ГАРДА

Гарда Скаут

Функциональная спецификация

gardatech.ru

2023

Тип документа:	Функциональная спецификация
Дата выпуска:	16.10.2023
Статус документа:	Released
Версия:	5.10

Содержание

1 Введение

1.1 Аннотация

В настоящем документе приведено описание функциональных возможностей программного модуля «Скаут», входящего в программное обеспечение Программный комплекс «Периметр» (Скаут, Система).

1.2 Типографические соглашения

Обозначения и типографические соглашения, используемые в данном документе, приведены ниже.

Пример	Обозначение
Примечание: *текст*	Важная информация, требующая особого внимания
См. Руководство администратора	Ссылка на документ
Войти	Названия элементов веб-интерфейса и конфигурационных параметров.
http://www.example.com/	Гиперссылки

1.3 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

Гарда Технологии (входит в ГК Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и

сертифицированы ФСТЭК.

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.

1.6 Перечень используемых терминов и сокращений

Система Скаут ПК «Скаут»	Программный модуль «Скаут», входящий в состав программного обеспечения Программный комплекс «Периметр»
DoS-атака	атака отказ в обслуживании (Denial of Service)
DDoS-атака	распределенная атака отказ в обслуживании (Distributed Denial of Service)
Вектор атаки	Общие характеристики трафика атаки, которые можно описать шаблонным пакетом, и характеризующие тип атаки
СПД	Сеть передачи данных
Профиль защиты Шаблон настроек методов защиты	Набор параметров методов фильтрации трафика, используемый при подавлении атаки
Профиль поведения	автоматически сформированное значение объемов трафика для каждого вида шаблонных пакетов
Шаблонный пакет	Набор значений параметров заголовков сетевого и транспортного уровня модели OSI, выделяющий определенный тип трафика, представленный в виде текстового описания

Сетевой хост	Узел сети, определяемый IP-адресом
Сетевой префикс	IP-адрес и маска подсети, определяющие набор сетевых хостов, принадлежащих одному сетевому сегменту
Наблюдаемый объект	Совокупность конфигурационных параметров Системы, применяемых к части сетевого трафика, определяемого набором сетевых префиксов или шаблонным пакетом

2 Обзор

2.1 Назначение системы

Скаут предназначен для обнаружения и противодействия сетевым атакам типа отказ в обслуживании (DoS/DDoS) на сети передачи данных (далее СПД).

Основные задачи, решаемые Системой:

- мониторинг сетевого трафика защищаемой инфраструктуры;
- обнаружение вредоносного трафика, относящегося к DDoS-атакам;
- очистка трафика от вредоносной составляющей DDoS атак;
- формирование и предоставление отчетной информации.

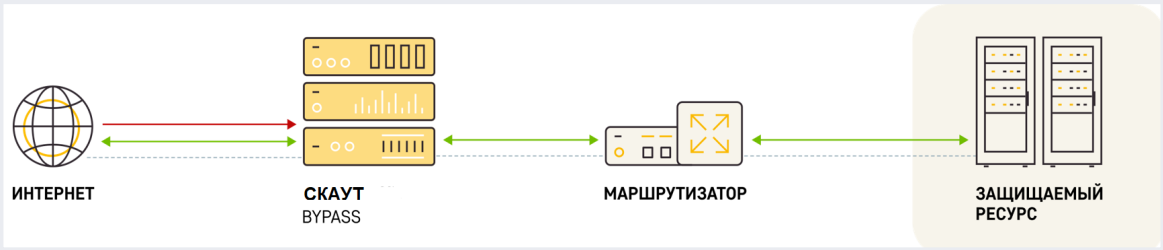
2.2 Структура системы

Скаут состоит из следующих логических подсистем:

- подсистема анализа сетевого трафика и детектирования атак, которая собирает информацию о трафике защищаемой инфраструктуры и выявляет вредоносное воздействие на основе превышения пороговых значений трафика, соответствующего имеющимся в Системе шаблонным пакетам и профилям поведения трафика.
- подсистема фильтрации трафика, которая выполняет очистку трафика от вредоносной составляющей в реальном времени.
- (опциональная) подсистема хранения метаданных о трафике, предназначена для накопления информации о трафике для дальнейшего ретроспективного анализа сетевой активности.

Логические подсистемы размещаются на одной аппаратной платформе: сервере с архитектурой x86-64.

