ГАРДА

Гарда Скаут

Руководство пользователя

gardatech.ru

2023

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

ООО «Гарда Технологии»
Все права сохраняются за правообладателем.

ООО «Гарда Технологии» оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО «Гарда Технологии». Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким- либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО «Гарда Технологии». Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

Содержание

1 Введение

1.1 Аннотация

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

1.2 Термины, определения и сокращения

ПО	программное обеспечение
ПК	программный комплекс
ООО	Общество с ограниченной ответственностью
Система	ПК «Периметр»
Скаут	Модуль «Скаут», входящий в состав программного обеспечения ПК «Периметр»
PCT95	95-й процентиль - мера, в которой процентное значение общих значений равно этой мере или меньше ее: 95 % значений данных находятся ниже 95-го процентиля.
DoS	англ. Denial of Service - отказ в обслуживании
DDoS	англ. Distributed Denial of Service - распределённый отказ в обслуживании
СПД	сеть передачи данных
API	программный интерфейс для внешних приложений (Application program interface)
DPI	англ. Deep Packet Inspection – технология глубокого анализа пакетов
gfcap	англ. Garda Technology Flow Capture fingerprint expression language - язык описания сигнатур трафика в методах фильтрации и фильтрах захвата пакетов
qty	англ. quantity – количественная характеристика, например, количество запросов или количество соединений

CEF	Common Event Format – настраиваемый формат сообщений, основанный на протоколе SYSLOG, совместимый с HP ArcSight
LEEF	Log Event Extended Format – настраиваемый формат сообщений, основанный на протоколе SYSLOG, совместимый с IBM QRadar
ToS	тип обслуживания (тип сервиса по rfc1349), поле в заголовке IP-пакета
DTRM	нотация поля ToS: D - минимальная задержка, T - максимальная пропускная способность, R - максимальная надежность, M - минимальная стоимость
IP Precedence	нотация поля ToS: биты 0-2, определяет важность датаграммы
DSCP	англ. differentiated services codepoint – часть поля DS (Differentiated Services) заголовка IP-пакета, отвечающая за обеспечение качества сервиса (rfc2474, rfc2475)

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 Первоначальный вход в систему

Управление Скаутом осуществляется через веб-интерфейс с использованием защищенного протокола HTTPS. Для доступа к веб-интерфейсу управления, необходимо:

- открыть браузер;
- ввести в адресную строку https://<IP_АДРЕС_УПРАВЛЕНИЯ>, где вместо <IP_АДРЕС_УПРАВЛЕНИЯ> необходимо подставить действительный IP-адрес, выделенный для управления Скаутом;
- ввести логин и пароль, полученные при установке Скаута в соответствующие поля и нажать на кнопку Войти.

3.1 Действия после первого входа в интерфейс управления

После успешного первоначального входа в интерфейс управления Скаута, рекомендуется выполнить следующие операции:

1. сменить пароль текущего пользователя (администратора), выполнив следующие действия:
   - в правом верхнем углу экрана щелкнуть левой кнопкой мыши по логину пользователя и в открывшемся меню выбрать пункт Учетная запись;
   - в правой части в форме редактирования параметров ввести новый пароль в соответствующее поле ввода;
   - повторить ввод нового пароля в поле Подтверждение пароля;
   - нажать на кнопку Сохранить;
2. настроить белый список доступа:
   - перейти в меню Настройки › Доступ и выбрать вкладку Опции;
   - указать количество попыток аутентификации, после исчерпания которых пользователь будет заблокирован, в соответствующем поле;
   - указать префиксы в формате CIDR-блоков в поле Белый список IP-адресов, доступ с которых пользователю будет разрешен, даже если его учетная запись заблокирована;
   - нажать кнопку Сохранить;

Примечание: *Данная операция необходима для организации доступа в систему даже при заблокированной учетной записи администратора.*

3. обеспечить сетевую безопасность интерфейса управления Скаута:
   - настроить фильтрацию сетей и портов на сетевом оборудовании, через которое организован доступ к управлению Скаутом;
   - настроить черный и белый список адресов для доступа к комплексу (см. раздел Ограничение доступа к интерфейсу управления);
   - настроить мониторинг сетевых подключений к комплексу (см. раздел Контроль сетевых подключений);.
4. выполнить проверку соответствия условий лицензии задачам, которые ставятся перед комплексом.

