состоит из следующих компонентов.

ЯДРО

Ядро ESET NOD32 Gateway Security включает демон ESETS – esets_daemon. Этот демон использует библиотеку ESETS API libesets.so и загружаемые модули ESETS em00X_xx.dat для обеспечения основных системных задач: сканирования, агентских процессов демона, обслуживания системы предоставления образцов, ведения журналов, уведомлений и т. д. Для получения дополнительных сведений обратитесь к странице руководства, посвященной esets_daemon (8).

АГЕНТЫ

Задачей модулей агента ESETS является интеграция ESETS с серверной средой Linux или BSD. Ознакомьтесь с соответствующей главой данного документа.

СЛУЖЕБНЫЕ ПРОГРАММЫ

Модули служебных программ являются особой частью системы. Они разработаны для обеспечения простого и эффективного управления системой и отвечают за выполнение соответствующих системных задач, например, за управление лицензиями, карантином, настройку и обновление системы. Ознакомьтесь с соответствующей главой данного документа.

НАСТРОЙКИ

Правильная настройка является важнейшим условием работы системы. Поэтому далее в этой главе будут описаны все соответствующие компоненты. Кроме того, настоятельно рекомендуется прочитать важные сведения о настройке ESETS на страницах руководства, посвященных esets.cfg (5).

После успешной установки продукта все соответствующие компоненты настроек хранятся в каталоге настроек ESETS. Каталог содержит следующие файлы.

@*ETCDIR*@/esets.cfg

Это наиболее важный файл конфигурации, поскольку он обслуживает основную часть выполняемых продуктом функций. Посмотрев файл, вы заметите, что он состоит из различных параметров, распределенных по разделам. Обратите внимание, что названия разделов всегда заключены в квадратные скобки. В файле *конфигурации ESETS* всегда присутствует один глобальный раздел и несколько так называемых агентских. Параметры в глобальном разделе используются для определения опций настройки демона ESETS, а также значений по умолчанию для опций настройки ядра сканирования ESETS. Параметры в агентских разделах служат для определения опций настройки так называемых агентов, то есть модулей, используемых для перехвата различных типов потоков данных в компьютере или его окружении, а также для подготовки этих данных к сканированию. Обратите внимание, что помимо множества параметров, используемых для настройки системы, существует также набор правил, определяющих организацию файла. Для изучения этой информации обратитесь к разделам руководства, посвященным esets.cfg(5), esets_daemon(8), а также к разделам, описывающим соответствующие агенты.

@*ETCDIR*@/certs

Этот каталог служит для хранения сертификатов, используемых в веб-интерфейсом ESETS для аутентификации (для получения более подробной информации см. в раздел, посвященный esets_wwwi(8)).

@*ETCDIR*@/license

Данный каталог используется для хранения лицензионных ключей продуктов, полученных от поставщика. Обратите внимание, что демон ESETS всегда обращается именно к этому каталогу для проверки правильности лицензионного ключа, если не переопределить его при помощи параметра **license_dir** в файле конфигурации ESETS.

@*ETCDIR*@/scripts/license_warning_script

Этот скрипт, если он включен параметром **license_warn_enabled** файла настройки ESETS, начнет выполняться за 30 дней до окончания срока действия лицензии и будет выполняться один раз в день. Он предназначен для отправки системному администратору по электронной почте уведомления об истечении срока лицензии.

@*ETCDIR*@/scripts/daemon_notification_script

Этот скрипт, если он включен параметром **exec_script** файла конфигурации ESETS, выполняется в случае обнаружения антивирусной системной вирусного проникновения. Он предназначен для отправки системному администратору по электронной почте уведомления о соответствующем событии.

Глава 5

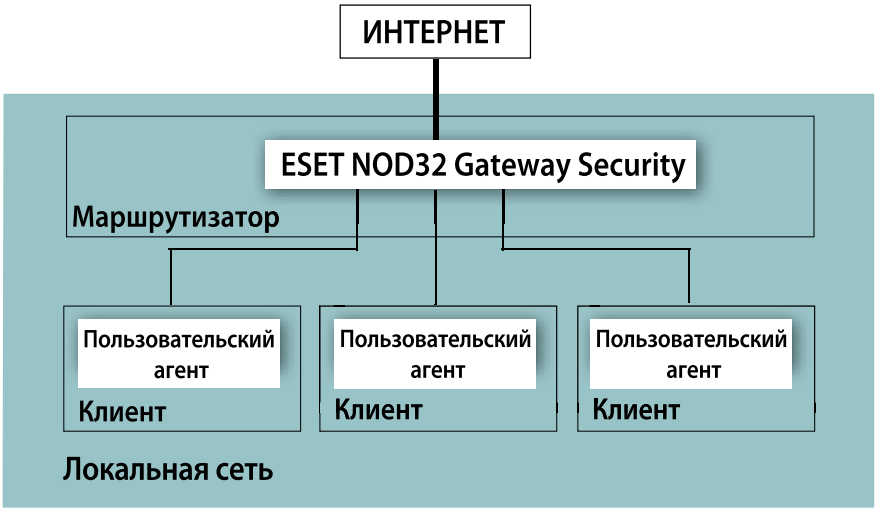
Интеграция со службами интернет-шлюзов

ESET NOD32 Gateway Security защищает HTTP- и FTP-службы организации от вирусов, червей, троянов и шпионского ПО, фишинг-атак и других интернет-угроз на уровне серверов интернет-шлюзов. Обратите внимание, что под шлюзовыми серверами понимаются шлюзы третьего уровня модели ISO/OSI, то есть маршрутизаторы. В этой главе представлен процесс интеграции продукта с описанными службами.