2.3 Принцип работы



Скаут включается в сеть согласно обобщенной функциональной схеме (Рисунок 1). Скаут всегда включается в разрыв каналов связи, при этом он ведет себя как

«умный провод», т.е. не обладает собственными адресами на сетевых адаптерах, обрабатывающих трафик защищаемых ресурсов. Подключение Системы к каналам связи, через которые проходит трафик к защищаемым ресурсам, производится с помощью выделенных интерфейсов 1G/10G, поддерживающих технологию «аппаратный байпас».

Трафик, проходящий через Скаут, подвергается глубокому анализу и фильтрации на основе правил и критериев, определённых в профилях защиты ресурсов (шаблонов настроек методов защиты). Постоянный анализ проходящего трафика уменьшает время реакции системы на атаку, обеспечивая надёжную защиту для ресурсов и сервисов.

Для корректной работы алгоритмических методов фильтрации Скаута, работающих с сессиями протокола TCP, а также с инкапсулированными в них протоколами уровня приложений, требуется, чтобы балансировка трафика сетевым оборудования приводила к перенаправлению всех пакетов одной TCP-сессии на один и тот же Скаут.

Информация о трафике, проходящем через Скаут, применяется для формирования профилей поведения, которые используются для обнаружения аномалий и DDoS-атак. При обнаружении формируется соответствующее событие («DDoS-атака»), а к профилю поведения автоматически добавляются те предварительно сконфигурированные контрмеры, которые необходимы для подавления выявленного вредоносного воздействия.

Администрирование Скаута осуществляется пользователями через отдельный интерфейс управления 1000Base-T, не связанный с прохождением трафика, используя встроенный веб-интерфейс, интерфейс командной строки или API интерфейс.

Взаимодействие с внешними серверами электронной почты, syslog, DNS и т.д. осуществляется через интерфейс управления.

Управление аппаратной платформой осуществляется через выделенный порт BMC IPMI или его аналог.

3 Функциональные возможности

3.1 Обнаружение атак

Скаут поддерживает следующие возможности при обнаружении DDoS-атак:

- выявление превышений пороговых значений количества и/или объема трафика на отдельных сетевой хост или на группу сетевых хостов, составляющих наблюдаемый объект;
- выявление векторов атаки по шаблонным пакетам, набор которых поставляется с Системой (Приложение 3) и может быть изменен или дополнен администратором;
- формирование профиля поведения трафика для каждого вида анализируемого трафика (шаблонного пакета);
- настройка для различных защищаемых ресурсов индивидуального набора используемых шаблонных пакетов;
- настройка параметров профиля поведения: пороговые значения или параметры алгоритма их автоматического определения, при превышении которых выявляются векторы DDoS-атак.

Детектирование DoS-атак позволяет выявлять превышение пороговых значений количества (pps) или объема (bps) трафика заданной сигнатуры, направленного на защищаемый ресурс (IP-адрес) или группу защищаемых ресурсов (IP-префикс), либо исходящего от защищаемого ресурса или группы защищаемых ресурсов.

Для защищаемых ресурсов в Скауте могут создаваться логические наблюдаемые объекты, позволяющие использовать собственные настройки для детектирования и подавления DoS-атак. Настройки детектирования могут задаваться на трех уровнях:

- глобально (применяются для ресурсов, не входящих в наблюдаемые объекты или для наблюдаемых объектов, использующих глобальные настройки детектирования);
- в шаблоне детектирования (применяются к группе наблюдаемых объектов);
- в наблюдаемом объекте (применяются к конкретному наблюдаемому объекту).

Основными методом выявления DoS-атак в Скауте является детектирование превышения порогов трафика (независимые пороги по bps и pps) по шаблонным пакетам. Шаблонный пакет представляет собой структуру, содержащую

информацию о трафике: IP-адреса источника и получателя, протокол транспортного уровня, порты источника и получателя для протоколов tcp и udp, коды и типы ICMP и принадлежность к наблюдаемым объектам.

Скаут позволяет определять до 100 видов шаблонных пакетов, при этом 10 из них неизменяемые, а остальные 90 могут быть самостоятельно сконфигурированы пользователем.

Детектирование атак осуществляется одновременно:

- по трафику хостов назначения — вектор атаки выявляется при превышении порогового значения для трафика хоста (IP-адреса), при этом в векторе присутствует атакуемый IP-адрес;
- по трафику наблюдаемого объекта — вектор атаки выявляется при превышении суммарного трафика наблюдаемого объекта, соответствующего шаблонному пакету, при этом в вектор отсутствует атакуемый IP-адрес (атакуемые адреса определяются позже после сбора детальной статистики по вектору атаки).