4 Подавление атак

Скаут защищает ресурсы и сервисы, в заданиях подавления. Задание подавления определяет параметры защиты и применяемые контрмеры для заданного набора IP-префиксов защищаемых ресурсов. Таком образом, Скаут защищает ресурс целиком, однако защита отдельных сервисов, которые располагаются на защищаемом ресурсе может выстраиваться по-разному.

4.1 Защита в рамках глобального задания подавления

После развертывания Скаут содержит одно специализированное задание подавления Global Mitigation, в котором производится фильтрация трафика защищаемых ресурсов, который не выделен в отдельные задания подавления.

> ***Примечание:*** *Защита конкретного ресурса производится в одном и только одном задании подавления. Если IP-префикс защищаемого ресурса не присутствует ни в одном задании подавления, то его защита осуществляется в специализированном задании Global Mitigation. В противном случае, защита осуществляется в созданном задании подавления.*

Каждое задание подавления связано с шаблоном подавления атак, в котором уже настроены параметры контрмер. Скаут включает в себя набор базовых шаблонов для защиты часто используемых ресурсов и сервисов:

Название	Назначение
DNS Server_high	Защита DNS-серверов (порт udp/53), включающая пассивную аутентификацию и проверку по DNS RFC. Защита DNS-серверов (порт tcp/53), включающая защиту от syn- и syn/ack- флудов и защиту от медленных атак.
DNS Server_medium	
DNS Server_low	
File Server_high	Защита FTP-серверов (порты tcp/21 и tcp/20), а также HTTP(S) серверов (порты tcp/80, tcp/443) включающая защиту от syn- и syn/ack- флудов, защиту от медленных атак и ограничение кол-ва соединений для каждого источника.
File Server_medium	
File Server_low	

Название	Назначение
Generic Server_high	Универсальная защита часто используемых сервисов DNS и HTTP(S), включающая защиту от syn- и syn/ack- флудов, проверку на соответствие RFC, ограничение кол-ва соединений от источника, а также ведение журнала запросов и ответов для HTTP.
Generic Server_medium	
Generic Server_low	
Mail Server_high	Защита почтовых сервисов, использующих транспорт TCP и HTTP(S), включающая , защиту от syn- и syn/ack-флудов, защиту от медленных атак, ограничение кол-ва соединений от источника, а также проверку на соответствие RFC для TLS.
Mail Server_medium	
Mail Server_low	
VOIP Server_high	Специализированный шаблон для защиты SIP-серверов, включающий шейпинг INVITE и REGISTER запросов, а также базовую защиту для HTTP(S).
VOIP Server_medium	
VOIP Server_low	
VPN Server_high	Защита всех tcp-портов хоста отsyn- и syn/ack-флудов, медленных атак, ограничение кол-ва соединений от источника, а также проверку на соответствие RFC для TLS и HTTP
VPN Server_medium	
VPN Server_low	
Web Server_high	Защита Web-серверов (порты tcp/80, tcp/443 и tcp/8080), включающая защиту от syn-, syn/ack- и ack-флудов, проверку по RFC для HTTP и TLS защиту от медленных атак и ограничение кол-ва соединений для каждого источника.
Web Server_medium	
Web Server_low	

Примечание: *Суффикс high в названии шаблона обеспечивает более агрессивную защиту по сравнению с medium и low. Шаблон с суффиксом low включает наиболее мягкую защиту.*

Любой шаблон может быть изменен в меню Настройки › Подавление атак на вкладке Шаблоны. Изменение параметров в шаблоне приведет к изменению параметров во всех заданиях подавления, основанных на измененном шаблоне, при условии, что эти параметры не были скорректированы в самом задании подавления.