5.1. Настройка прозрачного HTTP- и FTP- прокси

Настройка прозрачного прокси основывается на стандартном механизме маршрутизации, изображенном на следующем рисунке.

Рис. 5–1. Схема ESET NOD32 Gateway Security в качестве прозрачного прокси



Конфигурация создается естественным образом, поскольку таблицы IP-маршрутизации ядра определяются для каждого клиента локальной сети. Эти таблицы маршрутизации используются для настройки статических маршрутов к шлюзовому серверу, назначенному по умолчанию для локальной сети (маршрутизатору). Обратите внимание, что в сети DHCP это выполняется автоматически. При использовании этого метода все HTTP- (и, соответственно, FTP-) соединения с внешними серверами происходят через шлюзовой сервер локальной сети, где должен быть установлен ESET Gateway Server для сканирования соединений на наличие вирусов. Для этой цели разработан общий HTTP- (и, соответственно, FTP-) фильтр ESETS **esets_http** (и, соответственно, **esets_ftp**).

Чтобы настроить ESET NOD32 Gateway Security для сканирования HTTP- (и, соответственно, FTP-) сообщений, направляемых через шлюзовой сервер сети, введите следующую команду:

```
esets_setup
```

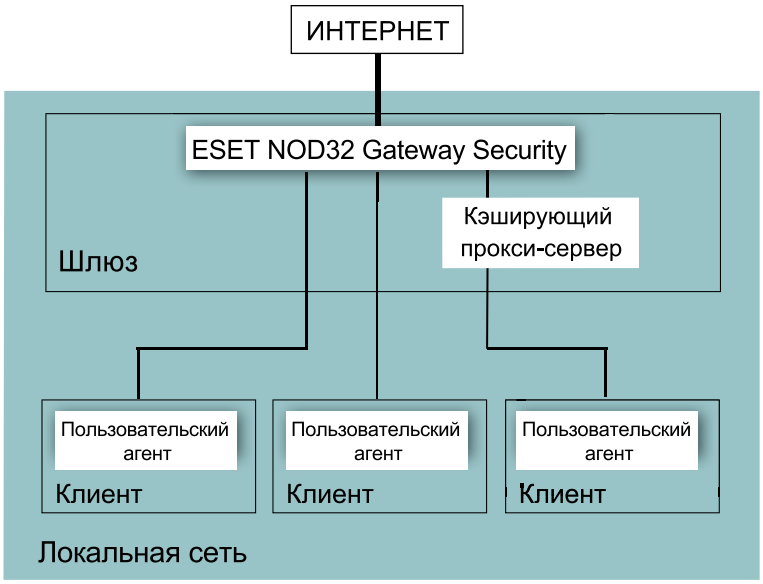
Следуйте инструкциям, приведенным в скрипте. После появления приглашения «Доступные установки/удаления» (Available installations/un-installations) выберите опцию HTTP (или, соответственно, FTP), чтобы получить доступ к опциям установки/удаления для соответствующего модуля. Выберите установку. Это автоматически настроит модуль на прослушивание предварительно определенного порта и перенаправление IP-пакетов из выбранной сети с конечным HTTP- (или, соответственно, FTP-) портом в тот порт, где **esets_http** (или, соответственно, **esets_ftp**) выполняет прослушивание. Это означает, что сканироваться будут только те запросы, которые изначально были направлены в конечный HTTP- (или, соответственно, FTP-) порт. Если требуется охватить другие порты, следует назначить аналогичные правила перенаправления.

Следует учесть, что в режиме по умолчанию инсталлятор отображает все шаги, которые предстоит выполнить, и создает резервную копию конфигурации, которую в дальнейшем можно будет восстановить в любое время. Более подробные сведения о действиях служебной программы-инсталлятора для возможных сценариев см. в приложении A данной документации.

5.2. Настройка HTTP/FTP-прокси вручную

Отличительным свойством настройки прокси вручную (см. рис. 5–2) является явное указание адреса и порта прослушивания родительского прокси в настройках пользовательского прокси-агента.

Рис. 5-2. Схема ESET NOD32 Gateway Security – настройка вручную



В этом случае прокси-сервер обычно изменяет переданные запросы и/или ответы, то есть, работает в непрозрачном режиме. Поддержка прокси **esets_http** вручную была протестирована на широком диапазоне наиболее часто используемых пользовательских агентов, то есть на кэширующих прокси-серверах (Squid Proxy Cache, SafeSquid) и клиентских браузерах (Firefox, Opera, Netscape, Konqueror). Иными словами, любой пользовательский HTTP-агент, поддерживающий возможность настройки родительского прокси вручную, будет работать с модулем esets_http. Далее описана настройка вручную прокси esets_http для браузера Mozilla Firefox и кэширующего прокси-сервера Squid, которые являются одними из наиболее часто используемых приложений пользовательских HTTP-агентов.