Пороговые значения для выявления атак могут задаваться двумя способами:

- статические пороги (задаются и изменяются пользователем вручную);
- динамические пороги (рассчитываются автоматически на основе накопленной информации о трафике).

В режиме статических порогов доступны для редактирования поля для ввода значений объема (bps) и количества (pps) трафика. Превышение этих значений приведет к выявлению вектора атаки. Нулевое значение в поле отключает выявление вектора атаки по соответствующему критерию, что позволяет выявлять векторы атаки только по превышению объема или только по превышению количества трафика.

В режиме динамических порогов происходит периодическая (1 раз в час) актуализация пороговых значений, на основе накопленных данных о трафике с учетом задаваемых пользователем статистических параметров:

- Процентиль порога — значение процентиля (мера, в которой процентное значение общих значений равно этой мере или меньше ее), определяющего предварительный порог (без учета мультипликатора), превышение которого должно приводить к выявлению аномалии.
- Мультипликатор — множитель на который умножается значения предварительного порога, определенного по процентилю. Произведение

мультипликатора и предварительного порога дает окончательный порог, при котором выявляется аномалия.

- Глубина истории определения порога — временной интервал, который комплекс будет рассматривать для расчета порогов.
- Минимальный порог выявления — статические минимальные пороги выявления аномалий (если произведение мультипликатора и предварительного порога даст значение меньше минимального порога, то аномалия выявлена не будет).

3.2 Фильтрация трафика

Скаут подключается к сети передачи данных компании. Фильтрация может выполняться как по всему трафику, так и по отдельной его части на постоянной основе или по факту выявления DDoS атак.

Для фильтрации трафика Скаут использует набор алгоритмических методов. В качестве меры дополнительной защиты Скаут поддерживает возможность загрузки из внешних источников сигнатур вредоносного трафика, включающих сетевые параметры источников вредоносной активности: IP-адреса, протоколы и порты tcp/udp.

3.2.1 Основные возможности по фильтрации

Скаут поддерживает следующие возможности при фильтрации трафика:

- очистка шифрованного трафика, идущего на ресурсы защищаемой инфраструктуры, на этапе установления защищенного соединения (handshake), а также с возможностью опционального полного вскрытия (поддерживаемые шифронаборы приведены в Приложении 2);
- автоматический подбор мер противодействия под характер векторов атаки;
- возможность использования облачной сигнализации на комплекс «Периметр», установленный на стороне вышестоящего оператора связи;
- встроенный пакетный анализатор и декодер, предоставляющий возможность ручного анализа характера атаки при сохранении «сырого» трафика;
- формирование журнала обращений к защищаемым веб-сервисам;
- поддержка IPv4 и IPv6 протоколов;
- очистка трафика от широкого спектра DDoS атак (см. Приложение 1).

3.3 Предоставление аналитической и отчетной информации

Скаут сохраняет и обрабатывает информацию о трафике. На основе данной информации формируется набор аналитических отчетов и опционально предоставляется интерфейс ретроспективного изучения данных о трафике.

Аналитические отчеты по трафику всегда строятся для выбранного в блоке фильтрации интервала времени. Интервал задается значениями Сутки, Вчера, 1 неделя и т.д., либо выбором произвольных дат (и времени), определяющих границы интервала.

Аналитические отчеты строятся для одной из двух единиц измерения: bps (объем трафика в битах в секунду) или pps (количество трафика в пакетах в секунду). Выбор единицы измерения производится в блоке фильтрации.

Аналитические отчеты по трафику делятся на две группы:

- Состояние сети — содержит отчеты по всему трафику, проходящему через Систему;
- Профиль — содержит отчеты по трафику, соответствующему наблюдаемому объекту (Профилю).

В каждой группе отчеты делятся на различные типы:

- Суммарный отчет – входящий и исходящий трафик;
- Приложения – входящий и исходящий трафик выбранного протокола (tcp, udp, icmp) с разбивкой по портам для tcp/udp или кодам сообщений для icmp;
    - допускается дополнительная фильтрация по портам протоколов tcp/udp или кодам и типам сообщений icmp;
- По объектам › Профили – входящий и исходящий трафик с разбивкой по наблюдаемым объектам (профилям);
    - допускается дополнительная фильтрация по наблюдаемым объектам (профилям);
- Размер пакетов – входящий и исходящий трафик с разбивкой по размерам IP-пакетов;
    - допускается дополнительная фильтрация по размерам пакетов;
- Протоколы – входящий и исходящий трафик с разбивкой по протоколам транспортного уровня;