Администратор Скаута может создать свои шаблоны и использовать их при подавлении атак.

Каждый шаблон содержит настройки методов защиты, специфичных для отражения определенных видов атак и(или) защиты определенных сервисов. Например, защита веб-сервера может блокировать весь трафик, не относящийся к сервису WWW, в то время как защита DNS-сервера может блокировать HTTP трафик на сетевом уровне.

4.1.1 Выбор шаблона подавления атаки

Чтобы выбрать шаблон подавления атаки для задания подавления Global Mitigation, необходимо:

- перейти в меню Подавление атак на вкладку Задания;
- найти в списке задание Global Mitigation и щелкнуть в найденной строке в столбце Название;
- в открывшемся окне найти поле Шаблон подавления атаки и нажать на кнопку Заменить;
- выбрать из списка шаблон, наиболее подходящий для защищаемых ресурсов и нажать на кнопку Применить;
- подтвердить изменение параметров нажатием на кнопку Сохранить.

Примечание: *В Скауте может быть запущено только одно глобальное задание подавление.*

Параметры контрмер, используемых для фильтрации трафика, можно корректировать путем изменения в задании подавления или в шаблоне, связанном с этим заданием.

4.1.2 Корректировка параметров контрмер в задании подавления

Для получение детализированной статистики и управления параметрами контрмер, необходимо:

- перейти в меню Подавление атак на вкладку Задания;
- найти в списке задание Global и щелкнуть в найденной строке в столбце Трафик на изображении мини-графика (если трафик отсутствует, в рамке будет присутствовать фраза «нет данных») для перехода к экрану статуса задания подавления.

Экран Статус задания содержит в левой части информацию о состоянии задания, задействованных инструментах подавления, а также информацию об отброшенном трафике в графическом и табличном представлении. В правой части расположены элементы управления методами фильтрации трафика.

Включение режима редактирования параметров контрмер

Экран статуса задания периодически обновляется, отображая текущее состояние методов фильтрации и статистику отброшенного трафика. Режим просмотра позволяет наблюдать за поведением системы.

Для того, чтобы изменить параметры контрмер, необходимо переключиться в режим редактирования, используя переключатель Режим редактирования, расположенный в верхней правой части экрана.

Управление контрмерами

В режиме редактирования возможно:

- включить или отключить отдельный метод защиты, используя переключатель слева от названия метода;
- изменить параметры метода защиты.

В некоторых случаях включение метода защиты требует предварительного включения другого метода защиты. Например, работа метода HTTP RFC невозможна без включения метода Фильтр TCP-соединений с нарушением последовательности, а метод JA3 фильтр не может работать без включения метода SSL и Фильтр TCP-соединений с нарушением последовательности. Включить зависимые методы можно раскрыв блок параметров метода и нажать на кнопку Включить в соответствующем информационном блоке.

Подтверждение внесенных изменений осуществляется нажатием на кнопку Сохранить, при этом производится проверка корректности и применение параметров во всех измененных методах фильтрации.

Выход из режима редактирования

Выход из режима редактирования осуществляется автоматически вместе с применением параметров, при условии, что все проверки параметров пройдены успешно.

При необходимости выхода из режима редактирования без сохранения значений измененных параметров, следует использовать кнопку Режим просмотра.

4.2 Защита в рамках индивидуального задания подавления

Для защиты ресурса с использованием особой или отличной от используемой в глобальном задании политики защиты, необходимо использовать индивидуальное задание подавления. Индивидуальное задание подавления, также, как и глобальное, может содержать собственные настройки методов фильтрации трафика или использовать политику защиты из шаблона настройки методов. Кроме того, индивидуальное задание подавление может быть связано с наблюдаемым объектом, что позволяет выявлять атаки и включать необходимые защитные механизмы только во время атаки, минимизируя воздействие на трафик.

4.2.1 Создание индивидуального задания подавления

Для создания нового задания подавления, необходимо перейти в меню Подавление атак и нажать на кнопку + Добавить задание, расположенную в правом верхнем углу над списком заданий.

