



we protect your digital worlds

## **ESET Mail Security**

*Посібник користувача*

## **Зміст**

<b>1. Введення .....</b>	<b>3</b>
<b>2. Терміни та аббревіатури.....</b>	<b>5</b>
<b>3. Інсталяція.....</b>	<b>9</b>
<b>4. Огляд внутрішньої будови.....</b>	<b>11</b>
<b>5. Інтеграція із слжбами Інтернет шлюзів.....</b>	<b>14</b>
5.1. Двунправлене сканування e-mail повідомлень в МТА.....	16
5.2. Сканування вхідних e-mail повідомлень.....	17
5.3. Сканування вихідних e-mail повідомлень.....	17
5.4. Сканування e-mail повідомлень завантажених з POP3/IMAP сервера.....	18
5.5. Альтернативні способи сканування вмісту.....	18
5.5.1. Сканування e-mail повідомлень за допомогою AMaViS.....	18
5.5.1.1. amavis.....	18
5.5.1.2. amavisd.....	19
5.5.1.3. amavisd-new.....	19
<b>6. Важливі механізми ESET Mail Security.....</b>	<b>21</b>
6.1. Політика обробки об'єктів (Handle Object Policy).....	22
6.2. Налаштування користувача (User Specific Configuration).....	23
6.3. «Білі» та «Чорні» списки.....	24
6.4. Антиспам Контроль.....	24
6.5. Система обробки зразків (Samples Submission System).....	25
6.6. Веб-Інтерфейс.....	25
6.7. Віддалена настройка.....	26
<b>7. Оновлення системи ESET Mail Security.....</b>	<b>27</b>
7.1. Утиліта оновлення ESETS.....	28
7.2. Опис процесу оновлення ESETS.....	28
<b>8. Оповіщення.....</b>	<b>30</b>
<b>Доповнення А. Опис процесу настройки ESETS.....</b>	<b>32</b>
<b>Доповнення В. Ліцензія PHP.....</b>	<b>42</b>

Copyright © 2007 ESET, spol. s r. o.

ESET Gateway Security розроблено ESET, spol. s r. o. За більш детальною інформацією звертайтесь до [www.eset.com.ua](http://www.eset.com.ua)

Всі права захищено. Жодна з частин цього документу не може бути скопійована, збережена або представлена у будь-якій системі зберігання даних або передана у будь-якій формі, будь-якими засобами (електронними, фотокопіювальними, записувачими, скануючими або іншими) та у будь-яких цілях без спеціальної письмової згоди з автором.

Компанія ESET, spol. s r. o. залишає за собою право змінити будь-яку частину описаної програми без попередження.

Розділ 1:

# Введення

Шановний користувач, Ви придбали ESET Mail Security – найсучаснішу систему безпеки, яка працює на основі ОС Linux/BSD/Solaris. Як Ви згодом переконаєтесь, досконалість механізму сканування ESET має неперевершені швидкість сканування та рівень виявлення загроз у поєднанні з малим розміром, що робить його ідеальним продуктом для будь-якої Linux/BSD/Solaris серверної ОС. У даному документі будуть описані основні функціональні можливості системи.

Головні характеристики системи:

- Алгоритми механізму антивірусного сканування ESET забезпечують найвищий рівень виявлення загроз за найменший час сканування.
- ESET Mail Security розроблений для роботи на однопроцесорних та багатопроцесорних системах.
- Продукт має функцію евристичного аналізу Win32 на виявлення черв'яків та обхідних шляхів.
- Встроєні архіватори розпаковують архівовані об'єкти не потребуючи наявності інших програм.
- Для покращення швидкості та продуктивності системи, її архітектура основана на процесі (резидентній програмі) якому відсилаються усі запити на сканування.
- Для підвищення рівня безпеки всі виконуючі процеси (окрім esets\_dac) запускаються під обліковим записом з обмеженими правами доступу.
- Система підтримує налаштування конфігурацію, основану на потребах користувача або клієнта\сервера.
- Для отримання інформації про активність системи та виявлення загроз можна настроїти шість рівнів ведення журналу.
- Конфігурація, керування та настройки ліцензії забезпечуються за допомогою легкого у користуванні веб-інтерфейсу
- Система підтримує ESET Remote Administrator, для віддаленого керування продуктом у великих мережах.
- Інсталяція ESET Mail Security не потребує зовнішніх бібліотек або програм за виключенням LIBC.
- У системі можна настроїти оповіщення будь-якого користувача, при виявленні загрози.

Для продуктивної роботи ESET Mail Security потрібно лише 16MB пам'яті на жорсткому диску та 32MB ОЗП. Програма працює на основі ОС Linux версій ядра 2.2.x, 2.4.x та 2.6.x та ОС FreeBSD версій ядра 5.x, 6.x.

Починаючи з менш потужних серверів для малих офісів і до ISP серверів на підприємствах з тисячами підключених користувачів, система забезпечує продуктивність, легкість інтеграції та перенесення, які Ви очікуєте від рішень на основі Unix, і у додаток забезпечує незрівнянний рівень безпеки.

Розділ 2:

## **Терміни та аббревіатури**

У цьому розділі будуть розглянуті терміни та аббревіатури, які використовуватимуться у документі (тільки PDF формат). Зверніть увагу, що жирним шрифтом будуть виділені назви компонентів продукту, а також нові терміни та аббревіатури. Усі терміни та аббревіатури зазначені у даному розділі будуть описані більш детально далі у документі (тільки PDF формат).

## ESETS

**ESET Security** стандартне скорочення для всіх продуктів безпеки, розроблених компанією ESET, для ОС Linux, BSD та Solaris. Також термін використовується, як назва (або частина назви) пакету програм у якому міститься продукт.

## RSR

Абревіатура для 'RedHat/Novell(SuSE) Ready'. Зверніть увагу, що ми підтримуємо різні версії продуктів RedHat Ready та Novell (SuSE) Ready. Пакет RSR відрізняється від «стандартних» версій Linux тим, що він підтримує FHS (File-system Hierarchy Standard яка є частиною Linux Standard Base) - документ, що потребується для сертифікації RedHat Ready та Novell(SuSE) Ready. Це значить, що пакет RSR інсталується як програма-доповнення – за замовчуванням, у папку '/opt/eset/esets'.

## Процес ESETS

Головний процес сканування та контролю системи ESETS : **esets\_daemon**.

## Основна папка ESETS

Папка, у якій зберігаються завантаженні модулі ESETS, наприклад, бази даних вірусних сигнатур. Надалі у документі використовуватиметься аббревіатура **@BASEDIR@** для позначення даної папки. Шлях директорії наведено нижче:

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

## Папка конфігурацій ESETS

Папка, де зберігаються усі файли конфігурації ESET Mail Security. Надалі у документі використовуватиметься аббревіатура **@ETCDIR@** для позначення даної папки. Шлях директорії наведено нижче:

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

## Файл конфігурації ESETS

Головний файл конфігурації ESET Mail Security. Абсолютний шлях файлу наступний:

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

### Папка бінарних файлів ESETS

Папка, де зберігаються необхідні бінарні файли ESET Mail Security. Надалі у документі використовуватиметься аббревіатура **@BINDIR@** для позначення даної папки. Шлях директорії наведено нижче:

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

### Папка системних бінарних файлів ESETS

Папка, де зберігаються системні бінарні файли ESETS. Надалі у документі використовуватиметься аббревіатура **@SBINDIR@** для позначення даної папки. Шлях директорії наведено нижче:

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

### Папка об'єктних файлів ESETS

Папка, де зберігаються необхідні об'єктні файли та бібліотеки ESET Mail Security. Надалі у документі використовуватиметься аббревіатура **@SBINDIR@** для позначення даної папки. Шлях директорії наведено нижче:

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



Розділ 3:

# Інсталяція

Даний продукт розповсюджується у вигляді бінарного файлу:

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

де 'ext' це частина назви, яка залежить від версії дистрибутиву ОС Linux/BSD/Solaris. 'deb' означає Debian, 'rpm' - RedHat та SuSE, 'tgz' означає інші версії продуктів ОС Linux, 'fbs5.tgz' - FreeBSD 5.xx, 'fbs6.tgz' - FreeBSD 6.xx, 'nbs4.tgz' - NetBSD 4.xx та 'solho.pkg.gz' означає Solaris 10.