  - допускается дополнительная фильтрация по протоколам транспортного уровня;
- QoS – входящий и исходящий трафик с разбивкой по типам сервиса в различных нотациях (TOS, DTRM, IP Precedence, DSCP);
  - допускается дополнительная фильтрация по кодам ToS, DTRM, IP Precedence или DSCP;
- География IP – трафик с разбивкой по географическим признакам источника и получателя (Страны, Регионы, Города);
  - допускается дополнительная фильтрация по стране, региону или городу;
- Рейтинг по потреблению трафика – топ-100 IP адресов по пиковому трафику (внутренних для наблюдаемого объекта или внешних для наблюдаемого объекта);
- Пользовательские отчеты – входящий и исходящий трафик наблюдаемого объекта (профиля), соответствующий заранее заданной пользователем сигнатуре трафика (пользовательскому отчету).

Карта отчетов аналитической подсистемы приведены в таблице:

Отчет		**Состояние сети**	**Профили**
Суммарный отчет		√	
Суммарный отчет	Сравнение профилей		√
	Профиль		√
Суммарный отчет IPv6		√	
Прогноз IPv6		√	
Приложения	Все	√	√
	ICMP	√	√
	TCP	√	√
	UDP	√	√
Приложения IPv6	TCP	√	√

Отчет		Состояние сети	Профили
	UDP	√	√
По объектам	Профили	√	
Размер пакетов		√	√
Пользовательские отчеты			√
Протоколы		√	√
QoS	Тип сервиса	√	√
	Тип сервиса (DTRM)	√	√
	IP Precedence	√	√
	DSCP	√	√
Рейтинг по потреблению трафика	Внутренние IP-префиксы		√
	Внешние IP-префиксы		√
География IP	Страны	√	√
	Регионы	√	√
	Города	√	√

Минимальное разрешение отчетов аналитической подсистемы составляет 5 минут. Т.е. каждый 5 минут заполняются необходимые отчеты, в них появляется один новый временной отсчет. С течением времени, в связи с тем, что система хранения аналитических данных имеет конечный размер, накопленные данные по трафику усредняются. 5-минутные отсчеты превращаются сначала в 30-минутные, затем в 120-минутные, суточные и 4-х дневные.

Отчеты могут быть экспортированы в виде печатной формы (файл в формате PDF) или файла, содержащего структурированные данные (форматы csv, xml). Печатная форма может периодически высылаться на электронную почту, связанную с учетной записью пользователя. Пользователь самостоятельно

управляет подписками на аналитические отчеты. Альтернативным вариантом высылки отчетов по трафику служат правила уведомлений, которые позволяют рассылать отчеты сказанными параметрами группе адресов электронной почты.

Ретроспективное изучение информации о трафике возможно при использовании опциональной подсистемы хранения метаданных о трафике, которая предоставляет доступ к информации о трафике, обогащенной данными подсистемы анализа сетевого трафика и детектирования атак. Скаут допускает фильтрацию сохраненных в БД записей по различным критериям:

- IP-адресам источников и(или) получателей трафика;
- протоколам и(или) портам транспортного уровня;
- флагам протокола TCP;
- размерам IP-пакетов;
- соответствию шаблонным пакетам и наблюдаемым объектам, определенным в конфигурации Системы;
- географической принадлежности IP-адресов источника и(или) получателя;

а также группировку данных по указанным выше критериям, что в итоге позволяет получать произвольные отчеты по трафику с фильтрацией и группировкой более чем по 5 параметрам.

3.4 Безопасность и управление доступом

Безопасность управления Системой обеспечивается следующими механизмами:

1. использование протоколов с шифрованием (https, ssh) для доступа к веб-интерфейсу, API и управлению посредством командной строки;
2. использование ролевой модели доступа к функциональным подсистемам на основе групп пользователей, наборов прав доступа и персональных учетных записей пользователей;
3. аутентификация пользователей посредством логина и пароля;
4. блокировка учетных записей пользователей, в случае превышения заданного в настройках количества неуспешных попыток аутентификации в Системе;
5. логирование попыток аутентификации пользователей, в т.ч. неуспешных;
6. логирование запросов пользователей к страницам веб-интерфейса, API-запросов, в т.ч. при использовании утилиты командной строки;

Для доступа к веб-интерфейсу Система генерирует индивидуальную пару закрытый ключ и самоподписанный сертификат. Пользователь имеет

возможность установить собственный закрытый ключ и соответствующую ему цепочку сертификатов через веб-интерфейс путем загрузки файлов в форматах pem, der, p7b, cer или pfx.