5.2.1. Настройка прокси для Mozilla Firefox вручную

Общая схема настройки HTTP/FTP-прокси **esets_http** вручную для Mozilla Firefox представлена в левой части рисунка 4–2.

Обратите внимание, что эта конфигурация позволяет устанавливать ESET NOD32 Gateway Security в любое место в локальной сети, включая шлюзовой сервер и компьютер пользовательского агента.

В этом примере выполнена настройка **esets_http** для прослушивания порта 8080 компьютера с IP-адресом локальной сети 192.168.1.10. Для этого в разделе [http] основного *файла конфигурации ESETS* указаны следующие параметры:

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

Внимание. Параметр listen_addr также может быть указан как имя хоста, видимого из другой локальной сети.

Чтобы настроить Mozilla для использования **esets_http**, необходимо в меню «Правка» (Edit) строки меню выбрать «Предпочтения» (Preferences) (в более старых версиях Mozilla необходимо в меню «Инструменты» (Tools) выбрать «Настройки» (Options)). Теперь щелкните «Настройки подключения» (Connection settings)

на вкладке «Общие» (General) и выберите «Конфигурация прокси вручную» (Manual Proxy Configuration). На заключительном этапе в полях «HTTP-прокси» (HTTP Proxy) (или, соответственно, «FTP-прокси» (FTP Proxy)) необходимо указать имя хоста (или, соответственно, IP-адрес), а в соответствующих полях «Порт» (Port) указать порт, где esets_http выполняет прослушивание (в данном примере должны быть указаны IP-адрес 192.168.1.10 и порт 8080). Для повторного считывания вновь созданной конфигурации перезагрузите демон ESETS.

Стоит отметить, что конфигурация, описанная здесь, не является оптимальной для сетей с большим числом клиентских компьютеров. Причина заключается в том, что в этом случае HTTP-кэш (если таковой имеется) присутствует только в пользовательском агенте, поэтому тот же самый исходный объект будет сканироваться несколько раз при запросах от различных пользовательских агентов.

5.2.2. Настройка прокси для кэширующего прокси-сервера Squid вручную

Общая схема настройки HTTP-прокси **esets_http** вручную для кэширующего прокси-сервера Squid представлена в правой части рисунка 4–2.

Существенное отличие от предыдущей описанной конфигурации заключается в том, что ESET NOD32 Gateway Security устанавливается в HTTP/FTP-шлюзе между кэширующим прокси-сервером (в данном примере – Squid) и Интернетом. Таким образом, все входящие в сеть HTTP/FTP-ответы вначале сканируются на наличие вирусов, а затем сохраняются в выделенном сетевом кэше, то есть все когда-либо запрошенные исходные объекты, находящиеся в кэширующем прокси-сервере, уже проверены на наличие вирусов, и при повторном запросе дополнительная проверка не требуется.

В этом примере выполнена настройка **esets_http** для прослушивания порта 8080 шлюзового сервера с IP-адресом локальной сети 192.168.1.10. Для этого в разделе [http] файла конфигурации ESETS указаны следующие параметры:

```
agent_enabled = yes
listen_addr = ”192.168.1.10” l
isten_port = 8080
```

Обратите внимание, что параметр listen_addr либо может быть указан как имя хоста, видимого из другой локальной сети, либо может использовать адрес 0.0.0.0, что позволит esets_http прослушивать все интерфейсы. В последнем случае необходимо соблюдать осторожность, так как пользователи, находящиеся за пределами локальной сети, также смогут пользоваться HTTP/ FTP-сканированием. Чтобы запретить подобный доступ, следует принять дополнительные меры безопасности.

Чтобы настроить Squid для использования **esets_http** в качестве родительского прокси, в файл конфигурации Squid (/etc/squid/squid.conf) необходимо добавить следующие строки:

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

В приведенных выше строках показана настройка Squid для использования http-прокси для прослушивания по IP-адресу 192.168.1.10 порта 8080 в качестве родительского прокси. Все запросы, обработанные Squid, таким образом, будут передаваться в это расположение. В остальных строках определяется поведение Squid для выдачи сообщений об ошибках в случае сбоя родительского прокси, или если прокси недоступен. Существует и другой способ настройки Squid для использования прямых подключений, если родительский прокси недоступен. В этом случае в файл конфигурации Squid необходимо добавить следующие параметры:

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

Для повторного считывания вновь созданной конфигурации перезагрузите демон ESETS.

5.3. Обработка крупных HTTP-объектов

В обычных условиях esets_http обрабатывает каждый передаваемый объект. При этом вначале объект передается от HTTP-сервера (или, соответственно, клиента) в **esets_http**, затем сканируется на наличие вирусов, а после этого передается в HTTP-клиент (или, соответственно, сервер). В отношении больших файлов (крупные объекты, время передачи которых превышает время ожидания, определенное параметром lo_timeout) такой сценарий не совсем удобен, поскольку время ожидания пользовательского агента или нетерпение пользователя могут стать причиной прерывания или даже отмены передачи объекта. Следовательно, необходимо использовать иные методы обработки крупных объектов.