Зверніть увагу, що формат бінарного файлу для Linux RSR:

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

Щоб виконати інсталяцію або оновити компоненти продукту використовуйте наступну команду:

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

У версіях для продукту Linux RSR використовуйте наступну команду:

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

При цьому на дисплей буде виведено ліцензійну угоду продукту (User License Acceptance Agreement). Щойно Ви погодитесь з умовами угоди, інсталяційний пакет буде скопійовано у поточну директорію і інформація щодо інсталяції пакету, деінсталяції та оновлення компонентів продукту буде зображена на екрані.

Як тільки пакет встановлено, Ви можете впевнитись, що головний процес ESETS запущено, використовуючи наступну команду:

Linux:

```
ps -C esets_daemon
```

BSD:

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

Solaris:

```
ps -A | grep esets_daemon
```

У результаті Ви повинні побачити наступне (або схоже) повідомлення:

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

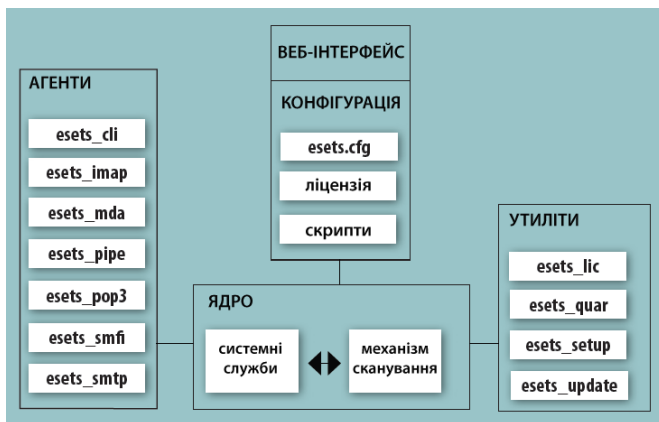
де щонайменше два процеси ESETS запущені у фоновому режимі. Перший PID представляє собою диспетчер контролю процесів та потоків системи. Другий PID є процесом сканування ESETS.

Розділ 4:

## Огляд внутрішньої будови

Як тільки ESET Mail Security успішно інстальований, Вам потрібно ознайомитись з його конфігурацією.

Рисунок 4-1. Структура ESET Gateway Security.



Структура ESET Mail Security зображена на рисунку 4-1. Система складається з наступних частин.

### CORE (Ядро)

Ядром ESET Mail Security є процес **esets\_daemon**. Процес використовує ESETS API бібліотеки libesets.so та ESETS модулі завантаження em00X\_XX.dat для забезпечення основних системних задач як, наприклад, сканування, підтримка агентів-процесів, підтримка Системи обробки зразків (Samples Submission System), підключення до системи, оповіщення тощо. Щоб отримати більш детальну інформацію про esets\_daemon (8) перегляньте сторінки довідки (man pages).

### AGENTS (Агенти)

Призначення модулів агентів - інтеграція ESETS у серверній середі Linux/BSD/Solaris. Зверніть увагу, що даній темі присвячено окремий розділ документу.

### UTILITIES (Утиліти)

Модулі утиліт – це спеціальні частини системи, які забезпечують просте та ефективне керування системою. Вони відповідають за системні задачі такі як: управління ліцензійними файлами, забезпечення належної роботи функції карантину, оновлення та конфігурацію системи. Зверніть увагу, що даній темі присвячено окремий розділ документу.

### CONFIGURATION (Конфігурація)

Належна конфігурація є найважливішим атрибутом продуктивно працюючої системи безпеки – усе написане нижче у цьому розділі, присвячене більш детальному опису компонентів конфігурації. Також рекомендується перечитати інформацію стосовно esets.cfg (5) на сторінках довідника, оскільки даний файл містить важливі параметри конфігурації ESETS.

Після успішної інсталяції продукту, усі компоненти конфігурації знаходитимуться у директорії конфігурацій ESETS, у якій містяться наступні файли.

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

Це найважливіший файл конфігурації, оскільки у ньому містяться всі найнеобхідніші настройки для належного функціонування продукту. Файл esets.cfg має декілька секцій, у кожній з яких зберігаються різні параметри. Файл містить одну загальну секцію і декілька секцій конфігурації агентів. Імена секцій написані у квадратних дужках. Параметри у загальній секції використовуються для визначення конфігурації процесів ESETS та значень за замовчуванням, для настройки механізму сканування. За допомогою параметрів у секції агентів виконується настройка конфігурації всіх модулів та агентів ESET Mail Security. Останні використовуються для перехоплення різних типів даних та підготовки їх до сканування. Зверніть увагу, що у придачу до різних параметрів, які використовуються для настройки системи, також існують правила, які встановлюють організацію файлу. Більш детальну інформацію про те, як найефективніше настроїти цей файл, Ви можете отримати на сторінках довідки (map pages) про esets.cfg(5) та esets\_daemon(8).

### **@ETCDIR@/certs**

У цій папці зберігаються сертифікати, які використовує веб-інтерфейс ESETS для аутентифікації. Більш детальну інформацію про esets\_wwwi(X) можна отримати на сторінці довідки (map page).

### **@ETCDIR@/license**

У цій папці зберігаються ліцензійні ключі продукту (продуктів), які Ви отримали при покупці. Зверніть увагу, якщо параметр 'license\_dir' у файлі конфігурації ESETS не змінено, то процес ESETS буде перевіряти тільки дану директорію на наявність ліцензійного ключа.

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

Якщо активовано параметр 'license\_warn\_enabled' у файлі конфігурації ESETS, то даний скрипт почне виконуватись за 30 днів до закінчення терміну дії ліцензії, висилаючи повідомлення про закінчення терміну дії ліцензії електронною поштою системному адміністратору. Скрипт виконуватиметься раз на день.

### **@ETCDIR@/scripts/daemon\_notification\_script**

Якщо активовано параметр 'exec\_script' у файлі конфігурації ESETS, то даний скрипт буде виконуватись при виявленні загроз антивірусною системою. Він використовується для надсилання повідомлень про подію електронною поштою системному адміністратору.

### **@ETCDIR@/anti-spam**

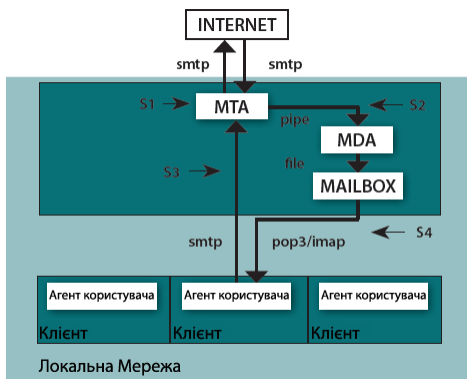
В даній директорії знаходиться файл конфігурації, який використовується для належної настройки механізму антиспам системи.

Розділ 5:

# **Інтеграція з системою e-mail повідомлень**

У даному розділі буде описано інтеграцію ESET Mail Security з різними системами e-mail повідомлень. Знання основних принципів роботи подібних систем (рисунок 5-1) є головною передумовою розуміння механізмів ESETS.

**Рисунок 5-1. Схема системи e-mail повідомлень ОС UNIX.**



MTA - Mail Transport Agent (Агент Пересилки Повідомлень)

Програма (наприклад, sendmail, postfix, qmail, exim тощо), що забезпечує передачу e-mail повідомлень серед локальних та віддалених доменів.