На панели Основная информация необходимо заполнить поля:

Название:	понятный человеку идентификатор создаваемого задания подавления;
Защищаемые префиксы:	список IP-префиксов защищаемых ресурсов, перечисленных через запятую;
Шаблон подавления атаки:	политика защиты, набор контрмер, с которым будет запускаться задание подавления.

На панели Инструменты подавления необходимо выбрать хотя бы один из инструментов:

Очиститель:	фильтрация трафика непосредственно в Скауте;
BGP FlowSpec:	фильтрация на маршрутизаторе согласно правилу BGP Flow Specification, отправляемому со Скаута;

Blackhole:	фильтрация на маршрутизаторе путем отбрасывания трафика или перенаправления на указанный next-hop.

Как правило, для фильтрации используется инструмент подавления Очиститель, поэтому необходимо в соответствующей строке нажать на кнопку ✚ Выбрать и выбрать один из шаблонов подключения очистителей.

После заполнения всех обязательных полей, необходимо нажать на кнопку Сохранить, чтобы создать задание, но не запускать его, либо на кнопку Сохранить и запустить, чтобы создать задание подавления и активировать фильтрацию трафика.

4.2.2 Запуск и остановка задания подавления

Запустить задание подавления можно несколькими способами:

1. перейти в меню Подавление атак на вкладку Задания, найти в списке задание, которое требуется запустить, и в столбце Действия нажать на кнопку ▶;
2. перейти в меню Подавление атак на вкладку Задания, найти в списке задание, которое требуется запустить, перейти на экран статуса задания, щелкнув левой кнопкой по мини-графику в столбце Трафик, а затем на экране статуса задания на жать на кнопку ▶ Запустить задание.

Остановка задания подавления производится теми же способами, что и запуск, только используется кнопка ■ Остановить задание. Также существует возможность остановки нескольких заданий одновременно. Для этого необходимо установить отметку (флажок в первом столбце) на необходимых заданиях, после чего нажать на кнопку ■ Остановить, расположенную в панели действий над списком заданий подавления.

4.2.3 Управление параметрами защиты в индивидуальном задании подавления

Для изменения параметров контрмер или используемого в индивидуальном задании шаблона подавления атаки, необходимо выполнять те же действия, что и для глобального задания, рассмотренные в разделах Выбор шаблона подавления атаки и Корректировка параметров контрмер в задании подавления.

4.3 Использование пользовательских списков

Скаут позволяет выполнять блокирование трафика от заданных источников, используя метод фильтрации Черный список.

Для работы метода необходимо предварительно создать или загрузить с внешнего ресурса список IP-префиксов, трафик с которых должен блокироваться. Созданные списки загружаются в подсистему фильтрации Скаута, после чего они могут быть использованы в заданиях подавления.

Для создания пользовательского списка, необходимо:

- перейти в меню Настройки › Подавление атак на вкладку Пользовательские списки;
- нажать на кнопку + Добавить запись;
- ввести название списка в соответствующее поле на вкладке Описание;
- перейти на вкладку Конфигурация;
- если планируется ручное заполнение списка, ввести в поле Перфиксы список префиксов источников (разделитель пробел и(или) запятая);
- если планируется загрузка списка из внешнего источника, выбрать в поле Загрузка списка протокол, который будет использоваться для загрузки, и заполните поля, указывающие источник загрузки списка (формат списка - простой текст, один префикс в каждой строке);
- активируйте переключатель Выгрузка на очиститель, чтобы список попал в подсистему фильтрации Скаута;
- нажмите на кнопку Сохранить.

Чтобы активировать использование списка в задании подавления, необходимо:

- включить метод фильтрации Черный список для выполнения блокировки трафика или метод Белый список для безусловного пропуска трафика от источников, заданных в списке;
- нажать на кнопку + Выбрать и переместить списки, которые необходимо использовать в правое окно;
- нажать на кнопку Применить для подтверждения изменений;
- нажать на кнопку Сохранить для применения обновленной конфигурации методов фильтрации.

