



we protect your digital worlds

ESET Gateway Security

Посібник користувача

Зміст

1. Введення.....	3
2. Терміни та аббревіатури.....	5
3. Інсталяція.....	9
4. Огляд внутрішньої будови.....	11
5. Інтеграція із слжбами Інтернет шлюзів.....	14
5.1. Конфігурація прозорого HTTP/FTP проксі.....	15
5.2. Налаштування HTTP/FTP проксі вручну.....	16
5.2.1. Налаштування проксі для Mozilla Firefox вручну.....	16
5.2.2. Налаштування проксі для Squid Web Proxy Cache вручну.....	17
5.3. Обробка великих HTTP-об'єктів.....	18
5.3.1. Спосіб відкладеного сканування.....	18
5.3.2. Спосіб часткового сканування.....	19
5.4. Інтегрований фільтр ESETS для SafeSquid Proxy Cache.....	19
5.4.1. Принцип роботи.....	19
5.4.2. Інсталяція та налаштування.....	19
6. Важливі механізми ESET Gateway Security.....	23
6.1. Політика обробки об'єктів (Handle Object Policy).....	24
6.2. Налаштування користувача (User Specific Configuration).....	24
6.3. «Білі» та «Чорні» списки.....	25
6.4. Система обробки зразків (Samples Submission System).....	26
6.5. Веб-Інтерфейс.....	27
6.6. Віддалена налаштування.....	27
7. Оновлення системи ESET Security.....	29
7.1. Утиліта оновлення ESETS.....	30
7.2. Опис процесу оновлення ESETS.....	30
8. Оповіщення.....	32
Доповнення А. Опис процесу налаштування ESETS.....	34
Доповнення В. Ліцензія PHP.....	38

Copyright © 2007 ESET, spol. s r. o.

ESET Gateway Security розроблено ESET, spol. s r. o. За більш детальною інформацією звертайтеся до www.eset.com.ua

Всі права захищено. Жодна з частин цього документа не може бути скопійована, збережена або представлена у будь-якій системі зберігання даних або передана у будь-якій формі, будь-якими засобами (електронними, фотокопіювальними, записуючими, 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. Продукт включає ПЗ від PHP, безкоштовно доступне на <http://www.php.net/software/>.

Розділ 1:

Введення

Шановний користувач, Ви придбали ESET Gateway 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 Gateway 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 Administration, для віддаленого керування продуктом у великих мережах.
- Інсталяція ESET Gateway 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 Gateway 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, які містять, наприклад, бази даних вірусних сигнатур. Надалі у документі використовуватиметься абревіатура **@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 Gateway Security. Надалі у документі використовуватиметься абревіатура **@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 Gateway Security. Абсолютний шлях файлу наступний:

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

Папка бінарних файлів ESETS

Папка, де зберігаються необхідні бінарні файли ESET Gateway 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 ESET Gateway Security. 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 Gateway 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 'sol10.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
```

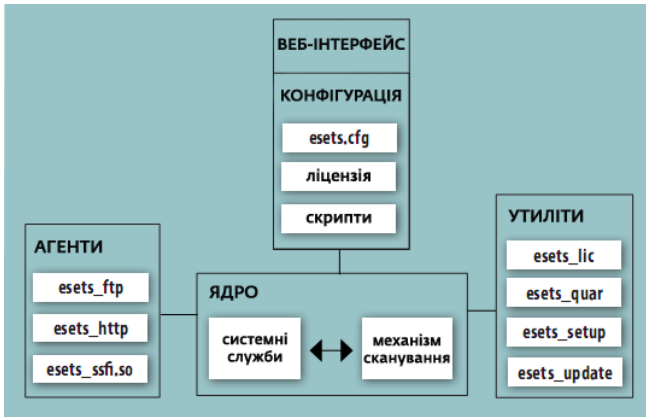
де щонайменше два процеси ESETS запущені у фоновому режимі. Перший PID представляє собою диспетчер контролю процесів та потоків системи. Другий PID є процесом сканування ESETS.

Розділ 4:

Огляд внутрішньої будови

Як тільки ESET Gateway Security успішно інстальований, вам потрібно ознайомитись з його конфігурацією.

Рисунок 4-1. Структура ESET Gateway Security.



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

CORE (Ядро)

Ядром ESET Gateway 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 ефективно 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 написано нижче у цьому розділі, присвячене більш

детальному опису компонентів конфігурації. Також рекомендується перечитати інформацію стосовно esets.cfg (5) на сторінках довідника, оскільки він 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 усі 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 усіх модулів та агентів ESET Gateway Security. Останні використовуються для перехоплення різних типів даних та підготовки їх до сканування. Зверніть увагу, що у прикладі 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 (man 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 (man 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.

Розділ 5:

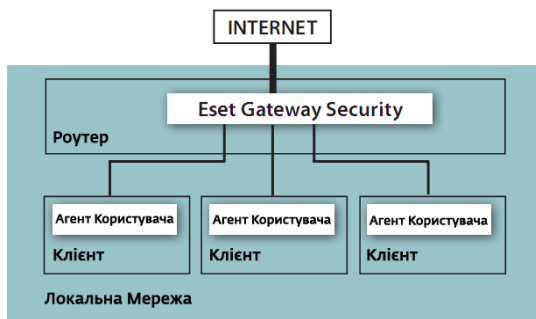
Інтеграція із слжбами Інтернет шлюзів

ESET Gateway Security захищає HTTP та FTP служби організації від вірусів, черв'яків, троянських та шпигунських програм, фішингу та інших загроз Інтернет на рівні серверів інтернет-шлюзу. Зверніть увагу, що під серверами інтернет-шлюзів мається на увазі шлюзи третього рівня моделі ISO/OSI, тобто маршрутизатори. У даній главі буде описана інтеграція продукту з вищезазначеними службами.

5.1. Конфігурація прозорого HTTP/FTP проксі

Конфігурація прозорого проксі основана на стандартному механізмі маршрутизації, який зображено на рисунку нижче.

Рисунок 5-1. Схема ESET Gateway Security у ролі прозорого проксі.



Конфігурація створюється звичайним чином, оскільки таблиці IP-маршрутизації ядра визначені для кожного клієнта локальної мережі. Подібні таблиці використовуються для настройки статичних маршрутів до локального шлюзового сервера, визначеного за замовченням (маршрутизатора). Зверніть увагу, що у DHCP мережі зазначена конфігурація задається автоматично. За допомогою даного механізму всі HTTP (відповідно, FTP) зв'язки з зовнішніми серверами виконуються через шлюзовий сервер локальної мережі, де потрібно встановити ESET Gateway Security для сканування з'єднань на інфільтрації. Для цієї цілі було розроблено загальний ESETS HTTP (відповідно, FTP) фільтр - **esets_http** (відповідно, **esets_ftp**).

Для того щоб настроїти ESET Gateway Security на сканування HTTP (відповідно, FTP) повідомлень, які проходять через локальний шлюзовий сервер, введіть команду:

```
esets_setup
```

Виконуйте інструкції, які наведені у скрипті. Як тільки з'явиться пропозиція 'Available installations/un-installations', виберіть опцію 'HTTP' (відповідно 'FTP'), яка виведе опції 'install/uninstall' потрібного модуля. Виберіть 'install', що автоматично настроїть модуль на прослуховування попередньо заданого порту та перенаправлення IP-пакетів, що надходять від заданої мережі з цільовим HTTP (відповідно, FTP) портом, на той, який прослуховує **esets_http** (відповідно, **esets_ftp**). Це значить, що скануватись будуть тільки ті запити, які спочатку були направлені на цільовий HTTP (відповідно, FTP) порт. Якщо необхідно охопити й інші

порти, тоді потрібно задати відповідні правила перенаправлення.

Зверніть увагу, що за замовчуванням інсталятор відображає усі дії, які він збирається виконати і забезпечує резервне копіювання конфігурації, яку потім можна відновити. Більш детально процес інсталяції описано у Додатку А.

5.2. Налаштування HTTP/FTP проксі вручну

На відміну від автоматичної настройки, вручну (рисунок 5-2) можна точно задати адресу вищого проксі та порта у параметрах проксі-агента користувача.

Рисунок 5-2. Схема ESET Gateway Security у ролі проксі, настроєного вручну



У цьому випадку проксі-сервер модифікує передані запити та/або відповіді, тобто працюватиме у не прозорому режимі. Підтримка проксі **esets_http** вручну тестувалась на великій кількості найпоширеніших агентів користувачів, тобто на проксі кеші (Squid Proxy Cache, SafeSquid), клієнтських браузерях (Mozilla Firefox, Opera, Netscape, Konqueror). Загалом, будь-який HTTP агент користувача, який підтримує настройку вищого проксі вручну, буде оперувати з модулем **esets_http**. Далі буде описана настройка параметрів **esets_http** за допомогою Mozilla Firefox та Squid Web Proxy Cache, які є найбільш поширеними HTTP програмами-агентами клієнтів.

5.2.1. Налаштування проксі для Mozilla Firefox вручну

У загальному вигляді настройка HTTP/FTP проксі **esets_http** для Mozilla Firefox вручну зображена на лівій частині рисунка 5-2.

Зверніть увагу, що за допомогою даної конфігурації можна інсталиувати ESET Gateway Security будь-де у межах локальної мережі, включаючи шлюзовий сервер та комп'ютер користувача з агентом.

У наведеному прикладі **esets_http** настроюється для прослуховування порту 8080 комп'ютера з локальною IP адресою 192.168.1.10. Для цього задаються наступні

параметри у секції [http] файлу конфігурації ESETS:

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

Зверніть увагу, що параметр 'listen_addr' можна задати також як ім'я хоста, доступне через локальну мережу.

Для того, щоб настроїти використання **esets_http** у Mozilla потрібно вибрати 'Edit' («Правка») у панелі меню, а потім 'Preferences' («Настройки») - у старих версіях Mozilla потрібно вибрати «Інструменти» а потім «Настройки». Потім зайдіть у підрозділ 'Connection settings' («Настройки з'єднання») у розділі 'General' («Загальне»), а там виберіть 'Manual Proxy Configuration' («Настройка проксі вручну»). І на кінець, потрібно задати значення 'HTTP Proxy' (відповідно, 'FTP Proxy'), ім'я хоста (відповідно, IP адресу) та необхідний 'Port' («Порт»), який прослуховує esets_http (у нашому прикладі будуть задані IP адреса '192.168.1.10' та порт 8080). Для активації нових настройок перезапустіть процес ESETS.

Варто зауважити, що подібна конфігурація не є оптимальною для мереж з великою кількістю підключених комп'ютерів. Причина у тому, що HTTP кеш (якщо він є) наявний лише у агенті клієнта, тому один і той же об'єкт сканується заново при запиті від іншого агента.

5.2.2. Настройка проксі для Squid Web Proxy Cache вручну

У загальному вигляді настройка HTTP проксі **esets_http** для Squid Web Proxy Cache вручну зображена на правій частині рисунка 5-2.

На відміну від попередньо описаної конфігурації, у даному випадку ESET Gateway Security встановлюється в HTTP/FTP шлюзі між кешовим проксі-сервером (у даному випадку це Squid Web Proxy) та Інтернет. Таким чином всі вхідні HTTP/FTP відповіді спочатку скануються на інфільтрації, а потім зберігаються у виділеному кеші мережі, тобто усі об'єкти, будь-коли запрошені, наявні у проксі кеші вже скановано, і при повторному запиті ніяких додаткових перевірок не потрібно.

У наведеному прикладі **esets_http** настроюється для прослуховування порту 8080 комп'ютера з локальною IP адресою 192.168.1.10. Для цього задаються наступні параметри у секції [http] файлу конфігурації ESETS:

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

Зверніть увагу, що параметр 'listen_addr' можна задати як ім'я хоста, доступне через локальну мережу або використовуючи адресу 0.0.0.0, що дозволить **esets_http** прослуховувати всі інтерфейси. У останньому випадку варто бути обережним, оскільки використовувати HTTP/FTP сканер зможуть також користувачі, за межами локальної мережі. Щоб заборонити цей доступ, потрібно прийняти додаткові міри.

Щоб настроїти Squid для використання **esets_http** як вищий проксі, потрібно додати наступні строчки в файл конфігурації Squid (/etc/squid/squid.conf):

```
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 попередньому прикладі Squid було настроєно на прослуховування HTTP проксі з IP адресою 192.168.1.10 по порту 8080 у якості вищого проксі. Таким чином в його розпорядження будуть переправлятися усі запити, які оброблятиме Squid. Інші строки задають режим роботи Squid так, щоб повідомити про помилку, якщо проксі недоступний. Є альтернативний спосіб настроїти Squid, щоб перенаправити з'єднання, коли вищий проксі недоступний. У цьому випадку потрібно додати наступні параметри у файл конфігурації Squid:

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

Щоб задіяти нову конфігурацію, перезапустіть процес ESETS.