5.3.1. Метод отложенного сканирования

Для обработки больших файлов в **esets_http** используется стандартный метод так называемого отложенного сканирования. Это означает, что если передаваемый объект становится большим, **esets_http** начинает прозрачную передачу этого объекта в ожидающую конечную точку HTTP (клиент или сервер). Объект сканируется на наличие вирусов после получения последней его части в **esets_http**. Если объект окажется зараженным, его последняя часть (в текущей версии ESET NOD32 Gateway Security последняя часть определяется как последние 4 КБ данных объекта) в ожидающую конечную точку не передается, и связь с конечной точкой прерывается. Одновременно с этим администратору шлюза электронной почтой направляется уведомление с соответствующими сведениями о передаче опасного файла. Обратите внимание, что уведомление направляется только в случае передачи данных от сервера к клиенту. В этом случае URL-адрес исходного объекта сохраняется в кэше **esets_http** для блокирования передачи при повторном запросе.

Здесь необходимо отметить, что в описанном выше методе «отложенного сканирования» заложен потенциальный риск для компьютера, чей пользовательский агент впервые запросил зараженный большой файл. Риск сохраняется, поскольку, даже если передача данных зараженного объекта была отложена, в некоторых уже переданных частях может содержаться выполняемый вредоносный код. По этой причине в ESET разработана модификация метода «отложенного сканирования», называемая методом «частичного сканирования».

5.3.2. Метод частичного сканирования

Метод «частичного сканирования» был разработан для обеспечения безопасности метода «отложенного сканирования». Принцип действия метода «частичного сканирования» заключается в том, что время сканирования крупного объекта незначительно по сравнению с общим временем обработки объекта. Обратите внимание, что это условие соблюдается при HTTP-передаче крупного объекта, поскольку для передачи объекта требуется гораздо большее время, чем для его сканирования на наличие вирусов. Эта предпосылка позволяет выполнять несколько операций сканирования во время передачи объекта.

После включения параметра `lo_partscan_enabled` в разделе [http] *файла конфигурации ESETS* сканирование крупного объекта на наличие вирусов будет выполняться через предварительно определенные периоды времени во время его передачи. Сканированные данные будут передаваться ожидающей конечной точке (то есть клиенту или серверу). При использовании этого метода отсутствует возможность попадания вирусов в компьютер, пользовательский агент которого запросил крупный инфицированный объект, поскольку безопасность каждой части переданных данных уже обеспечена.

Испытания показали, что в обычных условиях (за счет того, что скорость подключения шлюза к локальной сети на порядок выше скорости подключения шлюза к Интернету) при передаче крупного объекта обработка с использованием метода «частичного сканирования» занимает примерно такое же время, что и обработка с использованием стандартного метода «отложенного сканирования».

5.4. Подключаемый фильтр ESETS для кэширующего прокси-сервера SafeSquid

В предыдущих разделах описана интеграция ESET NOD32 Gateway Security с HTTP- и FTP-службами интернет-шлюза при помощи **esets_http** и **esets_ftp**. Описанные методы применимы для большинства обычных пользовательских агентов, включая хорошо известный интернет-прокси для фильтрации содержимого SafeSquid (http://www.safesquid.com). Однако для этого особого случая в ESET NOD32 Gateway Security также предлагается альтернативный способ защиты служб шлюза при помощи модуля esets_ssfi.so, специально разработанного для этой цели.

5.4.1. Принципы работы

Подключаемый модуль **esets_ssfi.so** предназначен для доступа ко всем объектам, обрабатываемым кэширующим прокси-сервером SafeSquid, при помощи особого интерфейса, созданного разработчиками SafeSquid для этой цели. После осуществления доступа модуля к объекту, последний будет сканирован на наличие вирусов при помощи *демона ESETS*. Если объект заражен, SafeSquid блокирует соответствующий ресурс и вместо него направляет предварительно определенную шаблонную страницу. Обратите внимание, что **esets_ssfi.so** поддерживается в SafeSquid Advanced начиная с версии 4.0.4.2.

5.4.2. Установка и настройка

Чтобы интегрировать модуль, необходимо установить связи между каталогом модулей SafeSquid и соответствующими расположениями установки программного пакета ESET NOD32 Gateway Security. В приведенном ниже примере предполагается, что SafeSquid установлен в ОС Linux в каталоге /opt/safesquid.

Если установлено программное обеспечение SafeSquid версии 4.2 и выше, введите следующие команды:

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

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

Если установлено программное обеспечение SafeSquid версии ниже 4.2, введите следующие команды:

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

Чтобы завершить установку подключаемого модуля SafeSquid, войдите в веб-интерфейс администрирования SafeSquid, на главной странице интерфейса выберите меню «Конфигурация» (Config) и в поле «Выбор раздела для настройки» (Select a Section to Configure) при помощи прокрутки найдите раздел «ESET NOD32 Gateway Security». Затем создайте профиль антивируса для раздела «ESET NOD32 Gateway Security». Для этого щелкните «Добавить» (Add) в нижней части раздела «ESET NOD32 Gateway Security» и в появившемся списке определите следующие параметры:

```
Комментарий: ESET NOD32 Gateway Security

Профили: антивирус
```

После установки подключаемый модуль SafeSquid готов к работе. Однако в конфигурацию SafeSquid необходимо внести еще несколько небольших уточнений. Далее будут показаны настройки SafeSquid, необходимые для использования предварительно определенных шаблонов блокировки ESETS, которые будут применяться, если переданный объект заражен (или, соответственно, не сканирован).