Примечание: *Одни и те же списки могут быть использованы в нескольких заданиях подавления. Изменение списка отразится на фильтрации трафика во всех заданиях подавления, использующих этот список. Если список не загружен в подсистему очистки, фильтрация трафика по этому списку осуществляться не будет до тех пор, пока список не будет загружен.*

4.4 Использование режима статистики

При использовании инструмента подавления Очистители, существует возможность минимизировать воздействие на фильтруемый в рамках задания трафик, путем перевода задания в режим статистики.

Режим статистики позволяет настроить поведение методов фильтрации, увидеть информацию об отброшенном трафике или заблокированных источниках **без фактической блокировки трафика**. На экране статуса задания при включенных методах фильтрации будет отображаться информация об отброшенном трафике, при этом трафик не будет блокироваться, сессии не будут разрываться, а черный список не будет блокировать трафик от источников. Это позволяет отследить влияние методов фильтрации на легитимный трафик и не допустить его блокирование.

Некоторые методы защиты являются активными, т.е. взаимодействуют с источником трафика. Такие методы не могут работать, если используется режим статистики. Оценить их влияние можно только после перевода задания в режим блокирования трафика. Кроме того, нужно понимать, что при включении рабочего режима характер трафика изменится. Методы начнут блокировать трафик, разрывать сессии, что приведет к изменениям на графике отброшенного трафика.

4.5 Сбор «сырого» трафика

На экране статуса задания подавления существует возможность сбора IP-пакетов с учетом заданных критериев. Для того, чтобы запустить сбор «сырого» трафика, необходимо:

- перейти в меню Подавление атак на вкладку Задания;
- перейти на экран статуса задания подавления, для которого необходимо собирать «сырой» трафик, щелкнув на мини-графике в столбце Трафик;
- на открывшемся экране статуса задания перейти на вкладку Сырой трафик;

- изменить параметры сбора трафика, если это необходимо, нажав на кнопку ⚙ Настройки дампа и изменив значения полей, например, увеличить количество собираемых пакетов или максимальное время сбора трафика;
- нажать на кнопку ▶ Запустить.

Информация о собранных пакетах будет отображаться в таблице, содержащей основные поля заголовка IP пакета, а также порты протоколов tcp и udp. Дополнительно, для заблокированных пакетов в столбце Информация отображается название метода, который принял решение о блокировке пакета.

Если отметить строку с информацией о пакете щелчком левой кнопки мыши, то будет проведено декодирование выбранного пакета. Информация о найденных заголовках будет отображена в разделе Содержимое пакета.

Собранный дамп трафика можно выгрузить в файл в формате PCAPNG, нажав на кнопку 📥 Скачать дамп. В выгружаемом файле кроме собранных пакетов присутствует дополнительная информация, например, направление в котором пакет прошел через подсистему фильтрации или состояние пакета: заблокирован, пропущен и т.д.

4.6 История изменений параметров задания подавления

Все действия, выполняемые в рамках задания подавления, журналируются. Журнал располагается на экране статуса задания подавления. Журналируются, как действия пользователей, так и изменения, вносимые самой Системой в случае использования автоматического детектирования и подавления атак.

5 Рекомендации по защите ресурсов и сервисов

Защита ресурсов и сервисов должна строиться по эшелонированному принципу. Необходимо минимизировать возможную поверхность атаки, причем блокировка вредоносного трафика должна по возможности осуществляться на пакетном уровне или путем блокирования всего трафика от источников атаки.

5.1 Базовая защита

Базовая защита включает в себя защиту от атак:

- пакетами с некорректно заполненными заголовками сетевого и транспортного уровней;
- пакетами с некорректными комбинациями флагов протокола TCP;
- пакетами с некорректными значениям контрольных сумм;
- пакетами транспортных протоколов, которые не используются защищаемым ресурсом/сервисом;
- фрагментированными IP-пакетами;
- ip private, ip null, land, fraggle, teardrop и их аналогов.