5.3. Обробка великих HTTP-об'єктів

За нормальних умов **esets_http** обробляє кожний переданий об'єкт наступним чином: по-перше, об'єкт передається з HTTP сервера (клієнта) до **esets_http**, по-друге, виконується його сканування на наявність інфільтрацій, і наприкінці, він передається HTTP клієнту (серверу). Що стосується великих об'єктів (об'єктів, час передачі яких більший ніж час, заданий параметром «`!o_timeout`»), то така схема не підходяща, оскільки вичерпання часу очікування агента або нетерпіння користувача може спричинити перешкоди і навіть відміну передачі об'єкта. Саме тому потрібно використовувати інші способи обробки великих об'єктів.

5.3.1. Спосіб відкладеного сканування

esets_http використовує стандартне так зване «відкладене сканування» для обробки великих файлів. Це значить, що якщо розмір об'єкта перевищує задані рамки, то **esets_http** починає прозору передачу об'єкта на цільовий HTTP (тобто клієнту або на сервер). Після того, як об'єкта цілком передано до **esets_http**, виконується сканування на загрози. Якщо об'єкт буде ідентифіковано як вірус, то остання його частина (поточна версія ESET Gateway Security визначає останню частину, як 4Кб даних об'єкта) не передається і виконується роз'єднання з цільовий HTTP. Також адміністратору шлюзу електронною поштою відсилається відповідне повідомлення про передачу небезпечного файлу. Зверніть увагу, що повідомлення відправляється тільки у випадку передачі даних клієнту з сервера. При цьому URL відповідного об'єкта зберігається в кеші **esets_http**, щоб заблокувати повторну передачу об'єкта.

Варто зазначити, що при використанні способу «відкладеного сканування» виникає потенціальна небезпека загрози комп'ютеру, чий агент завантажує інфікований файл вперше. Не зважаючи на те, що данні файлу діляться на декілька частин, ризик визиває передана частина файлу, яка може містити шкідливий

виконуваний код. Саме тому компанія ESET розробила удосконалений метод, так званий спосіб «часткового сканування».

5.3.2. Спосіб часткового сканування

Спосіб «часткового сканування» був розроблений спеціально для забезпечення безпеки способу «відкладеного сканування». Принцип функціонування способу «часткового сканування» оснований на тому, що час сканування об'єкта в порівнянні з часом його обробки незначний. Зверніть увагу, що ця ідея справедлива лише для HTTP передачі великих об'єктів. Це твердження дозволяє виконати більш ніж одне сканування під час передачі великого об'єкта.

Якщо включити параметр «`!o_partscan_enabled`» у секції `[http]` файлу конфігурації ESETS, то під час передачі з заданим інтервалом великі об'єкти скануватимуться на наявність загроз, а перевірені данні відправлятимуться на цільову точку (тобто клієнту або на сервер). При використанні такого способу інфіковані данні не передаватимуться на комп'ютер агента клієнта, що запросив об'єкт, адже до передачі усі данні перевіряються.

Під час тестування було виявлено, що при звичайних умовах роботи (мається на увазі, коли швидкість передачі через шлюз по локальній мережі значно більша від швидкості передачі через шлюз по Інтернет) швидкість передачі великих об'єктів за допомогою способу «часткового сканування» приблизно така ж, як і при використанні способу «відкладеного сканування».