Войдите в веб-интерфейс администрирования SafeSquid, на главной странице интерфейса откройте меню «Конфигурация» (Config) и в поле «Выбор раздела для настройки» (Select a Section to Configure) при помощи прокрутки найдите раздел «ESET NOD32 Gateway Security». Затем измените вновь созданный профиль антивируса. Для этого щелкните «Изменить» (Edit) в нижней части раздела «ESET NOD32 Gateway Security» и в появившемся списке определите следующие параметры:

```
Шаблон «инфицировано»: esets_infected
Шаблон «не сканировано»: esets_not_scanned
```

После сохранения списка шаблонов перейдите на страницу «Шаблоны» (Templates) главного меню «Конфигурация» (Config). Будет показан параметр «Путь» (Path), который определяет путь к каталогу шаблонов SafeSquid (далее предполагается, что этому параметру присвоено значение /opt/safesquid/templates). Убедитесь, что соответствующий каталог существует. В противном случае создайте его. Чтобы получить доступ к предварительно определенным шаблонам ESETS из этого каталога, необходимо установить соответствующие связи при помощи следующих команд командного процессора:

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

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

Также необходимо добавить определения новых шаблонов в конфигурацию SafeSquid. Для этого щелкните «Добавить» (Add) в разделе «Шаблоны» (Templates). Для страницы блокировки зараженных объектов ESETS в появившемся списке необходимо определить следующие параметры:

```
Комментарий: ESET NOD32 Gateway Security infected template
Имя: esets_infected
Файл: ssfi_infected.html
Тип Mime: text/html
Код ответа: 200
Тип: файл
Анализируемый: да
```

Соответственно, для страницы блокировки несканированных объектов ESETS список выглядит так:

```
Комментарий: ESET NOD32 Gateway Security not scanned
template
Имя: esets_not_scanned
Файл: ssfi_not_scanned.html
Тип Mime: text/html
Код ответа: 200
Тип: файл
Анализируемый: да
```

Для повторного считывания вновь созданной конфигурации перезагрузите SafeSquid и демон ESETS.

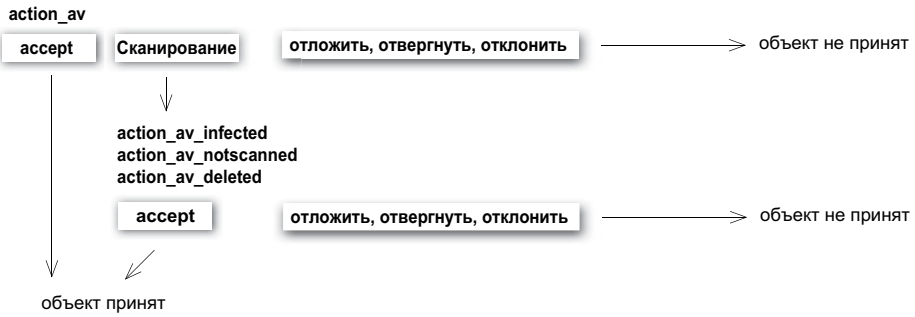
Глава 6

Основные механизмы ESET NOD32 Gateway Security

6.1. Политика обработки объектов

Политика обработки объектов (см. рис. 6–1) – это механизм, обеспечивающий обработку просканированных объектов в соответствии с их статусом сканирования. Механизм основан на так называемых опциях настройки действий action_av, action_av_infected, action_av_notscanned, action_av_deleted. Для получения более подробной информации по этим опциям обратитесь к разделу руководства, посвященному esets.cfg(5).

Рис. 6–1. Схема механизма политик обработки объектов



Каждый обрабатываемый объект вначале рассматривается с учетом настройки опции конфигурации action_av. Если для опции установлено значение «принять» (accept) (соответственно, «отложить» (defer), «сбросить» (discard), «отклонить» (reject)), объект будет принят (соответственно, отложен, сброшен, отклонен). Если для опции установлено значение «сканировать» (scan), объект будет сканирован на наличие вирусов (и, соответственно, очищен, если это требуется в соответствии с опцией настройки av_clean_mode). Для оценки дальнейшей обработки объекта будет учитываться набор опций настройки действий action_av_infected, action_av_notscanned и action_av_deleted. Если в результате применения трех представленных выше опций действий было выполнено действие «принять», обработанный объект будет принят. В противном случае объект блокируется.

ПРИМЕЧАНИЕ. Следует учесть, что некоторые модули были написаны с целью обеспечить интеграцию ESETS в среду, в которой изменение сканируемых объектов недопустимо. В связи с этим соответствующая функциональность в модуле отключена. В частности, это означает, что опция настройки **av_clean_mode** будет игнорироваться модулем. Для получения более подробной информации по этой теме см. соответствующие страницы руководства, посвященные модулям.

6.2. Настройки пользователя

В продукте используется механизм настроек пользователя, который предоставляет администратору более широкие возможности настройки. Он позволяет выборочно определять параметры антивирусного сканирования ESETS для идентификации клиента/сервера.

Более подробное описание этих возможностей см. в разделе руководства, посвященном esets.cfg(5), а также в указанных там разделах. Поэтому здесь будет приведен лишь краткий пример настройки пользователя.