Базовая защита строится на основе анализа соответствия сетевых пакетов основным правилам, описанным в RFC, а также путем выполнения пакетной фильтрации согласно пользовательским правилам.

Контроль корректности заголовков сетевых пакетов выполняется для всех пакетов. Некорректные пакеты отбрасываются на входе подсистемы очистки трафика Скаута или в методе Базовая очистка в задании подавления.

В методе Базовая очистка рекомендуется включить опции:

- Правильность контрольной суммы IP;
- Правильность контрольной суммы TCP;
- Правильность контрольной суммы UDP;

для блокировки пакетов с некорректными контрольными суммами.

Рекомендуется разрешить прохождение пакетов только для тех протоколов транспортного уровня, которые используются защищаемым ресурсом/сервисом. Все остальные протоколы следует заблокировать. Блокировка осуществляется путем создание в методе Фильтр задания очистки правил вида:

```
drop not tcp,udp
```

Для протоколов tcp и udp рекомендуется ограничить прохождение трафика на неиспользуемые защищаемым ресурсом порты путем создания в методе Фильтр задания очистки правил вида:

```
drop tcp and not dst port 80,443
```

Рекомендуется использовать пользовательские черные списки источников вредоносного трафика для блокировки трафика от известных источников. Работа с пользовательскими списками рассмотрена в разделе Использование пользовательских списков.

Рекомендуется ограничить прохождение IP-фрагментов путем создания в методе Фильтр задания очистки правил вида:

```
drop ipfrag
```

При невозможности полного запрета прохождения IP-фрагментов, рекомендуется включить метод IP Фрагентация, позволяющий защититься от атак повторными фрагментами, фрагментами выходящими за длину пакета или с некорректно заданной длиной, а также teardrop-атак.

Для защиты от land-атак, рекомендуется заблокировать трафик от источников, которые совпадают с защищаемыми префиксами. Например, если под защитой находится подсеть 192.0.2.0/24, то необходимо добавить правило в методе Фильтр задания очистки:

```
drop src 192.0.2.0/24 and dst 192.0.2.0/24
```

Аналогичным образом рекомендуется блокировать трафик, исходящий из приватных IPv4 диапазонов.

Если в правилах не создавались ограничения на используемые сервисом протоколы транспортного уровня, для защиты от атак ip null, рекомендуется добавить правило в методе Фильтр задания очистки:

```
drop proto 0
```

5.2 Защита TCP-сервисов

При защите сервисов, использующих протокол TCP, в дополнение к рекомендациям по обеспечению базовой защиты, необходимо обеспечить защиту от атак, направленных на уязвимости протокола TCP:

- атаки пакетами с флагами syn, syn+ack, ack и т.д.;

- атаки пакетами не принадлежащими легитимным соединениям tcp;
- атаки соединениями tcp (connection flood);
- атаки медленными соединениями (slow connection flood).

Для отслеживания tcp-подключений необходимо, задать tcp-порты защищаемых ресурсов, для которых будет осуществляться регистрация и контроль. Для этого необходимо использовать пункт Порты контрмер раздела Настройки в контрмерах задания подавления. Если порт не будет присутствовать в списке, защита не будет обеспечена.

Для защиты от атак syn-flood или syn/ack-flood используются активные методы аутентификации клиента. Источник, желающий установить соединение по протоколу TCP проверяется путем отсылки ему специализированных пакетов и получения от него верных ответов. После успешной аутентификации, источнику разрешается открыть некоторое число tcp-соединений, после чего процесс аутентификации повторяется.

Защита от атак, связанных с отправкой tcp-пакетов не принадлежащих открытым соединениям, предполагает отслеживание tcp-соединений и отбрасывание вредоносной составляющей.