Для подключения к ssh-серверу Система генерирует индивидуальные ключи RSA с длиной ключа 2048 бит, ECDSA с длиной ключа 256 бит и ED25519 с длиной ключа 256 бит.

Ролевая модель управления доступом основана на наборах прав доступа. Каждый набор прав доступа – это дерево разделов главного меню, в которых проставлен признак доступности (доступен пункт меню или не доступен). Один или более наборов прав доступа сопоставляется с группой пользователей (учетных записей). Каждая учетная запись входит в одну и только в одну группу пользователей.

В Системе существуют группы пользователей с двумя типами вхождения учетных записей:

- Обычный – учетные записи, входящие в группу, имеют доступ ко всем данным, находящимся в разделах меню, доступных в сопоставленных наборах прав доступа;
- Ограниченный – учетные записи, входящие в группу, имеют доступ к данным сопоставленным с одним наблюдаемым объектом (профилем), указанным в свойствах группы в разделах меню, доступных в сопоставленных наборах прав доступа.

Наборы прав доступа для групп с обычными пользователями и с ограниченными пользователями не пересекаются. Для ограниченных пользователей доступна функциональность личного кабинета пользователя. В личном кабинете существует возможность просмотра отчетов по трафику, выявленных DoS-атак и заданий подавления. Личный кабинет не позволяет изменять параметры Системы.

Пользователи аутентифицируются в веб-интерфейсе посредством ввода логина и пароля. Пароль должен отвечать политике сложности пароля:

- пароль должен содержать как минимум 8 символов;
- пароль должен содержать как минимум одну латинскую букву верхнего регистра;
- пароль должен содержать как минимум одну латинскую букву нижнего регистра;
- пароль должен содержать как минимум одну цифру;

- пароль должен содержать как минимум один специальный символ.

Учетная запись пользователя блокируется, если превышено количество попыток ввода пароля, приводящих к ошибке аутентификации. Разблокировать учетную запись может только пользователь, входящий в группу «Администратор системы» или администратор группы, в которую входит пользователь.

Попытки входа в систему (аутентификации) и выхода из неё заносятся в журнал истории пользователей. Ведется журнал доступа к страницам веб-интерфейса, а также журнал API-запросов.

3.5 Интеграция с внешними системами

Скаут поддерживает полнофункциональный API, используемый для управления, извлечения информации о выявленных атаках или отброшенном трафике, а также для доступа к подсистеме аналитических отчетов, включая опциональную подсистему хранения метаданных о трафике.

Доступна отправка уведомлений и отчетов на электронную почту, а также посредством протоколов SNMP и SYSLOG (форматы CEF и LEEF).

Скаут позволяет загружать с внешних ресурсов и периодически обновлять списки для фильтрации в различных форматах, формируемые, например, системами WAF или DPI:

- списки префиксов черных или белых списков;
- списки разрешенных или запрещенных DNS доменов;
- списки JA3-сигнатур для фильтрации.

Загрузка может выполняться с внешних веб-серверов, в том числе использующих HTTPS, (S)FTP-серверов или используя протокол SCP. Списки также могут обновляться посредством API.

3.6 Администрирование системы

Управление основано на ролевой модели пользователей и доступно через:

- графический веб-интерфейс;
- режим командной строки (CLI-интерфейс);
- интеграционный интерфейс (API).

Система ведет журнал действий пользователей.

3.6.1 Надежность

- Круглосуточная работа 24/7 в необслуживаемом режиме.
- Коэффициент готовности Системы – 99,0%.

3.6.2 Масштабируемость

Масштабирование системы возможно в рамках одной аппаратной платформы, требует её модернизации в соответствии с требованиями к аппаратной платформе (см. Раздел 3), соответствующего лицензионного расширения полосы фильтрации и добавления опциональных возможностей (вскрытие трафика, активация подсистемы хранения метаданных).

3.6.3 Лицензирование

Лицензия выдается на конкретный экземпляр ПО.

Контролируются следующие параметры:

- Интервал действия лицензии (от, до);
- Полоса пропускания (входящий трафик);
- Поддержка вскрытия SSL;
- Поддержка хранения информации о трафике.

Функционал, заблокированный лицензионными ограничениями, не активируется. При покупке (замене) лицензии происходит активация функциональности без необходимости полной переустановки ПО.