MDA - Mail Delivery Agent (Агент Доставки Повідомлень)

Програма (наприклад, maildrop, procmail, deliver, local.mail тощо), що забезпечує доставку e-mail повідомлень з локальною адресою на цільовий поштовий ящик.

MUA - Mail User Agent (Мейл Клієнт)

Програма (наприклад, MS Outlook, Mozilla Mail, Eudora тощо), що забезпечує доступ до повідомлень, які знаходяться у поштовому ящику, та їх управління, наприклад, читання, створення нових повідомлень, друк тощо.

## ПОШТОВИЙ ЯЩИК

Файл або структура файлів, яка використовується як місце зберігання e-mail повідомлень. Зверніть увагу, що у ОС Linux/BSD/Solaris існує декілька форматів ПОШТОВОГО ЯЩИКА: старий стиль, у якому e-mails повідомлення кожного користувача зберігаються послідовно у одному окремому файлі користувача (/var/spool/mail); MBOX (оновлений але загалом старий формат), у якому e-mail повідомлення зберігаються послідовно в одному файлі, який знаходиться у домашній директорії користувача; MAILDIR, у якому e-mail повідомлення зберігаються у окремих файлах директорії з ієрархічною структурою.

Передача даних на поштовий сервер зазвичай виконується за допомогою SMTP

- Simple Mail Transfer Protocol. Отримане повідомлення або пересилається MTA до іншої системи e-mail повідомлень, або доставляється MDA цільовому ПОШТОВОМУ ЯЩИКУ (передбачається, що кожний користувач має ПОШТОВИЙ ЯЩИК, який знаходиться на жорсткому диску сервера). Зверніть увагу, що завантаження та належна інтерпретація повідомлення на комп'ютері клієнта є функцією локального MUA. Під час отримання даних з ПОШТОВОГО ЯЩИКА, зазвичай MUA використовує POP3 - Post Office Protocol або IMAP - Internet Message Access Protocol, для з'єднання з MTA. Щоб переслати данні через Internet виконується з'єднання за допомогою протоколу SMTP.

Принцип роботи ESETS оснований на перехопленні даних, під час обміну, та їх сканування на різних етапах передачі. Схематично, перехоплення зображені на рисунку 4-1 і позначені як S1, S2, S3 та S4.

S1

Двонаправлене сканування e-mail повідомлень, наприклад, фільтрація вмісту в MTA.

S2

Сканування вхідних e-mail повідомлень, тобто повідомлень, цільова адреса яких відповідає адресі всередині локального домену.

S3

Сканування вихідних e-mail повідомлень, тобто повідомлень, цільова адреса яких обмежена певним Інтернет доменом.

S4

Сканування e-mail повідомлень, завантажених з POP3/IMAP сервера.

Наступна частина розділу присвячена методам інтеграції ESETS з різними поштовими системами.

## 5.1. Двонаправлене сканування e-mail повідомлень в MTA

Перевага модуля двонаправленого сканування e-mail повідомлень полягає у тому, що він надає можливість сканування вхідних та вихідних повідомлень по одному й тому ж алгоритму дій. З іншої сторони двонаправлений метод (фільтрація вмісту) залежний від MTA. У продукт ESET чотири фільтри вмісту розроблені для найбільш популярних MTA, тобто MTA Sendmail, Postfix, Exim, QMail та ZMailer.

Щоб настроїти двонаправлене сканування e-mail повідомлень у ESET Mail Security, потрібно ввевнитись у належній конфігурації та роботі MTA. Потім запустити наступний скрипт:

```
esets_setup
```

Виберіть опції установки фільтру вмісту MTA. Також буде зображено модуль ESETS, який використовується.

Варто зауважити, що інстальатор зберігає всі зміни конфігураційних файлів і має функцію відображення всіх команд, які будуть виконані після підтвердження. Дану функцію також можна використовувати для деінсталяції. Більш детально процес інсталяції описано у Додатку А.

## 5.2. Сканування вхідних e-mail повідомлень

Сканування вхідних e-mail повідомлень виконується під час обміну даними між MTA та MDA (пересилання повідомлення). Вхідне повідомлення перехоплюється модулем **esets\_mda**, сканується процесом ESETS і пересилається далі в ПОШТОВИЙ ЯЩИК за допомогою MDA. Як показано на рисунку, сканування наявності вірусів можна настроїти за допомогою належних файлів конфігурації модуля MTA та **esets\_mda**. Зверніть увагу, що ESET Mail Security підтримує найбільш поширені MTA, тобто MTA Sendmail, Postfix, Exim, QMail та ZMailer, а також у ESETS реалізована підтримка всіх MDA. Зокрема, було протестовано наступні MDA: prosmail, maildrop, deliver та local.mail.

Щоб настроїти сканування вхідних e-mail повідомлень у ESET Mail Security, потрібно впевнитись у належній конфігурації та роботі MTA. Потім запустити наступний скрипт:

```
esets_setup
```

Виберіть опції установки фільтру вмісту MTA. Також буде зображено модуль ESETS, який використовується.

Варто зауважити, що інстальатор зберігає всі зміни конфігураційних файлів і має функцію відображення всіх команд, які будуть виконані після підтвердження. Дану функцію також можна використовувати для деінсталяції. Більш детально процес інсталяції описано у Додатку А.

## 5.3. Сканування вихідних e-mail повідомлень

Сканування вхідних e-mail повідомлень виконується під час обміну даними між MUA та MTA (пересилання повідомлення).

Щоб настроїти сканування вихідних e-mail повідомлень у ESET Mail Security, потрібно запустити наступний скрипт:

```
esets_setup
```

Виберіть опції установки SMTP, що настроїть модуль **esets\_smtp** на прослуховування зазначеного порту та перенаправить IP пакети. Перевірте додане правило брандмауера та видаліть або змініть його відповідно до Ваших потреб.

Варто зауважити, що інстальатор зберігає всі зміни конфігураційних файлів і має функцію відображення всіх команд, які будуть виконані після підтвердження. Дану

функцію також можна використовувати для деінсталяції. Більш детально процес інсталяції описано у Доповненні А.

## 5.4. Сканування е-mail повідомлень завантажених з POP3/IMAP сервера

Щоб настроїти сканування е-mail повідомлень в ESET Mail Security, які завантажено з POP3 (відповідно, IMAP) сервера, запустіть наступний скрипт:

```
esets_setup
```

Виберіть опції установки POP3 або IMAP, що настроїть відповідний модуль на прослуховування зазначеного порту та перенаправить IP пакети. Перевірте додане правило брандмауера та видаліть або змініть його відповідно до Ваших потреб.

Варто зауважити, що інстальатор зберігає всі зміни конфігураційних файлів і має функцію відображення всіх команд, які будуть виконані після підтвердження. Дану функцію також можна використовувати для деінсталяції. Більш детально процес інсталяції описано у Доповненні А.

## 5.5. Альтернативні способи сканування вмісту

### 5.5.1. Сканування е-mail повідомлень за допомогою AMAViS

AMaViS (A Mail Virus Scanner - сканер файлів прикріплених до повідомлень) - це інструмент, який є інтерфейсом для MTA та інших сканерів. Він підтримує різноманітні MTA і має три версії: **amavis**, **amavisd** та **amavisd-new**. Взаємодія AMaViS з ESET Mail Security забезпечується за допомогою **esets\_cli**. Перед тим, як приступити до більш детального опису настройки AMaViS, варто звернути увагу на вплив зазначених методів на функціонування ESET Mail Security.

По-перше, AMaViS не дозволяє модифікувати е-mail повідомлення. Тобто ESETS не може змінити або модифікувати жодний файл, прикріплений до е-mail повідомлення. По-друге, ніяких приміток від системи ESETS з полями заголовку журналу та статусу не буде додано в повідомлення. Також, **amavis** не підтримує даних відправника та одержувача, тому опції настроєної конфігурації не має. Розширена обробка повідомлень (прийняти, відкласти, скинути, відмовити) також обмежена **esets\_cli**. І на останок, він сканує файли, а тому не використовується механізм анти-спам сканування ESETS.

