ГАРДА

Гарда Скаут

Руководство администратора

gardatech.ru

2023

Тип документа:	Руководство администратора
Дата выпуска:	16.10.2023
Статус документа:	Released
Версия:	5.10

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора к программному модулю «Скаут», входящий в состав программного обеспечения ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР».

1.2 Термины, определения и сокращения

Термин	Значение
ПК	ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР»
ПО	программное обеспечение, программа
Система	ПК «ПЕРИМЕТР»
Модуль	Модуль «Скаут»
СПД	Сеть передачи данных
DoS	Сетевая (компьютерная) атака, направленная на отказ в обслуживании
DDoS	DoS-атака, выполняемая одновременно с большого числа компьютеров

1.3 Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие

данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних

угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов. Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ.

Подробнее – на gardatech.ru

1.5 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании «Гарда Технологии»:

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: ddos.support@gardatech.ru

2 Назначение Системы

ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР» (далее ПК «ПЕРИМЕТР») представляет собой систему обнаружения и противодействия сетевым атакам типа «Отказ в обслуживании DoS/DDoS» (далее DDoS) и анализа трафика на сети передачи данных (далее СПД).

Решение данной задачи основано на:

- постоянном контроле состояния трафика СПД и его многостороннем анализе;
- обнаружении отклонений параметров трафика (аномалий);
- интеллектуальной фильтрации трафика с блокированием вредоносной составляющей и пропуском легитимной.

Модуль Скаут является средством мониторинга проходящего через него трафика, выявления аномалий и очистки трафика.

3 Требования к аппаратной платформе

Требования к аппаратной платформе для установки Модуля зависят от требуемой производительности, а также используемых типов сетевых интерфейсов.

Общими требованиями для всех вариантов использования являются:

- CPU с частотой не менее 2.1 GHz и поддержкой технологии SSE4.2;
- использование аппаратного RAID с дополнительным питанием кеш-памяти;
- жесткие диски не менее 2x960Gb SSD, организованные в RAID1;
- сдвоенный блок питания с возможностью горячей замены;
- сетевой интерфейс Gigabit Ethernet (интерфейс управления Модуля);
- BMC с возможностью удаленного подключения к консоли (IPMI, ILO и их аналоги).

Требования к процессору, оперативной памяти и сетевым интерфейсам зависят от требуемой производительности Модуля

Производительность	Процессор	Память	Сетевые адаптеры
1 x 1Gbps **2 x 1Gbps**	2 x 8-core	192 Gb	1 x Silicom PE2G4BPi35LA-SD Quad Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter Intel® i350AM4 Based
3 x 1Gbps **4 x 1Gbps**	2 x 12-core	256 Gb	2 x Silicom PE2G4BPi35LA-SD Quad Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter Intel® i350AM4 Based
1 x 10Gbps **single mode**	2 x 20-core	256 Gb	1 x Silicom PE310G4BPI9-LRD-SD 1000BASE-LX/10GBASE-LR Quad Port Fiber 10 Gigabit Ethernet Bypass Server Adapter Intel® 82599ES Based

Производительность	Процессор	Память	Сетевые адаптеры
1 x 10Gbps **multi mode**	2 x 20-core	256 Gb	1 x Silicom PE310G4BPi9-SRD-SD 4x1000Base-SX/10GBase-SR Bypass LC Intel 82599ES Based

Технические характеристики Модуля могут различаться на конкретных моделях серверов, и определяются после тестирования производительности в лаборатории.

4 Настройка аппаратной платформы

Для корректной работы Модуля необходимо настроить некоторые параметры UEFI/BIOS. Аппаратные платформы могут отличаться набором настраиваемых параметров и их обозначениями, поэтому ниже приведены общие названия параметров, которые необходимо настроить. В случае отсутствия указанных параметров, необходимо обратиться к документации на аппаратную платформу или к производителю аппаратной платформы.