Предположим, **esets_http** используется для контроля HTTP-трафика порта 8080 шлюзового сервера с локальным IP-адресом 192.168.1.10. Настройка модуля осуществляется в разделе [http] *файла конфигурации ESETS*. Раздел выглядит следующим образом.

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

Чтобы указать индивидуальные настройки параметров, необходимо определить параметр user_config и путь к особому файлу конфигурации, в котором хранятся эти настройки. В следующем примере создается ссылка на файл специальных настроек esets_http_spec.cfg, расположенный в *каталоге настроек ESET*S.

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

После создания в разделе [http] ссылки на файл специальных настроек необходимо создать этот файл в *каталоге настроек ESETS* и прописать в нем соответствующие индивидуальные настройки. Вот как выглядит индивидуальная настройка параметра action_on_processed для IP-адреса клиента 192.168.1.40.

```
[|192.168.1.40]

action_av = ”reject”
```

Обратите внимание, что название заголовка особого раздела содержит сведения идентификации HTTP-клиента, для которого созданы индивидуальные настройки. В теле раздела содержатся индивидуальные параметры, указанные для соответствующей идентификационной записи. Таким образом, при помощи этой специальной настройки HTTP-трафик всех клиентов локальной сети будет обрабатываться, т. е, сканироваться на обнаружение проникновений, а трафик клиента, определенного IP-адресом 192.168.1.40, будет отклонен или блокирован в любом случае.

6.3. «Черные» и «белые» списки

В следующем примере показано создание «черных» и «белых» списков для модуля esets_http, настроенного как HTTP прокси-сканер. Обратите внимание, что для этой цели используется конфигурация, описанная в предыдущем разделе.

Таким образом, чтобы создать «черный список», используемый в **esets_http**, необходимо создать следующий групповой раздел в файле специальных настроек **esets_http_spec.cfg**, описанном в предыдущем разделе документации.

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

Далее необходимо добавить какой-либо HTTP-сервер в «черный» список. Для этого нужно создать особый раздел

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

где aaa.bbb.ccc.ddd – это IP-адрес сервера, добавленного в «черный список». Обратите внимание, что при такой настройке будет отклоняться весь HTTP-трафик, связанный с указанным сервером, то есть сервер будет заблокирован.

Если требуется создать «белый список», используемый в **esets_http**, необходимо создать следующий групповой раздел в файле специальных настроек **esets_http_spec.cfg**, описанном в предыдущем разделе документации.

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

Добавление HTTP-серверов в список объяснений не требует.

6.4. Система предоставления образцов

Система предоставления образцов – это интеллектуальная технология ThreatSense.NET, которая обеспечивает перехват зараженных объектов, обнаруженных методом расширенной эвристики, и доставку этих объектов на сервер системы предоставления образцов. Все образцы вирусов, отобранные системой, исследуются сотрудниками лаборатории в компании ESET и затем при необходимости добавляются в базу данных вирусов.

ПРИМЕЧАНИЕ. В СООТВЕТСТВИИ С УСЛОВИЯМИ НАШЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ, ЗАПУСКАЯ СИСТЕМУ ПРЕДОСТАВЛЕНИЯ ОБРАЗЦОВ, ВЫ ДАЕТЕ РАЗРЕШЕНИЕ КОМПЬЮТЕРУ ИЛИ ПЛАТФОРМЕ, НА КОТОРОЙ УСТАНОВЛЕН ДЕМОН ESETS_DAEMON, СОБИРАТЬ ДАННЫЕ (КОТОРЫЕ МОГУТ ВКЛЮЧАТЬ ЛИЧНЫЕ СВЕДЕНИЯ О ВАС И ПОЛЬЗОВАТЕЛЯХ ДАННОГО КОМПЬЮТЕРА) И ОБРАЗЦЫ ВНОВЬ ОБНАРУЖЕННЫХ ВИРУСОВ ИЛИ ДРУГИХ УГРОЗ И ОТПРАВЛЯТЬ ИХ В ВИРУСНУЮ ЛАБОРАТОРИЮ. ПО УМОЛЧАНИЮ ЭТА ФУНКЦИЯ ОТКЛЮЧЕНА. ЭТА ИНФОРМАЦИЯ И ДАННЫЕ БУДУТ ИСПОЛЬЗОВАНЫ НАМИ ТОЛЬКО ДЛЯ ИЗУЧЕНИЯ УГРОЗ, И МЫ ПРИМЕМ ВСЕ ЦЕЛЕСООБРАЗНЫЕ МЕРЫ ПО СОХРАНЕНИЮ КОНФИДЕЦИАЛЬНОСТИ ДАННОЙ ИНФОРМАЦИИ.

Для включения системы выдачи образцов требуется подключить её кэш. Для этого следует включить опцию настройки samples_enabled в разделе [global] *файла конфигурации ESETS*. Чтобы включить процесс предоставления образцов на серверы вирусной лаборатории ESET, необходимо также включить параметр samples_send_enabled в том же разделе.

Пользователь может принять решение о предоставлении сотрудникам вирусной лаборатории ESET дополнительных сведений. Для этого используются опция samples_provider_mail или samples_provider_country. Эта информация помогает получению представления о том, какие угрозы распространяются через Интернет.

Для получения более подробной информации о системе предоставления образцов обратитесь к разделу руководства, посвященному esets_daemon(8).