Ураховуючи зазначені недоліки, подібна конфігурація підходить лише якщо особливості продукту не суттєві.

#### 5.5.1.1. amavis

Настройка AMaViS виконується безпосередньо під час інсталяції. Після розпаковки **amavis-o.x.y.tgz**, створіть файл **amavis/av/esets\_cli** з наступним вмістом:

```

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

```

Зверніть увагу, що наведений вище скрипт приймає e-mail повідомлення тільки якщо їх допускає Система обробки об'єктів (Handle Object Policy) **esets\_cli**. У іншому випадку повідомлення блокується. При виявленні вірусу, його ім'я видаляється з вихідних даних.

Далі, при використанні пакету Linux RSR, потрібно оновити змінну середи PATH за допомогою наступної команди:

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

Для успішної інсталяції може виникнути потреба у додатковому ПЗ, як наприклад, arg, unarj, unrar, zoo. Також у директорії /usr/bin потрібно запакувати символічне посилання у формат gzip і створити користувача amavis у відповідній групі з домашньою директорією /var/amavis. Після цього продовжуйте звичайну інсталяцію (./configure, make, make install) і виконуйте правила, зазначені в README.mta, які відповідають Вашому поштовому серверу.

### 5.5.1.2. amavisd

Настройка amavisd виконується під час інсталяції. Розпакуйте amavisd-o.x.tgz і виконайте кроки, описані у підрозділі «5.5.1.1. amavis».

Після використання команди 'make install' може знадобитись перенести файл /usr/etc/amavisd.conf в /etc і повторно виконати команду 'make install'.

### 5.5.1.3. amavisd-new

Щоб установити продукт за допомогою Amavisd-new, розпакуйте та інсталюйте amavisd-new-2.x.y.tgz у Вашу директорію інсталяцій. Потім у файлі amavisd.conf видаліть строку 'ESET Software ESETS' і замініть строку 'ESET Software ESETS - Client/ServerVersion' на наступне:

```
### http://www.eset.com/  
['ESET Software ESETS Command Line Interface',  
 '@BINDIR/esets_cli', '--subdir {}',  
 [0], [1, 2, 3], qr/virus="([^\"]+)" / ],
```

Може виникнути необхідність установки додаткових Perl модулів Archive-Tar, Archive-Zip, BerkeleyDB, Compress-Zlib, Convert-TNEF, Convert-UUlib, IO-stringy, MailTools, MIME-Base64, MIME-tools, Net-Server та Unix-Syslog, які доступні на [www.cpan.org/modules](http://www.cpan.org/modules). У кожному випадку процедура інсталяції буде наступною: perl Makefile.PL; make; make install.

Після настройки, будь-ласка виконайте рекомендації що до конфігурації Amavisd-new - README.mta, що знаходяться в Amavisd-new відповідно до Вашого поштового сервера.

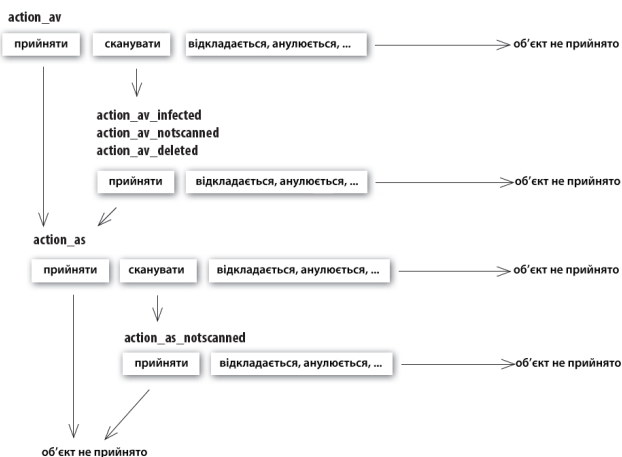
Розділ 6:

## **Важливі механізми ESET Mail Security**

## 6.1. Політика обробки об'єктів (Handle Object Policy)

Політика обробки об'єктів (дивитись рисунок 6-1) – це механізм, що забезпечує фільтрацію сканованих об'єктів відповідно до їх статусу. Ця функціональність основана на опціях настройки дій: 'action\_av', 'action\_av\_infected', 'action\_av\_notscanned', 'action\_av\_deleted'. Щоб отримати детальнішу інформацію про ці опції, продивіться сторінку довідки (map page) esets.cfg(5).

Рисунок 6-1. Схема механізму політики обробки об'єктів.



При проведенні операцій над об'єктом спочатку виконуються дії, відповідно до настройок опції 'action\_av'. Якщо значення цієї опції 'accept' (відповідно або 'defer', 'discard', 'reject') об'єкт приймається (відповідно або відкладається, анулюється, відкидається). Якщо значення опції настроєне на 'scan', об'єкт сканується на наявність вірусних інфільтрації, а якщо значення опції 'av\_clean\_mode' настроєне на 'yes', то при скануванні об'єкт очищується. У придачу, перед подальшими діями з об'єктом ураховуються значення опцій 'action\_av\_infected', 'action\_av\_notscanned' та 'action\_av\_deleted'. Якщо дія 'accept' прийнята, як результат цих трьох опцій, об'єкт приймається. У іншому випадку об'єкт блокується.

Варто зауважити, що об'єкт сканується на спам тільки якщо опція 'action\_as' має значення 'scan'. Також у цьому випадку враховуються значення опцій 'action\_as\_spam' та 'action\_as\_notscanned'. Якщо дія 'accept' прийнята (відповідно, 'defer', 'discard', 'reject'), як результат двох опцій, наведених вище, об'єкт приймається для подальшої обробки (відповідно, відкладається або не приймається)

**ЗВЕРНІТЬ УВАГУ:** Варто зауважити, що деякі модулі написані для забезпечення інтеграції ESETS у середовище, у якому не дозволяється змінювати скановані об'єкти, тому ця функціональність модулю вимкнена. Тобто, це значить, що опція конфігурації `av_clean_mode` буде ігноруватись модулем. Більш детальну інформацію можна отримати на відповідних сторінках довідки (map pages).

## 6.2. Налаштування користувача (User Specific Configuration)

Механізм Налаштування користувача (User Specific Configuration) реалізований з ціллю забезпечити більш високий рівень функціональності конфігурації, що дозволяє системному адміністратору налаштувати параметри антивірусного сканування ESETS відповідно до потреб користувача або сервера.

Зверніть увагу, що більш детальний опис функціональності можна знайти на сторінках довідки (man pages) про `esets.cfg(5)`. Тому в даному розділі будуть наведені лише невеликі приклади Налаштування користувача (User Specific Configuration).

Припустимо, що ми використовуємо модуль `esets_smtp` для фільтрації вмісту MTA Postfix. Налаштування модуля знаходяться у секції `[smtp]` файлу конфігурації ESETS і мають наступний вигляд:

```
[smtp]
agent_enabled = yes
listen_addr = "localhost"
listen_port = 2526
server_addr = "localhost"
server_port = 2525
action_av = "scan"
```

Щоб визначити індивідуальні налаштування, потрібно задати параметр `'user_config'` – шлях до спеціального файлу конфігурації, де будуть зберігатись індивідуальні налаштування. У наступному прикладі створено посилання на файл конфігурації `'esets_smtp_spec.cfg'`, який знаходиться у папці конфігурації ESETS.

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

Як тільки у секції `[smtp]` створено посилання на спеціальний файл конфігурації, потрібно створити файл у папці конфігурації ESETS та задати у ньому належні налаштування.

```
[rcptuser@rcptdomain.com]
action_av = "reject"
```

Зверніть увагу, що назва спеціальної секції містить ідентифікацію одержувача-клієнта, для якого була створена конфігурація. У контексті секції містяться індивідуальні параметри, задані для даної ідентифікації. Таким чином всі е-mail повідомлення будуть оброблені, тобто скановані на наявність інфільтрацій, окрім надісланих на `rcptuser@rcptdomain.com`, які не прийматимуться.