5.4. Інтегрований фільтр ESETS для SafeSquid Proxy Cache

У попередньому підрозділі було розглянуто ESET Gateway Security з шлюзовими HTTP та FTP Інтернет службами за допомогою `esets_http` та `esets_ftp`. Описані способи можна застосовувати для більшості популярних агентів, включаючи відомий Інтернет проксі фільтрації контенту - SafeSquid (<http://www.safesquid.com>). У цьому випадку ESET Gateway Security пропонує альтернативний шлях захистити шлюзові послуги - за допомогою спеціально розробленого модуля `esets_ssfi.so`.

5.4.1. Принцип роботи

Модуль `esets_ssfi.so` розроблений з ціллю отримати доступ до всіх об'єктів, які обробляє кешовий проксі SafeSquid за допомогою інтерфейсу, розробленого SafeSquid. Як тільки модуль отримав доступ – об'єкт сканується на наявність інфільтрації за допомогою процесу ESETS. При виявленні загрози, SafeSquid блокує відповідний ресурс та замість нього надсилає визначену шаблонну сторінку. Зверніть увагу, що `esets_ssfi.so` підтримує SafeSquid Advanced версії 4.0.4.2 та новіші.

5.4.2. Інсталяція та настройка

Для інтеграції модуля необхідно задати посилання з папки модулів SafeSquid на відповідні пакети інсталяції ESET Gateway Security. У наступному прикладі SafeSquid інстальовано на ОС Linux у директорию `/opt/safesquid/`.

Якщо використовується SafeSquid версії 4.2 або новішої, введіть наступні команди:

```
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
```

Якщо використовується SafeSquid старіший за 4.2, введіть наступні команди:

```
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
```

Щоб завершити інсталяцію модуля у SafeSquid, зайдіть у веб-інтерфейс адміністратора SafeSquid, виберіть меню 'Config' ("Конфігурація") головної сторінки інтерфейсу і у полі 'Select a Section to Configure' ("Вибрати розділ для настройки") за допомогою прокрутки знайдіть розділ 'ESET Gateway Security'. Потім створіть профіль 'antivirus' для розділу 'ESET Gateway Security' натиснувши кнопку 'Add' ("Додати") знизу. У списку, який з'явився, визначте наступні параметри:

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

Після інсталяції, модуль SafeSquid готовий до роботи. Але у конфігурацію SafeSquid необхідно внести деякі параметри. Далі показана настройка SafeSquid для використання шаблонів блокування ESETS, якщо об'єкт інфікований (або не перевірений).

Зайдіть у веб-інтерфейс адміністратора SafeSquid, виберіть меню 'Config' ("Конфігурація") головної сторінки інтерфейсу і у полі 'Select a Section to Configure' ("Вибрати розділ для настройки") за допомогою прокрутки знайдіть розділ 'ESET Gateway Security'. Потім настройте профіль 'antivirus' натиснувши на кнопку 'Edit' ("Настроїти") знизу. У списку, який з'явився, визначте наступні параметри:

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

Після збереження списку шаблонів перейдіть на сторінку 'Templates' ("Шаблони") головного меню 'Config' ("Конфігурація"). Буде зображено параметр 'Path' ("Шлях"), який визначає шлях папки шаблонів SafeSquid (надалі ми припустимо, що параметр має значення '/opt/safesquid/templates'). Впевніться б що відповідна папка існує, у протилежному випадку створіть її. Щоб отримати доступ до шаблонів ESETS з даної директорії необхідно надати відповідні посилання використовуючи наступні команди оболонки:

```
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
```

Також необхідно додати нові шаблони у конфігурації SafeSquid. Для цього натисніть кнопку 'Add' ("Додати") у розділі 'Templates' ("Шаблони"). З'явиться список, у якому потрібно задати наступні параметри для сторінки блокування інфікованих об'єктів ESETS:

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

Відповідно, для сторінки блокування неперевічених об'єктів ESETS:

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

Для активації нової конфігурації перезавантажте SafeSquid та процес ESETS.