- Server Availability

Auto Power-On:	Always Power On
Power-on Delay:	No delay

- BIOS/Platform Configuration

Workload Profile:	High Perfomance (HPC)

- Processor Options:

Hyper-Threading:	Disabled

- Virtualization Options:

Intel (R) Virtualization Technology (Intel VT):	Disabled
Intel (R) VT-d:	Disabled
SR-IOV:	Disabled
Virtual NUMA:	Disabled

Для Модуля важно, чтобы дисковая подсистема обеспечивала высокую производительность и надежность при выполнении операций ввода/вывода, поэтому требуется наличие аппаратного RAID.

Рекомендуемая конфигурация дискового массива – RAID1 или RAID10. Не рекомендуется использовать массивы в конфигурации RAID5 из-за значительного снижения производительности при выходе из строя физического диска.

Рекомендуется использовать один дисковый массив, в который включены все доступные физические диски. В этом случае для установки операционной системы

возможно использование подготовленного производителем Системы образа в формате ISO.

Примечание: *Подготовленный образ создает все необходимые для работы Модуля логические разделы на первом дисковом устройстве /dev/sda. В случае использования иной конфигурации дисковых массивов, необходимо выполнить установку операционной системы вручную.*

5 Установка ОС с использованием подготовленного образа

Для упрощения и ускорения установки операционной системы, производитель Модуля подготовил специализированный образ в формате ISO, содержащий необходимые настройки. Образ доступен для загрузки с облака производителя Системы.

Примечание: *Образ предназначен для развертывания на первое дисковое устройство /dev/sda. Если необходимо выполнить установку в иной конфигурации дисковой подсистемы, требуется установить операционную систему вручную.*

В случае, если в подготовленном образе отсутствуют драйверы для дискового контроллера, необходимо выполнить установку операционной системы в ручном режиме, с подключением дополнительного диска, содержащего драйверы дискового контроллера.

Для установки операционной системы из подготовленного образа, выполните следующие шаги:

- подключите образ в формате ISO к виртуальному CD-устройству в BMC сервера для возможности загрузки с образа, либо используйте иной способ, обеспечивающий возможность загрузки с подготовленного образа;
- загрузитесь с подготовленного образа;
- в меню загрузки выберите пункт Perimeter 4.19.0-23 и подтвердите выбор нажатием на клавиатуре кнопки Enter;
- дождитесь окончания процесса установки;
- отключите образ и выполните штатную загрузку аппаратной платформы с дискового устройства.

Внимание: *После установки операционной системы из образа, необходимо войти в консоль, используя имя пользователя* ***root*** *и пароль* ***garda****, после чего выполнить смену пароля суперпользователя.*

Изменение размеров логических разделов

В процессе установки из подготовленного образа создаются все необходимые логические разделы на базе Linux LVM, при этом они имеют минимальный размер. Перед установкой ПО Модуля необходимо увеличить размеры разделов следующим образом:

Логический том	Описание	Тестовая среда	Производственная среда
synta/root	корневая файловая система	20G	50G
synta/home	профили учетных записей	10G	20G
synta/dbdata	база данных	20G	400G
synta/dbbackup	резервные копии	20G	300G
synta/dumps	дампы трафика	10G	20G
synta/syn	подсистема очистки трафика	10G	100G
synta/clickhouse	информация о трафике	10G	500G

Для изменения размера необходимо войти в консоль суперпользователем и выполнить команду:

```
lvresize -r -L <размер раздела> <наименование логического тома>
```

Операционная система готова к установке ПО Модуля.

6 Установка ПО Модуля

Перед началом установки необходимо получить дистрибутивные комплекты ПО Модуля. Для получения ссылки на скачивание обратитесь к представителю компании производителя Системы.

Модуль поставляется в виде следующих архивных файлов:

ta-<MajorVersion>.<MinorVersion>-<details>-amd64.tar:	дистрибутив подсистемы анализа и управления;
tc-<MajorVersion>.<MinorVersion>-<details>-amd64.tar:	дистрибутив подсистемы фильтрации трафика.