## 6.3. «Білі» та «Чорні» списки

---

У наступному прикладі продемонстровано створення «Чорних» та «Білих» списків для конфігурації **esets\_http** у ролі HTTP проксі-сканера. Зверніть увагу, що для цієї цілі використано настройки, описані у попередньому розділі.

Таким чином для створення «Чорного» списку, який використовує **esets\_http**, потрібно створити наступну секцію-групу в спеціальному файлі конфігурації 'esets\_http\_spec.cfg', який описано в попередньому розділі.

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

Після цього потрібно додати HTTP сервер у групу 'black-list'. Для цього потрібно створити окрему секцію:

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

де 'aaa.bbb.ccc.ddd' – це IP адреса сервера. Зверніть увагу, що при цьому весь HTTP трафік заданого сервера буде відкинута, у даному випадку сервер буде заблоковано.

Якщо потрібно створити «Білий» список, який використовуватиме **esets\_http**, потрібно створити наступну секцію-групу в спеціальному файлі конфігурації 'esets\_http\_spec.cfg', який описано в попередньому розділі.

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

Додати HTTP сервер у список можна аналогічно.

## 6.4. Антиспам Контроль

---

Задача антиспам системи фільтрувати всі спам повідомлення, тобто е-mail повідомлення, які небажані одержувачем, з всього потоку даних у процесі передачі е-mail.

Щоб позбавитись від спам, даний продукт використовує механізм антиспам контролю. Функцію антиспам можна включити за допомогою параметру 'as\_enabled' (опис параметру можна знайти на сторінках довідки esets.cfg(5)). Варто зауважити, що антиспам сканування виконується лише для об'єктів електронної пошти, тобто дана функціональність доступна лише в модулях **esets\_imap**, **esets\_mda**, **esets\_pipe**, **esets\_pop3**, **esets\_smtp** та **esets\_smfi**.

Як тільки функція антиспам включена у будь-якому розділі конфігурації, механізм антиспам сканування запускається під час ініціалізації головного процесу сканування. Під час цього процесу відповідні модулі підтримки антиспам завантажуються з кеш-директорії.

Також можна настроїти функції антиспам у файлі конфігурації:

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

Зверніть увагу на кількість файлів у даній директорії: кожний відповідає окремій рекомендованій конфігурації антиспам механізму. Варто зауважити, що файл конфігурації за замовчуванням - 'spamcatcher.conf.faster'. Щоб використати один з файлів конфігурації, просто замініть 'spamcatcher.conf' потрібним файлом та перезавантажте процес ESETS.

## 6.5. Система обробки зразків (Samples Submission System)

Система обробки зразків реалізована за допомогою інтелектуальної технології ThreatSense.NET, яка збирає інфіковані об'єкти, виявлені за допомогою евристичного аналізу, і відправляє їх на сервер системи обробки зразків ESET. Усі зразки вірусів зібрані Системою обробки зразків будуть проаналізовані у вірусній лабораторії ESET і, при потребі, будуть внесені у базу даних вірусних сигнатур ESET.

**ЗВЕРНІТЬ УВАГУ:** ВІДПОВІДНО ДО НАШОЇ ЛІЦЕНЗІЙНОЇ УГОДИ, ПРИ УВІМКНЕННІ СИСТЕМИ ОБРОБКИ ЗРАЗКІВ ВИ ПОГОДЖУЄТЕСЬ НА ТЕ, ЩО КОМП'ЮТЕР ТА/АБО ПЛАТФОРМА, НА ЯКІЙ ІНСТАЛЬОВАНО ESETS\_DAEMON, МОЖЕ ЗБИРАТИ ДАННІ (ЯКІ МОЖУТЬ ВКЛЮЧАТИ ПЕРСОНАЛЬНУ ІНФОРМАЦІЮ ПРО ВАС ТА/АБО КОРИСТУВАЧА КОМП'ЮТЕРА) ТА ЗРАЗКИ НЕЩОДАВНО ВИЯВЛЕНИХ ВІРУСІВ, АБО ІНШИХ ЗАГРОЗ ТА ВІДСИЛАТИ ЇХ У НАШІ ВІРУСНІ ЛАБОРАТОРІЇ. ВСЯ ЗІБРАНА ІНФОРМАЦІЯ БУДЕ ВИКОРИСТАНА ЛИШЕ ДЛЯ АНАЛІЗУ НОВИХ ЗАГРОЗ І НЕ БУДЕ ВИКОРИСТОВУВАТИСЬ У ІНШИХ ЦІЛЯХ. ЗА ЗАМОВЧУВАННЯМ, ЦЯ ФУНКЦІЯ ВИМКНЕНА.

Щоб активувати Систему обробки зразків, спочатку треба ініціювати кешування. Це можна зробити ввімкнувши опцію 'samples\_enabled' секції [global] у файлі конфігурації ESETS. Щоб ввімкнути відправлення зразків до серверів вірусних лабораторій ESET, у тій же секції задайте параметр 'samples\_send\_enabled'.

У додаток, користувач може забезпечити команду дослідників вірусних лабораторій ESET інформацією опцій 'samples\_provider\_mail' та/або 'samples\_provider\_country'. Ця інформація надасть команді ESET загальні данні про інфільтрацію, яка, можливо, поширюється через Інтернет.

Більш детальну інформацію про Систему обробки зразків можна знайти на сторінці [esets\\_daemon\(8\)](#) довідки (man pages).

## 6.6. Веб-Інтерфейс

Веб-інтерфейс забезпечує легкість настройки конфігурації ESETS, адміністрування та управління ліцензіями ESET.

Цей модуль є окремим агентом і потребує детальної настройки. Щоб швидко настроїти веб-інтерфейс задайте наступні опції файлу конфігурації ESETS, а потім перезапустіть процес ESETS:

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Введіть свої власні параметри замість тих, що подано у якості прикладу. Налаштуйте свій браузер на 'https://адреса:порт' (зверніть увагу на https). Ввійдіть в систему за допомогою 'ім'я користувача/пароль'. Основні поради щодо користування можна знайти на сторінці help, а технічні деталі esets\_wwwi можна знайти на сторінці esets\_wwwi(1) довідки (man pages).

## 6.7. Віддалена настройка

ESETS підтримує ESET Remote Administration для керування у великих комп'ютерних мережах. Більш детальну інформацію можна знайти у Посібнику користувача ESET Remote Administrator на нашому веб-сайті:

<http://eset.com.ua/download/manual>

ESETS Remote Administration Client є частиною процесу ESETS. Для настройки системи задайте адресу Вашого сервера ERA у параметрі 'rac1\_server\_addr' (а також 'rac1\_password', при необхідності) секції [global] файлу конфігурації ESETS. Всі змінні ERA Client описані на сторінках довідки (man pages) про esets\_daemon(8).

Unix ESETS ERA Client виконує наступні функції:

- Взаємодія з сервером ERA та надання даних про Інформацію Системи (System Information), Конфігурацію (Configuration), Стан Захисту (Protection Status) та Функціональність (Features).
- Забезпечення відображення та настройки Конфігурації за допомогою Редактора Конфігурацій ESET (Configuration Editor) та її використання у Задачах Конфігурації (Configuration Task).
- Виконання сканування за вимогою та Задачі негайного Оновлення (Update Now Tasks) відповідно до запиту та відправка Журналу Сканування (Scan Logs) серверу ERA.
- Відправка повідомлень про сканування, виконані процесом ESETS, до Журналу Загроз (Threat Log).
- Відправка всіх неопрацьованих повідомлень до Журналу Подій (Event Log).