6.5. Веб-интерфейс

Веб-интерфейс обеспечивает удобство настройки, администрирования и управления лицензиями ESETS.

Этот модуль является отдельной программой-агентом и должен быть активирован явным образом. Для быстрого запуска установите все следующие опции в *файле конфигурации ESETS* и перезапустите *демон ESETS:*

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

Для получения более подробной технической информации о **esets_wwwi** обратитесь к разделу руководства, посвященному esets_wwwi(1).

6.6 Удаленное администрирование

В ESETS используется ESET Remote Administration для обеспечения удаленного управления в компьютерных сетях. Более подробные сведения см. в руководстве по ESET Remote Administrator.

Клиент ESETS Remote Administration является частью основного демона ESETS. Для выполнения основной настройки укажите адрес сервера ERA в параметре racl_server_addr (и racl_password, если необходимо) в разделе [global] файла конфигурации ESETS. Все переменные клиента RA см. на страницах руководства, посвященных esets_daemon(8).

Клиент Unix ESETS RA обладает следующей функциональностью:

- вход на сервер ERA и предоставление системных сведений, данных о конфигурации, состоянии и характеристиках защиты;
- конфигурацию можно просмотреть и изменить при помощи редактора конфигурации ESET (ESET Configuration Editor), также применить при помощи задачи «Конфигурирование»;
- выполнение задач «Сканирование по запросу» (On-Demand Scan) и «Обновить сейчас» (Update Now) по требованию с отправкой журналов сканирования на сервер ERA;
- отправка важных результатов сканирования, выполненного демоном ESETS, в журнал угроз;
- отправка всех сообщений, не относящихся к отладке, в журнал событий.

Следующие функции не поддерживаются:

- журнал файервола;
- удаленная установка.

Глава 7

Обновление системы ESET Security

7.1. Служебная программа обновления *ESETS*

Для обеспечения эффективности работы ESET NOD32 Gateway Security требуется регулярное обновление базы данных вирусных сигнатур. Для этой цели разработана служебная программа esets_update (дополнительные сведения см. на страницах руководства, посвященных esets_update(8)). Чтобы запустить обновление, необходимо определить опции настройки av_update_username и av_update_password в разделе [global] файла конфигурации ESETS. Следует учесть, что при подключении к Интернету через HTTP-прокси также необходимо указать опции proxy_addr, proxy_port и при необходимости proxy_username и proxy_ password. Для запуска обновления введите команду:

```
@SBINDIR@/esets_update
```

Для обеспечения максимальной безопасности сотрудники ESET непрерывно собирают определения вирусов по всему миру. Новые образцы могут появляться в базе через очень короткие промежутки времени. Поэтому рекомендуется регулярно выполнять обновление. Обратите внимание, что демон ESETS может выполнять периодическое обновление системы, если демон запущен и в разделе [global] файла конфигурации ESET указана опция av_update_period.

7.2. Описание процесса обновления *ESETS*

Процесс обновления состоит из двух этапов. Во-первых, с исходного сервера ESET загружаются так называемые предварительно скомпилированные модули. Если в разделе [global] файла конфигурации ESETS включена опция настройки av_mirror_enabled, в каталоге будет создаваться зеркало этих модулей:

```
@BASEDIR@/mirror
```

Следует учесть, что путь к каталогу зеркала может быть переопределен при помощи опции настройки av_mirror_dir в разделе [update] файла конфигурации ESET. Таким образом, вновь созданное зеркало служит как полнофункциональный сервер загрузки модулей и может использоваться для создания подчиненных зеркал. Однако для этого требуется соблюдение нескольких условий. Во-первых, на компьютере, откуда будут загружаться модули, должен быть установлен http-сервер. Во-вторых, модули, подлежащие загрузке другими компьютерами, должны быть расположены в каталоге с путем:

```
/http-serv-base-path/eset_upd
```

где **http-serv-base-path** является основным путем к каталогу http-сервера, поскольку это первое расположение, где служебная программа обновления ищет модули.

Вторым этапом процесса обновления является компиляция модулей, загружаемых сканером ESET NOD32 Gateway Security, из модулей, сохраненных в локальном зеркале. Обычно создаются следующие модули загрузки ESETS: модуль загрузчика (em000.dat), модуль сканирования (em001.dat), модуль базы данных вирусных сигнатур (em002.dat), модуль поддержки архивов (em003.dat), модуль расширенной эвристики (em004.dat) и т. д. в каталоге:

```
@BASEDIR@
```

Обратите внимание, что это тот же каталог, из которого демон ESETS загружает модули. Таким образом, он может быть переопределен при помощи опции настройки **base_dir** в разделе [global] файла конфигурации ESETS.

Глава 8

Обратная связь

Уважаемый пользователь! Данное руководство должно было предоставить достаточный объем сведений об установке, настройке и поддержке программного пакета ESET NOD32 для защиты сервера. Однако написание документации никогда нельзя считать завершенным. Всегда будут обнаруживаться отдельные моменты, которые могли бы быть освещены лучше или даже не были затронуты совсем. Поэтому просим сообщать о найденных в данной документации ошибках или несоответствиях в наш центр поддержки по адресу

http://esetnod32.ru/support/

Будем рады помочь в решении любых проблем, касающихся данного продукта.