Для защиты от таких атак рекомендуется включить два метода защиты:

1. TCP-аутентификация;
2. Фильтр TCP-соединений с нарушением последовательности

Внимание: *Метод контроля последовательности TCP должен всегда использоваться в паре с методом tcp-аутентификации для исключения переполнения числа отслеживаемых tcp-подключений во время атак типа syn-flood.*

Для защиты от атак соединениями tcp (connection flood), необходимо ограничить число активных tcp-соединений от одного источника (без учета dst IP в рамках одного задания подавления) путем включения метода фильтрации Ограничение кол-ва TCP-соединений для хоста. Количество разрешенных соединений может варьироваться в зависимости от конкретного защищаемого сервиса.

Стратегия защиты от атак медленными соединениями предполагает использование двух компонентов:

1. отслеживание tcp-соединений и принятие решения о том, что соединение медленное;
2. блокировка IP-источников, которые создают медленные соединения.

Для защиты от медленных атак, рекомендуется включить два метода:

1. Простаивающие установленные TCP-соединения с действием Заносить в черный список;
2. Динамический черный список.

5.3 Защита UDP-сервисов

При защите сервисов, использующих протокол UDP, в дополнение к рекомендациям по обеспечению базовой защиты, необходимо обеспечить защиту от атак, направленных на уязвимости протокола UDP:

- атака пакетами со случайным содержимым (udp random flood);
- объемные атаки с отражением и усилением.

Протокол UDP позволяет переносить любую информацию, поэтому для защиты от атак пакетами со случайным содержимым, рекомендуется (в дополнение к блокировкам базовой защиты) включить метод Зомби, в котором настроить ожидаемый сервисом поток UDP-пакетов от одного источника (IP-адреса) в качестве порогового значения и определить сигнатуру трафика, для которой будет контролироваться скорость поступления пакетов от источников, и метод Динамический черный список, в который метод Зомби будет помещать IP-адреса выявленных ботов. Например, если защищаемый сервис прослушивает порт udp/33333 и ожидает поток пакетов от одного источника не более 1Kpps, сигнатура анализируемого трафика будет выглядеть следующим образом:

```
udp and dst port 33333
```

Использование действия В черный список приведет к тому, что трафик с IP-адресов, для которых зафиксировано превышение порога в 1Kpps будет полностью блокироваться. Длительность блокировки определяется временем, на которое адрес помещается в черный список.

В случае, если в пакетах защищаемого сервиса можно выделить общий признак, для защиты от атак пакетами со случайным содержимым, необходимо включить метод Payload regexp, в котором определить регулярное выражение для отрицания этого общего признака. Например, если в пакете должна присутствовать последовательность *xyz* в 7-м байте пакета, то регулярное выражение будет выглядеть следующим образом:

```
^.{6}(?!xyz)
```

Примечание: *Если в параметрах метода Payload regexp флаг Отключить сэмплирование не установлен, возможны пропуски некоторых пакетов, соответствующих регулярному выражению, если подсистема фильтрации не успевает обработать их в условиях высокой нагрузки. Флаг необходимо установить, если требуется отбрасывать пакеты, которые невозможно проанализировать из-за перегрузки.*

5.4 Защита от атак с отражением и усилением

Атаки с отражением (Reflection) и усилением (Amplification) относятся к классу объемных атак, направленных на исчерпание полосы пропускания каналов связи. Однако, некоторые варианты могут быть направлены на исчерпание ресурсов защищаемых ресурсов.

Атаки этого типа, как правило, выполняются с использованием открытых серверов, дающих необходимый коэффициент усиления атаки. Поэтому для защиты можно использовать заранее подготовленные черные списки с уязвимыми серверами, подключая необходимые списки после выявления атаки и отключая их после завершения атаки.

Простейшим способом подавление атак с усилением является фильтрация трафика, при которой доступ с проверенных серверов, предоставляющих необходимые защищаемому ресурсу сервисы, принудительно разрешается, а остальной трафик блокируется:

```
pass src 8.8.8.8 and src port 53
pass src 129.6.15.28 and src port 123
drop src port 53,111,123,161,135,139,389,445,1900,3389,11211
drop ipfrag
```

Более сложные варианты атак с отражением и усилением используют произвольные устройства в сети Интернет для генерации tcp-пакетов с флагами syn+ack, при этом усиление достигается повторной отправкой этих пакетов (retransmission) в случае, если источник не получает пакет с флагом rst. Для ослабления такой атаки, рекомендуется использовать методику защиты tcp-сервисов с включением аутентификации для пакетов syn+ack и контролем последовательности tcp-подключений.