Наступні функції не підтримуються:

- Ведення Журналу Брандмауера
- Віддалена Інсталяція

Розділ 7:

# Оновлення системи ESET Mail Security

## 7.1. Утиліта оновлення ESETS

---

Щоб забезпечити ефективність ESET Mail Security, необхідно використовувати найостанніші оновлення бази даних вірусних сигнатур. Спеціально для цього була розроблена утиліта **esets\_update** (Більш детальну інформацію про esets\_update(8) можна отримати на сторінці довідки (man pages)). Щоб запустити оновлення, потрібно настроїти опції 'av\_update\_username' та 'av\_update\_password' у секції [global] файлу конфігурації ESETS. Варто зауважити, що якщо Ви підключаєтесь до Інтернет через HTTP проксі-сервер, то потрібно настроїти додаткові опції 'proxu\_addr', 'proxu\_port' і при потребі 'proxu\_username' та 'proxu\_password'. Для запуску оновлення введіть наступну команду:

```
@SBINDIR/esets_update
```

Для забезпечення найвищого захисту клієнтів, команда ESET постійно збирає екземпляри нових загроз по всьому світу – зразки нових вірусів можуть з'явитись у базі даних вірусних сигнатур за дуже малий проміжок часу. Саме тому рекомендується виконувати оновлення регулярно. Для визначення частоти оновлення, потрібно настроїти опцію 'av\_update\_period' секції [global] у файлі конфігурації ESETS. Для успішного оновлення бази даних вірусних сигнатур, процес ESETS повинен бути у робочому стані.

## 7.2. Опис процесу оновлення ESETS

---

Процес оновлення складається з двох кроків: перший, попередньо скопійовані модулі оновлення завантажуються з сервера ESET. Якщо у секції [global] файлу конфігурації ESETS задана опція 'av\_mirror\_enabled', копії модулів оновлення створюються у наступній директорії (директорії "Дзеркала"):

```
@BASEDIR/mirror
```

При потребі, шлях папки "Дзеркала" можна змінити за допомогою опції 'av\_mirror\_dir' секції [update] у файлі конфігурації ESETS. Створене «Дзеркало» буде працювати як повнофункціональний сервер оновлення, який можна використовувати для створення нижчих (дочірніх) «Дзеркал». Однак, для цього необхідне виконання наступних умов: по-перше, на нижньому комп'ютері, звідки завантажуватимуться модулі, повинен бути інстальований HTTP сервер. По-друге, щоб модулі оновлення могли завантажити інші комп'ютери, вони повинні знаходитись у наступній директорії:

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

де 'http-serv-base-path' головна директорія сервера HTTP – спочатку утиліта оновлення шукатиме модулі саме тут.

Другий крок процесу оновлення – компіляція модулів, які завантажують сканер ESET Mail Security із тих, що зберігаються у «Дзеркалі». Зазвичай створюються наступні модулі ESETS: модуль загрузки (em000.dat), модуль сканування (em001.dat), модуль бази даних вірусних сигнатур (em002.dat), модуль обробки архівів (em003.dat), модуль розширеної евристики (em004.dat) тощо. Модулі створюються

у наступній директорії:

@BASEDIR@

Зверніть увагу, що це директорія, з якої процес ESETS завантажує модулі. Її можна змінити у параметрі 'base\_dir' секції [global] файлу конфігурації ESETS.

Розділ 8:

# Оповіщення

Шановний користувач, ми сподіваємося, що даний посібник забезпечив вичерпне розуміння системних вимог для інсталяції, настройки та управління ESET Mail Security. Однак, нашою ціллю є постійне покращення якості та ефективності документації продуктів. Тому, якщо Ви вважаєте, що якийсь розділ даного посібника незрозумілий або не повний, будь-ласка сповістіть наш центр технічної підтримки клієнтів:

<http://www.eset.com.ua/support> (або пишіть на [support@ eset.com.ua](mailto:support@ eset.com.ua))

Ми надамо Вам найвищий рівень підтримки та допоможемо, якщо у Вас виникнуть якісь проблеми стосовно даного продукту.

## **Доповнення А. Опис процесу настройки ESETS**

## A.1. Налаштування ESETS для MTA-агента Postfix

### A.1.1. Сканування вхідних е-mail повідомлень

**ЗВЕРНІТЬ УВАГУ:** Дана інсталяція не сумісна з SELinux. Будь-ласка, або виключіть SELinux, або перейдіть до наступного підрозділу.

Ціль поточної інсталяції: вставити **esets\_mda** перед MDA-агентом Postfix. Використаний MDA-агент (з параметрами) задається в параметрі Postfix 'mailbox\_command'.

**ЗВЕРНІТЬ УВАГУ:** Якщо значення не задане, Postfix доставлятиме пошту власноруч. Потрібно інсталювати та настроїти MDA (наприклад procmail) та перш за все використати його в 'mailbox\_command' з параметрами (наприклад, /usr/bin/procmail -d "\$USER"). Перезавантажити Postfix та впевнитись, що повідомлення доставляються відповідно ваших потреб. Потім можна продовжити інсталяцію ESETS.

Задайте значення параметра 'mda\_path' у секції [mda] файлу конфігурації ESETS відповідне абсолютному шляху MDA-агента Postfix, у нашому прикладі:

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

та перезапустіть процес ESETS. Потім замініть шлях до MDA-агента Postfix шляхом модуля **esets\_mda** і додайте до аргументів -- --recipient="\$RECIPIENT" --sender="\$SENDER", у нашому випадку:

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

Щоб задіяти нову конфігурацію перезавантажте Postfix.

### A.1.2. Двонаправлене сканування е-mail повідомлень

Задача даної інсталяції доставити всі повідомлення від Postfix до **esets\_smtp** і отримати їх назад. У секції [smtp] файлу конфігурації ESETS задайте наступні параметри:

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

та перезавантажте процес ESETS, що запустить **esets\_smtp** і скануватиме всі дані, отримані по SMTP протоколу і прийняті по порту 'listen\_addr:listen\_port' і переправлятиме по порту 'server\_addr:server\_port'. Щоб доставляти всю пошту esets\_smtp настройте в Postfix наступне:

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

**ЗВЕРНИТЬ УВАГУ:** Якщо параметр 'content\_filter' вже має задане значення, не виконуйте наведені інструкції. Замість цього внесіть **esets\_smtп** (або інший ESETS модуль сканування пошти) перед або після 'content\_filter'.

Останнє, що потрібно зробити – настроїти прийом повідомлень та їх обробку в Postfix по порту 2525. Додайте наступне в файл Postfix master.cf:

```
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
```

замініть yourdomain.com ім'ям Вашого хоста (після першої точки). Перевірте наявність відступів у всіх строчках, окрім першої. Для активації нових налаштувань перезапустіть Postfix.

**ЗВЕРНИТЬ УВАГУ:** Якщо у Вас включено SELinux, який блокує прослуховування порту 2525 в Postfix (наприклад, Fedora Core >= 5), запустіть наступну команду: semanage -a -t smtp\_port\_t -p tcp 2525

## A.2. Налаштування ESETS для MTA-агента Sendmail

### A.1.1. Сканування вхідних е-mail повідомлень

**ЗВЕРНИТЬ УВАГУ:** Дана інсталяція не сумісна з SELinux. Будь-ласка, виключіть SELinux, або перейдіть до наступного підрозділу.

Ціль поточної інсталяції – помістити **esets\_mda** перед MDA-агентом Sendmail.

**ЗВЕРНИТЬ УВАГУ:** В FreeBSD, Sendmail може з'єднуватись з MDA за допомогою LMTP. Однак, **esets\_mda** не сумісний з LMTP. Тому, якщо у файлі `hostname`.mc є строка FEATURE(local\_lmtp) її потрібно закоментувати і повторно створити файл sendmail.cf.

Поточний MDA-агент можна знайти у файлі sendmail.cf у секції Mlocal: у параметрах 'P' (виконуючий) та 'A' (його ім'я та аргумент).