Приложение А. Описание процесса настройки ESETS

A.1. Настройка ESETS для сканирования HTTP-соединений в прозрачном режиме

Сканирование HTTP-соединений выполняется при помощи демона esets_http. В разделе [http] *файла конфигурации ESETS* установите следующие параметры:

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

где listen_addr является адресом интерфейса локальной сети с именем *if0*. Затем выполните перезапуск демона ESETS. Далее следует перенаправить все HTTP-запросы в **esets_http**. Если IP-фильтрация обеспечивается инструментом администрирования ipchains, необходимо использовать следующее правило:

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

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

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

соответственно, если используется инструмент ipfw (в случае ОС BSD), необходимо использовать следующее правило:

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

A.2. Настройка ESETS для сканирования FTP-соединений в прозрачном режиме

Сканирование FTP-соединений выполняется при помощи демона **esets_ftp**. В разделе [ftp] *файла конфигурации ESETS* установите следующие параметры:

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

где **listen_addr** является адресом интерфейса локальной сети с именем if0. Затем выполните перезапуск *демона ESETS*. Далее следует перенаправить все FTP-запросы в **esets_ftp**. Если IP-фильтрация обеспечивается инструментом администрирования ipchains, необходимо использовать следующее правило:

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

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

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

соответственно, если используется инструмент ipfw (в случае ОС BSD), необходимо использовать следующее правило:

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

Приложение А. Лицензия PHP

Лицензия PHP, версия 3.01, (c) PHP Group, 1999–2006. Все права защищены. Распространение и использование в форме исходных кодов и бинарных файлов, с изменениями или без таковых, разрешается при условии соблюдения следующих условий.

1. Распространение исходного кода должно происходить с сохранением вышеуказанного уведомления об авторских правах, данного списка условий и приведенного ниже отказа от ответственности.

2. При распространении в форме бинарных файлов в документации и/или других материалах, предоставляемых с дистрибутивом, должны воспроизводиться вышеуказанное уведомление об авторских правах, данный список условий и приведенный ниже отказ от ответственности.

3. Название «PHP» не должно использоваться для поддержки или продвижения продуктов, созданных на основе данного программного обеспечения, без предварительного письменного разрешения. Для получения письменного разрешения обратитесь по адресу group@php.net.

4. Продукты, созданные на основе данного программного обеспечения, не могут быть названы «PHP», и «PHP» не может являться частью их наименования без предварительного письменного разрешения, которое может быть получено по адресу group@php.net. Допускается указание того, что программное обеспечение работает в сочетании с PHP. В этом случае должна использоваться формулировка «Нечто для PHP» вместо названия «Нечто PHP» или «phpнечто».

5. PHP Group может публиковать обновленные и/или новые версии лицензии при необходимости. Каждой версии будет присваиваться отличительный номер. После публикации рассматриваемого здесь кода в рамках конкретной версии лицензии его использование может продолжаться в соответствии с условиями упомянутой версии. Также можно использовать рассматриваемый здесь код в соответствии с условиями любой последующей версии лицензии, опубликованной PHP Group. PHP Group обладает исключительным правом изменять условия, применимые к рассматриваемому здесь коду, созданному в соответствии с данной лицензией.

6. При распространении в любой форме должно сохраняться следующее уведомление: «В данном продукте содержится программное обеспечение PHP, свободно распространяемое и доступное по адресу http://www.php.net/software/».

ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО ГРУППОЙ РАЗРАБОТЧИКОВ PHP «КАК ЕСТЬ». НАСТОЯЩИМ ЗАЯВЛЯЕТСЯ ОТКАЗ ОТ ЛЮБЫХ ГАРАНТИЙ, ЯВНЫХ ИЛИ СКРЫТЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ) СКРЫТЫЕ ГАРАНТИИ ПРИГОДНОСТИ И АДЕКВАТНОСТИ КОНКРЕТНОЙ ЦЕЛИ. ГРУППА РАЗРАБОТЧИКОВ PHP ИЛИ ЕЕ УЧАСТНИКИ НИ В КАКОМ СЛУЧАЕ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА ЛЮБЫЕ ПРЯМЫЕ, КОСВЕННЫЕ, ДОПОЛНИТЕЛЬНЫЕ, ШТРАФНЫЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ/УЩЕРБ (ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ) ПРИОБРЕТЕНИЕ СУРРОГАТНЫХ ТОВАРОВ И УСЛУГ, УБЫТКИ, НЕДОПОЛУЧЕНИЕ КОММЕРЧЕСКОЙ ПРИБЫЛИ, ПРЕРЫВАНИЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ, УТРАТУ КОММЕРЧЕСКИХ СВЕДЕНИЙ И ТОМУ ПОДОБНОЕ), ВОЗНИКШИЕ ПО КАКОЙ-ЛИБО ПРИЧИНЕ ИЛИ НА ОСНОВАНИИ КАКОЙ-ЛИБО ТЕОРИИ ОТВЕТСТВЕННОСТИ, КАК КОНТРАКТНОЙ, ТАК И ОБЪЕКТИВНОЙ ЛИБО ГРАЖДАНСКОЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ ИЛИ ИНОЕ), ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЛЮБЫМ СПОСОБОМ, ДАЖЕ ЕСЛИ БЫЛО ИЗВЕСТНО ЛИБО ДОЛЖНО БЫЛО БЫТЬ ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ/УЩЕРБА.