Для работы Модуля операционная система должна иметь ядро linux-image-4.19.0-23-amd64-unsigned_4.19.269-1_amd64.deb.

Убедитесь, что операционная система установлена в соответствии с рекомендациями раздела Установка ОС с использованием подготовленного образа или Установка ОС в интерактивном режиме.

Все действия по установке Модуля выполняются в локальной консоли или удаленном терминале (ssh-подключение) от имени суперпользователя.

6.1 Распаковка дистрибутивного комплекта

Создайте директорию /opt/scout, введя команду:

```
mkdir -p /opt/scout
```

Поместите файлы дистрибутивного комплекта в созданный выше каталог путем копирования через локальную сеть по протоколам scp/sftp:

```
scp ta-*.tar.gz root@<IP-адрес интерфейса
управления>:/opt/scout
scp tc-*.tar.gz root@<IP-адрес интерфейса
управления>:/opt/scout
```

или подключив внешний накопитель к серверу с помощью команды cp.

Перейдите в директорию /opt/scout, введя команду:

```
cd /opt/scout
```

и распакуйте дистрибутивные комплекты:

```
tar zxf ta-*.tar.gz
tar zxf tc-*.tar.gz
```

Дистрибутивные комплекты будут распакованы в каталоги, соответствующие именам архивных файлов.

6.2 Установка подсистемы управления и анализа

Перейдите в директорию с распакованным дистрибутивным комплектом подсистемы управления и анализа (каталог, начинающийся на `ta-`).

Отредактируйте файл конфигурации config.yaml, приведя его к следующему виду:

```
ta:
  mailname: scout.local
  netflow_interface: lo
  is_1min_rep: false
```

Примечание: *Вместо почтового домена* `scout.local` *укажите почтовый домен, который планируется использовать или оставьте предлагаемое значение (его можно будет изменить в будущем).*

Запустите процесс установки, введя команду:

```
./install.sh ./config.yaml
```

Дождитесь завершения процесса установки.

Примечание: *Создание базы данных может занять длительное время, при этом изменений в консоли не будет. Индикатором этого состояния служит строка* `Creating database`.

6.3 Установка подсистемы фильтрации трафика

Перейдите в директорию с распакованным дистрибутивным комплектом подсистемы фильтрации трафика (каталог, начинающийся на `tc-`).

Определите идентификаторы PCI-устройств, которые будут использоваться как сетевые интерфейсы для прохождения трафика. Для этого выполните команду:

```
grep PCI_SLOT_NAME /sys/class/net/en*/device/uevent | \
sed "s#/sys/class/net/\(.*\)/device/uevent:PCI_SLOT_NAME=\(.*\)
#\1 --> \2#"
```

результатом выполнения которой будет соответствие имени сетевого интерфейса в операционной системе и идентификатора PCI-устройства.

Например, для сервера с тремя сетевыми интерфейсами, присутствующими в операционной системе, может использоваться следующая конфигурация:

ens192:	интерфейс управления;
ens224:	интерфейс, подключенный к вышестоящей сети;
ens256:	интерфейс, подключенный к защищаемой сети.

Определение идентификаторов PCI с помощью команды выше даст следующий результат:

```
ens192 --> 0000:0b:00.0
ens224 --> 0000:13:00.0
ens256 --> 0000:1b:00.0
```

Значения идентификаторов PCI-устройств для сетевых интерфейсов ens224 и ens256 потребуются при заполнении конфигурационного файла.

Отредактируйте файл конфигурации config.yaml, приведя его к следующему виду:

```
tc:
  input_interfaces: "0000:13:00.0"
  output_interfaces: "0000:1b:00.0"
  bypass_mode: bypass
  rx_params: "-r 3:1"
```

Примечание: *Значения названий сетевых интерфейсов и идентификаторов устройств приведены для примера и могут отличаться в реальных системах.*

Запустите процесс установки, введя команду:
`./install.sh ./config.yaml`

Дождитесь завершения процесса установки.