Спочатку здайте параметр 'mda\_path' в секції [mda] файлу конфігурації ESETS зі значенням поточного виконуючого MDA-агента (параметр 'P' в Sendmail) та перезапустіть процес ESETS.

Потім додайте у файл sendmail.mc (або `hostname`.mc в FreeBSD та Solaris) перед всіма визначеннями MAILER наступне:

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

де `original_arguments` - це параметр 'A' в Sendmail без ім'я (перше слово).

На кінець, заново створіть файл `sendmail.cf` та перезапустіть Sendmail.

## A.2.2. Двонаправлене сканування е-mail повідомлень

Задача даної інсталяції - сканування всіх повідомлень в Sendmail за допомогою фільтра **esets\_smfi**. У секції `[smtp]` файлу конфігурації ESETS задайте наступні параметри:

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

та переважанте процес ESETS. Потім додайте у файл `sendmail.mc` (або `'hostname'.mc` в FreeBSD та Solaris) перед всіма визначеннями MAILER наступне:

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

За допомогою даних настройок Sendmail буде зв'язуватись з **esets\_smfi** через unix сокети `/var/run/esets_smfi.sock`. Флаг `F=T` спричинить тимчасове роз'єднання зв'язку, якщо фільтр недоступний. Обмеження часу `S:2m` задає 2 хвилинне обмеження на посилання інформації з MTA-агента на фільтр, `R:2m` - 2 хвилинне обмеження на зчитування відповіді фільтра, а `E:5m` значить загальний 5 хвилинне обмеження на посилання останнього фрагменту е-mail повідомлення і очікування остаточного підтвердження.

Зверніть увагу, якщо обмеження часу для **esets\_smfi** фільтру задані занадто малими, Sendmail може тимчасово відкласти повідомлення в чергу і через деякий час повторити спробу передачі. Це може спричинити велику кількість відкладень одного й того ж повідомлення. Щоб вирішити проблему, потрібно задавати належні обмеження часу. Також можна настроїти параметр Sendmail `'confMAX_MESSAGE_SIZE'`, який задасть максимально допустимий розмір повідомлення у байтах. Враховуючи значення даного параметра та максимальний час для обробки об'єму даних MTA-агентом (дане значення можна поррахувати), можна визначити відповідне обмеження часу для фільтра **esets\_smfi**.

На кінець, заново створіть файл `sendmail.cf` та перезапустіть Sendmail.

## A.3. Настройка ESETS для MTA-агента Qmail

### A.3.1. Сканування вхідних е-mail повідомлень

Задача даної інсталяції – помістити **esets\_mda** перед локальним агентом Qmail. Припустимо, що Qmail інстальовано у директорії `/var/qmail directory`. В секції

[mda] файлу конфігурації ESETS задайте наступний параметр:

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

та перезапустіть процес ESETS. Створіть файл /var/qmail/bin/qmail-esets\_mda з наступним вмістом і використайте команду chmod a+x:

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

що дозволить модулю **esets\_mda** визвати локальний агент Qmail. Тепер створіть файл /var/qmail/bin/qmail-start.esets з наступним вмістом і виконайте команду chmod a+x:

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

що запустить Qmail, у якому **esets\_mda** використовуватиметься для доставки локальних повідомлень. Однак, в qmail-local через **esets\_mda** передається специфікація доставки. Зверніть увагу, що в даній конфігурації **esets\_mda** використовуватиме коди виходу Qmail (продивіться qmail-command(8)). На кінець, замініть qmail-start за допомогою команд:

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

та перезапустіть Qmail.

### А.3.2. Двонаправлене сканування e-mail повідомлень

Ціль даної інсталяції – помістити **esets\_mda** перед функцією qmail-queue, в якій всі повідомлення електронної пошти перед доставкою ставляться в чергу. Припустимо, що Qmail інстальовано в директорію /var/qmail. В секції [mda] файлу конфігурації ESETS задайте наступний параметр:

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

та перезапустіть процес ESETS. На кінець, замініть qmail-queue використовуючи команди:

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

Не потрібно перезапускати Qmail. Тепер всі повідомлення, поставлені в чергу, будуть скановані за допомогою ESETS. Зверніть увагу, що при такій конфігурації **esets\_mda** використовуватиме коди виходу qmail-queue (передивіться qmail-queue(8)).

## A.4. Налаштування ESETS для MTA-агента Exim (версії 3)

### A.4.1. Скандування вхідних e-mail повідомлень

Мета даної інсталяції створити Exim-передачу з **esets\_mda** для локальних користувачів. У секції [mda] файлу конфігурації ESETS налаштуйте наступне:

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

де /usr/sbin/exim - це повний шлях до бінарного файлу Exim. Потім перезапустіть процес ESETS. Після цього додайте наступний запис передачі у список (в будь-яке місце) Exim-передач:

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

де mail – це один з Exim 'trusted\_users' («довірих користувачів»). Потім додайте наведений запис пристрою на першу позицію списку пристроїв Exim:

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

що перешле всі неперевірені повідомлення локальних користувачів до **esets\_mda**, який у свою чергу переправлятиме їх до Exim для подальшої обробки. Для активації нової конфігурації перезавантажте Exim.

### A.4.2. Двонаправлене скандування e-mail повідомлень

Ціль даної інсталяції - створити Exim-передачу від **esets\_mda** для всіх повідомлень. Виконайте всі процедури попереднього підрозділу, а також додайте наступний маршрутизатор на першу позицію маршрутизаторів Exim:

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

## A.5. Налаштування ESETS для MTA-агента Exim (версії 4)

### A.5.1. Скандування вхідних e-mail повідомлень

Мета даної інсталяції створити Exim-передачу з **esets\_mda** для локальних

користувачів. У секції [mda] файлу конфігурації ESETS настройте наступне:

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

де /usr/sbin/exim - це повний шлях до бінарного файлу Exim. Потім перезапустіть процес ESETS. Додайте наступний запис маршрутизатора у список маршрутизаторів Exim:

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

після цього додайте наступний запис передачі у список (в будь-яке місце) Exim-передач:

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

що перешле всі неперевірені повідомлення локальних користувачів до **esets\_mda**, який у свою чергу переправлятиме їх до Exim для подальшої обробки. Для активації нової конфігурації перезавантажте Exim.

## А.5.2. Двонаправлене сканування е-mail повідомлень

Ціль даної інсталяції - створити Exim-передачу від **esets\_mda** для всіх повідомлень. Виконайте всі процедури попереднього підрозділу, але пропустіть наступну строчку у esets\_router:

```
domains = +local_domains
```

## А.6. Налаштування ESETS для MTA-агента ZMailer

---

### А.6.1. Сканування вхідних е-mail повідомлень

Ціль даної інсталяції - використати **esets\_mda** у якості локального агента доставки ZMailer. Однак, необхідно мати інший інстальований MDA, наприклад, procmail. У секції [mda] файлу конфігурації ESETS настройте наступний параметр:

```
mda_path = "/path/to/procmail"
```

та перезапустіть процес ESETS. Procmail не підтримує повні е-mail адреси, тому закоментуйте наступну строчку в ZMailer router.cf за допомогою '#':

```
localdoesdomain=1
```

Потім в операторі 'local/' файлу scheduler.conf замініть поточну команду доставки на наступну:

```
command="sm -c $channel esets"
```

та додайте строку в sm.conf (замініть your.hostname.com на FQDN):

```
esets sSPfn @BINDIR@/esets_mda esets_mda -a $h -d $u  
-- --sender $g --recipient $u@your.hostname.com
```

Вкінці перезапустіть ZMailer.

## A.6.2. Двонаправлене сканування e-mail повідомлень

Мета даної інсталяції - використання **esets\_zmfi** у ролі smtp фільтра вмісту в ZMailer. Спочатку перезапустіть процес ESETS. Потім додайте наступну строку в smtpserver.conf:

```
PARAM contentfilter @BINDIR@/esets_zmfi
```

та перезапустіть ZMailer.