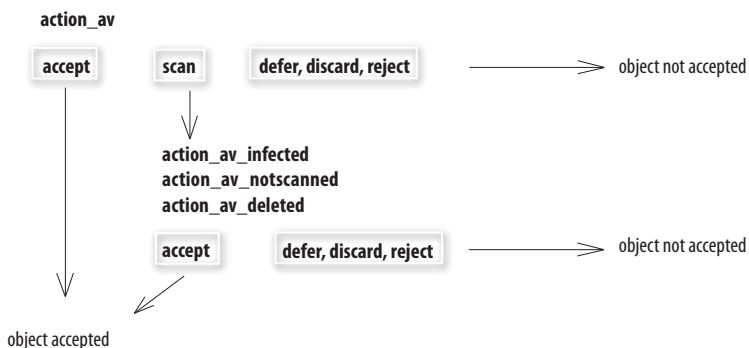
Розділ 6:

Важливі механізми ESET Gateway 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 ґрунтується 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 (man page) esets.cfg(5).

Рисунок 6-1. Схема механізмів 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 інфільтрацій, а якщо значення опції 'av_clean_mode' настроєне на 'yes', то при скануванні об'єкт очищається. У прикладі, 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.

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 (man 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 настроїти 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 **esets_http** для контролю трафіка по порту 8080 шляхом з локальною IP адресою 192.168.1.10. Налаштування модуля знаходяться у секції [http] файлу конфігурації ESETS і мають наступний вигляд:

```
[http]
agent_enabled = yes
listen_addr = "192.168.1.10"
listen_port = 8080
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_http_spec.cfg', який знаходиться у папці конфігурації ESETS.

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

Як тільки у секції [http] створено посилання на спеціальний файл конфігурації, потрібно створити файл у папці конфігурації ESETS та задати у ньому належні налаштування. Наступний приклад демонструє налаштування параметра 'action_on_processed' для IP адреси клієнта 192.168.1.40.

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

Зверніть увагу, що назва спеціальної секції містить ідентифікацію HTTP клієнта, для якого була створена конфігурація. У контексті секції містяться індивідуальні параметри, задані для даної ідентифікації. Таким чином HTTP трафік всіх клієнтів локальної мережі буде оброблено, у даному випадку скановано на загрози, окрім одного клієнта з IP адресою 192.168.1.40, який буде відкинуто, у даному випадку заблоковано у будь-якому випадку.

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 налаштування, 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. 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. УСЯ 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 увімкнувши опцію 'samples_enabled' секції [global] у файлі конфігурації ESETS. Щоб увімкнути 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 детально інформацію про Систему обробки зразків можна знайти на

сторінці esets_daemon(8) довідки (man pages).

6.5. 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).

6.6. 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 сторінка 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\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) до сервера 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 Gateway Security

7.1. Утиліта оновлення ESETS

Щоб забезпечити ефективність ESET Gateway Security, необхідно використовувати найостанніші оновлення бази даних вірусних сигнатур. Спеціально для цього була розроблена утиліта **esets_update** (Більш детальну інформацію про esets_update(8) Ви можете 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 'proxy_addr', 'proxy_port' і при потребі 'proxy_username' та 'proxy_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 скомпільовані 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 Gateway 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 Gateway 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)

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 сканування HTTP з'єднань - прозорий режим

Сканування HTTP з'єднань виконується за допомогою процесу **esets_http**. У секції [http] файлу конфігурації ESETS задайте наступні параметри:

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

де 'listen_addr' є адресою інтерфейсу локальної мережі з ім'ям ifo. Після цього перезапустіть процес ESETS. Наступним кроком є перенаправлення усіх HTTP запитів до **esets_http**. Якщо IP-фільтрація виконується за допомогою інструменту адміністрування ipchains, необхідно використовувати наступне правило:

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

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

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

FreeBSD:

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

NetBSD та Solaris:

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

A.2. Налаштування ESETS для сканування FTP з'єднань - прозорий режим

Сканування FTP зв'язку виконується за допомогою процесу **esets_ftp**. У секції [ftp] файлу конфігурації ESETS настройте наступні параметри:

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

де 'listen_addr' є адресою інтерфейсу локальної мережі з ім'ям ifo. Після цього перезапустіть процес ESETS. Наступним кроком є перенаправлення усіх FTP запитів до **esets_ftp**. Якщо IP-фільтрація забезпечується інструментом адміністрування ipchains, необхідно використовувати наступне правило:

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

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

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

FreeBSD:

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

NetBSD та Solaris:

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

Доповнення В. Ліцензія РНР

Ліцензія PHP, версія 3.01 Права (с) 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.
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. 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, ДАНИХ 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.