Запустите сервис конфигурирования подсистемы фильтрации, введя команду:

```
/etc/init.d/configure_syntc start
```

В результате конфигурирования загружаются драйверы uio и igb_uio, а также конфигурируются страницы памяти hugepages.

6.4 Настройка точного времени

Для корректной работы Модуля требуется синхронизация с сервером точного времени с использованием протокола NTP. Сервис ntp входит в дистрибутивный комплект и настроен на получение точного времени из сети Интернет. Если предполагается использовать альтернативный источник точного времени, то необходимо изменить конфигурационный файл /etc/ntp.conf:

1. закомментировать строки:

```
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst
```

2. добавить строки:

```
server <FQDN или IP альтернативного сервера>
```

После изменения конфигурационного файла, необходимо выполнить перезапуск сервиса ntp с помощью команды:

```
systemctl restart ntp
```

6.5 Запуск и остановка Модуля

Для запуска Модуля необходимо выполнить команды:

```
/etc/init.d/synta start
/etc/init.d/syntc start
```

В результирующем выводе не должно содержаться сообщений об ошибках.

Для остановки Модуля необходимо выполнить команды:

```
/etc/init.d/synta stop
/etc/init.d/syntc stop
```

Сетевые интерфейсы, указанные в конфигурационном файле, подключаются к загруженным драйверам и недоступны в операционной системе после старта подсистемы фильтрации. Контроль корректности подключения сетевых интерфейсов может быть выполнен с помощью команды:

```
/usr/bin/syn/igb_uio_bind.py --status-dev net | grep
"drv=igb_uio"
```

В выводе должны присутствовать PCI-устройства, которые были указаны при инсталляции в конфигурационном файле.

7 Активация лицензионного ключа

Модуль выполняет свои функции только при наличии корректного лицензионного ключа. Ключ распространяется в виде файла **license.key**, имеющего привязку к аппаратной платформе, на которой установлено ПО Модуля.

Запрос лицензионного ключа

Для получение лицензионного ключа необходимо выполнить следующие действия:

1. выполните команду в консоли от имени суперпользователя:

```
(date && uname -a && hostname && \
/usr/bin/syn/synlicprintsystemid) > request.lic
```

2. передайте файл запроса лицензии **request.lic** по согласованным каналам связи в компанию производителя Системы для создания лицензионного ключа;
3. получите по согласованным каналам связи лицензионный ключ **license.key**.

Установка лицензионного ключа

Для установки файла лицензии **license.key** необходимо:

1. остановить сервисы Модуля, используя методику раздела Настройка точного времени;
2. скопировать полученный файл **license.key** в каталог **/etc/syn/** в Модуле, например, используя протокол **scp**

```
scp license.key root@<IP-адрес интерфейса управления>:/etc/syn/
```

3. в консоли Модуля от имени суперпользователя выполнить команды:

```
chmod 440 /etc/syn/license.key
chown root:synconf-readers /etc/syn/license.key
```

4. запустить сервисы Модуля, используя методику раздела Настройка точного времени.

Примечание: *Проверка и активация лицензии может занять несколько минут, после чего Модуль перейдет в рабочий режим.*

8 Устранение неисправностей

8.1 Нет доступа к веб-интерфейсу

Симптомы

При попытке подключения к веб-интерфейсу через браузер, возникает сообщение Не удается получить доступ к сайту.

Возможные неисправности и пути их решения

1. Доступ с данного IP запрещен политикой ограничения доступа к порталу.

Подключитесь к веб-интерфейсу с IP адреса, который разрешен политикой ограничения доступа к порталу. Перейдите в меню Настройки › Доступ на вкладку Сетевые подключения › Ограничение доступа к порталу.

Разрешите доступ к порталу с нужного IP-префикса

2. Не запущен сервис synta.

Запустите сервис командой

```
/etc/init.d/synta start
```

3. Веб-сервер не запускается из-за ошибки.