Зверніть увагу, що при даних настройка скануватиметься лише пошта, отримана через smtp сервер. Впевніться, що політика smtp фільтрує всю пошту, яку Вам необхідно.

## A.7. Налаштування ESETS для сканування вихідних повідомлень електронної пошти

Сканування вихідні e-mail повідомлень виконується за допомогою процесу **esets\_smtp**. У секції [smtp] файлу конфігурації ESETS настройте наступні параметри:

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

де 'listen\_addr' – це адреса інтерфейсу локальної мережі з ім'ям ifo. Після цього перезапустіть процес ESETS. Наступним кроком є перенаправлення всіх SMTP запитів на esets\_smtp. Якщо IP-фільтрація забезпечується інструментом адміністрування ipchains, необхідно використовувати наступне правило:

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

Якщо IP-фільтрація забезпечується інструментом адміністрування iptables, необхідно використовувати наступне правило:

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

В FreeBSD необхідно використовувати наступне правило:

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

В NetBSD та Solaris необхідно використовувати наступне правило:

```
echo 'rdr if0 0.0.0.0/0 port 25 -> 192.168.1.10 \  
port 2525 tcp' | ipnat -f -
```

**ЗВЕРНІТЬ УВАГУ:** Ваш МТА-агент може дозволяти всі з'єднання без їх ретельної перевірки за допомогою **esets\_smtp**, оскільки вони локальні. Використовуючи власну політику брандмауера, перевірте, щоб не було відкрито ззовні доступ open relay, тобто не дозволити комусь ззовні підключитись до **esets\_smtp** і використовувати його як SMTP-relay сервер.

## A.8. Налаштування ESETS для сканування зв'язку по POP3

Сканування зв'язку по POP3 виконується за допомогою процесу **esets\_pop3**. В секції [pop3] файлу конфігурації ESETS настройте наступні параметри:

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

де 'listen\_addr' – це адреса інтерфейсу локальної мережі з ім'ям if0. Потім перезапустіть процес ESETS. Наступним кроком є переадресація всіх POP3 запитів до **esets\_pop3**. Якщо IP-фільтрація забезпечується інструментом адміністрування ipchains, необхідно використовувати наступне правило:

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

Якщо IP-фільтрація забезпечується інструментом адміністрування iptables, необхідно використовувати наступне правило:

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

В FreeBSD необхідно використовувати наступне правило:

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

В NetBSD та Solaris необхідно використовувати наступне правило:

```
echo 'rdr if0 0.0.0.0/0 port 110 -> 192.168.1.10 \  
port 8110 tcp' | ipnat -f -
```

## A.9. Налаштування ESETS для сканування зв'язку по IMAP

Сканування з'єднання по IMAP виконується за допомогою процесу `esets_imap`. В секції `[imap]` файлу конфігурації ESETS налаштуйте наступні параметри:

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

да `'listen_addr'` – це адреса інтерфейсу локальної мережі з ім'ям `ifo`. Потім перезапустіть процес ESETS. Наступним кроком є пере направлення всіх IMAP запитів до `esets_imap`. Якщо IP-фільтрація забезпечується інструментом адміністрування `ipchains`, необхідно використовувати наступне правило:

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

Якщо IP-фільтрація забезпечується інструментом адміністрування `iptables`, необхідно використовувати наступне правило:

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

В FreeBSD необхідно використовувати наступне правило:

```
ipfw add fwd 192.168.1.10,8143 tcp from any to any 143 via if0 in
```

В NetBSD та Solaris необхідно використовувати наступне правило:

```
echo 'rdr if0 0.0.0.0/0 port 143 -> 192.168.1.10 \
port 8143 tcp' | ipnat -f -
```

# **Доповнення В. Ліцензія РНР**

Ліцензія PHP, версія 3.01 Права (c) 1999 – 2006 PHP Group. Всі права захищено. Розповсюдження та використання оригіналу коду або бінарних файлів з або без модифікацій дозволено, якщо наступні умови виконані:

1. При розповсюдженні оригіналу коду повинні бути вказані: ліцензійні права, написані зверху, даний список умов та відмова від прав, знизу.
2. При розповсюдженні бінарних файлів, у документації або у інших матеріалах, які надаються разом з розповсюджуваним продуктом повинні міститись ліцензійні права, написані зверху, даний список умов та відмова від прав, знизу.
3. Ім'я «PHP» не повинно використовуватись для надпису на дистрибутиві або для реклами продукту, розробленого на основі даного продукту, без попереднього письмового дозволу. Для отримання дозволу пишіть на електронну пошту [group@php.net](mailto:group@php.net).
4. Продукти, розроблені на основі даного продукту не можуть називатись «PHP», а також не можуть використовувати у своїй назві ім'я «PHP» без попереднього письмового дозволу від [group@php.net](mailto:group@php.net). Ви можете зазначити, що Ваш продукт сумісний з PHP наступною стрічкою «Foo for PHP» замість «PHP Foo» або «phpfoo».
5. PHP Group час від часу може публікувати виправлені або нові версії ліцензійної угоди. Кожній ліцензії надаватиметься ідентифікаційний номер. Тільки-но код продукту опубліковано з указанням певної версії ліцензії, його можна використовувати і надалі відповідно до положень цієї версії або відповідно до положень будь-якої наступної версії ліцензії, опублікованої PHP Group. Ніхто, окрім PHP Group, не має прав змінювати положення ліцензії, відповідно до якої опубліковано продукт.
6. При розповсюдженні продукту у будь-якій формі, дистрибутив повинен мати наступну примітку: «This product includes PHP software, freely available from <http://www.php.net/software/>».

ЦЕЙ ПРОДУКТ НАДАНИЙ КОМАНДОЮ РОЗРОБНИКІВ PHP «AS IS», ЯКІ ВІДМОВЛЯЮТЬСЯ ВІД БУДЬ-ЯКИХ ЗАЗНАЧЕНИХ АБО ВИПЛИВАЮЧИХ ЯК НАСЛІДОК ГАРАНТІЙ, ВКЛЮЧАЮЧИ ГАРАНТІЇ ПРИДАТНОСТІ ДЛЯ ПРОДАЖІ ТА ПРИДАТНОСТІ ДЛЯ СПЕЦИФІЧНИХ ЦІЛЕЙ. КОМАНДА РОЗРОБНИКІВ PHP ТА ЇХ СПОНСОРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНІСТЬ ЗА БУДЬ-ЯКИЙ СПРИЧИНЕНИЙ ПРЯМИЙ, НЕПРЯМИЙ, ВИПАДКОВИЙ, НАВМИСНИЙ ЗБИТОК, А ТАКОЖ ЗБИТОК, СПРИЧИНЕНИЙ ЯК НАСЛІДОК (ВКЛЮЧАЮЧИ ПРИДБАННЯ ЗАМІНЕНИХ ТОВАРІВ АБО ПОСЛУГ; ВТРАТА ПРАЦЕЗДАТНОСТІ, ДАННИХ АБО КОРИСНОСТІ ПРОДУКТУ; ПРИПИНЕННЯ ВЕДЕННЯ БІЗНЕСУ), А ТАКОЖ НЕ ЗОБОВ'ЯЗУЄТЬСЯ НА ГРОМАДСЬКІ, ПРЯМІ ТА ЗАЗНАЧЕНІ У КОНТРАКТІ ОБОВ'ЯЗКИ (ВКЛЮЧАЮЧИ НЕДБАЛІСТЬ ТА ІНШЕ), ЩО У БУДЬ-ЯКІЙ ФОРМІ ВИПЛИВАЮТЬ З КОРИСТУВАННЯ ДАНИМ ПРОГРАМНИМ ПРОДУКТОМ, НАВІТЬ ПРИ ОГОВОРЕННІ МОЖЛИВОСТІ ПОДІБНОГО ЗБИТКУ.