Убедитесь, что веб-сервер запущен, используя команду

```
systemctl status nginx
```

Если сервер не запущен из-за возникающей ошибки, проанализируйте журнал веб-сервера, используя команду

```
journalctl -xe -u nginx
```

устраните проблему и запустите сервис командой

```
systemctl start nginx
```

8.2 Ошибка загрузки файла лицензии!

При попытке войти в веб-интерфейс, возникает сообщение об ошибке вида

```
Ошибка загрузки файла лицензии! Подробная информация об ошибке
записана в syslog
```

Отсутствует лицензия на использование Модуля. Выполните установку лицензионного ключа согласно разделу Активация лицензионного ключа

8.3 Не блокируется трафик, не детектируются атаки

Симптомы

1. Отсутствует трафик во всех отчетах в меню Отчеты и при снятии дампа информации о трафике, в то же время трафик виден в заданиях подавления и при снятии дампа "сырого" трафика.
2. Подсистема фильтрации не блокирует трафик, даже если создать правило для блокировки всего трафика.

Возможные неисправности и пути их решения

В Модуль загружена не действительная лицензия, вследствии чего подсистема фильтрации не включает режим блокировки трафика и не отправляет информацию о трафике в подсистему анализа и детектирования аномалий и подсистему аналитической отчетности по трафику. Для корректной работы всех подсистем необходима действующая лицензия.

Запросите и установите действующую лицензию, руководствуясь разделом Активация лицензионного ключа.

8.4 Подсистема очистки не запускается

8.4.1 FAILED 2014(115);Cleaner doesn’t respond in 115 secs

Симптомы

При запуске подсистемы фильтрации с помощью команды

```
/etc/init.d/syntc start
```

вместо сообщения SUCCESS появляется сообщение

```
Initializing please wait a moment… FAILED 2014(115);Cleaner
doesn’t respond in 115 secs
```

Диагностика

Выполните команду поиска ошибок в журнале подсистемы фильтрации трафика:

```
grep -P "ERROR|Unknown device" /var/log/syn/syn.log
```

Возможные неисправности и пути их решения

- В журнале присутствуют сообщения вида:

```
syn-dpdk: ERROR: not enough ethernet ports (0 instead of 2).
syn-dpdk: ERROR: MIMO channels assignment has failed.
syn-dpdk: ERROR: Driver (ports) initialization has failed.
syn-dpdk: ERROR: can not configure device: err = -22, port = 0
syn-dpdk: ERROR: devices configuration has failed.
```

1. Выбрано некорректное значение параметра rx_params при инсталляции.

Удалите пакет syntc-dpdk и выполните повторную инсталляцию дистрибутивного комплекта tc-, указав в файле конфигурации config.yaml меньшие значения для параметра rx_params, например -r 1:1

2. Недостаточно ядер CPU для запуска подсистемы фильтрации.

Увеличьте количество ядер CPU.

3. Не загружен модуль ibg_uio.

Выполните команду

```
/etc/init.d/configure_syntc start
```

проверьте, что модуль загружен командой

```
lsmod | grep igb_uio
```

- при старте в консоли присутствуют сообщения вида:

```
Unknown device: 0000:1b:00.1. Please specify device in
"bus:slot.func" format
```

Указанное в конфигурационном файле config.yaml устройство не существует в системе.

Удалите пакет syntc-dpdk и выполните повторную инсталляцию дистрибутивного комплекта tc-, указав в файле конфигурации config.yaml существующие идентификаторы PCI-устройств сетевых адаптеров.

8.4.2 Could not open pidile: /var/tmp/flog.pid

Симптомы

Запуск подсистемы фильтрации командой /etc/init.d/syntc start приводит к сообщениям

```
Starting syntc:
Cleaning up obsolete statistics...

start_tc: Starting cleaner....
Could not open pidile: /var/tmp/flog.pidFailed to start TC
FAILED
```

Возможные неисправности и пути их решения

1. Была произведена попытка запуска подсистемы фильтрации трафика напрямую без использования команды /etc/init.d/syntc start
2. Процесс журналирования событий flog запущен вручную, что не является корректным способом запуска.

Удалите PID файл командой

```
rm /var/tmp/flog.pid
```

и запустите подсистему фильтрации трафика командой

```
/etc/init.d/syntc start
```

9 Приложения

9.1 Установка ОС в интерактивном режиме

> ***Внимание:*** *Установка должна проводиться без доступа к сети Интернет. Нельзя обновлять компоненты до последних версий в процессе установки. Это приведет к невозможности установки Модуля.*

Для установки ОС в интерактивном режиме необходимо:

- подключить исходный образ для установки debian-10.0.0-amd64-DVD-1.iso и выполнить загрузку с устройства, в которое смонтирован этот образ;
- в загрузочном меню выбрать пункт Install;
- выбрать язык установки (рекомендуется оставить English);
- выбрать регион установки other;
- выбрать континент установки Europe;
- выбрать страну Russian Federation;
- выбрать язык локализации (рекомендуется оставить United States - en_US.UTF-8);
- выбрать раскладку клавиатуры (рекомендуется оставить American English);
- указать наименование сетевого узла для устройства (hostname), например, scout;
- указать домен при необходимости (можно оставить пустым);
- создать и ввести пароль пользователя root, повторно ввести тот же пароль на следующем экране и заполнить полное имя пользователя при необходимости;
- в поле Username for your account ввести значение syn;
- создать и ввести пароль для пользователя syn, отличный от пароля пользователя root;
- выбрать часовой пояс (рекомендуется оставить Moscow+00 - Moscow);
- на экране Partition disks выбрать вариант Manual;
- выполнить разметку диска следующим образом:
    - при использовании загрузки EFI, создать раздел EFI System Partition размером 500Mb;

- создать раздел swap (размер должен соответствовать размеру оперативной памяти);
- создать раздел physical volume for LVM, задействовав весь оставшийся объем;
- перейти в меню Configure the Logical Volume Manager и согласиться (выбрать Yes) в ответ на запрос Keep current partition layout and configure LVM?;
- создать группу томов, выбрав меню Create volume group;
- указать в качестве имени группы томов значение synta

Примечание: *Название synta зарезервировано системой для выполнения некоторых операций, поэтому другие имена групп не допускаются.*

- указать для группы томов использование физического раздела LVM, созданного ранее (как правило, /dev/sda3);
- создать логические тома, используя меню Create logical volume согласно таблице (в таблице указаны минимальные размеры):

Логический том	Точка монтирования	Тестовая среда	Производственная среда
synta/root	/	10G	50G
synta/home	/home	10G	20G
synta/dbdata	/var/lib/mysql	20G	400G
synta/dbbackup	/var/dbbackup	20G	400G
synta/dumps	/var/syn/dumps	10G	50G
synta/syn	/syn	10G	50G
synta/clickhouse	/var/lib/clickhouse	10G	500G

Примечание: *Логический том synta/clickhouse не является обязательным и может отсутствовать, либо располагаться на иных дисковых устройствах.*

- после создания логических томов, необходимо для каждого тома выбрать файловую систему и точку монтирования, для этого:

- перейти в списке доступных логических томов к разделу

- подтвердить внесение изменений, выбрав пункт меню Finish partitioning and write changes to disk
- в разделе Software slection выбрать пункты SSH server и Standard system utilites;
- подтвердить создание загрузчика и указать дисковое устройство, на которое он будет записан;
- дождаться окончания установки.

После окончания процесса установки и загрузки ОС, необходимо выполнить установку ядра ОС версии 4.19.0-23. Для этого необходимо:

- скопировать файл **linux-image-4.19.0-23-amd64-unsigned_4.19.269-1_amd64.deb** в установленную систему;
- выполнить команду, находясь в каталоге со скопированным файлом:

```
dpkg -i linux-image-4.19.0-23-amd64-unsigned_4.19.269-
1_amd64.deb
```

- дождаться установки ядра и перезагрузить операционную систему;

Операционная система готова к установке ПО Модуля.