5.5 Защита web-серверов

В дополнение к базовой защите и защите tcp-сервисов, при защите web-серверов на базе протокола http/1, рекомендуется:

- включать метод HTTP-аутентификация в режиме Двойное перенаправление (HTTP 302) или JavaScript переадресация;
- активировать параметр Проверять URL для защиты от open redirect.

> ***Примечание:*** *Клиенты сервиса должны поддерживать используемый метод перенаправления.*

Для защиты от атак HTTP-запросами, содержащими некорректные с точки зрения RFC значения, рекомендуется включить метод HTTP RFC.

Если все HTTP-запросы к защищаемому ресурсу должны содержать обязательные заголовки, то рекомендуется включить метод Расширенная фильтрация HTTP и внести эти заголовки в параметр Список обязательных HTTP заголовков.

Дополнительные ограничения, накладываемые на URI или имя запрашиваемого хоста, устанавливаются в методе HTTP regexp путем указания регулярного выражения в формате PCRE.

При использовании защищенного протокола HTTPS, методы работы с протоколом HTTP будут работать с расшифрованным трафиком, если включен метод Перехват SSL.

Если метод Перехват SSL не используется, то защита web-сервера возможна только на этапе установки соединения TLS. Рекомендуется активировать метод SSL и включить параметр Проверять RFC для защиты от атак на протокол SSL/TLS.

Если при установке TLS-соединения существуют обязательные или запрещенные к использованию значения параметров сообщения ClientHello, они могут быть определены в разделе Фильтры. Фильтры могут значительно снизить поверхность атаки, однако устанавливать их необходимо по согласованию с владельцем защищаемого ресурса.

Еще одним вариантом фильтрации сообщений ClientHello является использование списков JA3 и метода JA3 фильтр. Методика работы полностью аналогична пользовательским спискам, рассмотренным в разделе Использование пользовательских списков.

5.6 Защита серверов DNS

В дополнение к обеспечению базовой защиты, при защите DNS-серверов, необходимо обеспечить защиту от атак:

- DNS-запросами с некорректным содержимым (garbage dns attack);
- DNS-запросами ресурсов, которые DNS-сервер не должен обрабатывать;
- DNS-запросами, создаваемыми ботами, а не легитимными пользователями.

Защита от атак некорректными DNS-запросами или UDP-пакетами, содержащими данные не соответствующие протоколу DNS, обеспечивается включением параметра Проверка DNS RFC в методе фильтрации DNS.

Методика защиты от атак корректными DNS-запросами зависит от роли, которую выполняет DNS-сервер: рекурсивный или авторитетный.

Для рекурсивных DNS-серверов, находящихся под атакой, рекомендуется принудительно переводить клиентов на использование протокола TCP, включив параметр Формировать DNS через TCP в методе DNS. При этом, необходимо рассматривать DNS-сервер как tcp-сервис, и обеспечить его защиту методами, рассмотренными выше.

Для авторитетных DNS-серверов, необходимо использовать методы активной аутентификации, включив параметр Перенаправление на несуществующий домен в методе DNS и(или) загрузить в подсистему очистки Скаута списки разрешенных (или наоборот, запрещенных) ресурсов и включить метод DNS список. Методика работы со списками DNS ресурсов полностью аналогична пользовательским спискам, рассмотренным в разделе Использование пользовательских списков.

6 Перехват SSL-сессий

Скаут способен использовать методы работы с HTTP/1.X-запросами HTTP-RFC, HTTP-журнал, HTTP-regexp, и Расширенная фильтрация HTTP даже при использовании протокола HTTPS. Это дает возможность отражать атаки вида HTTP request flood даже внутри защищенных соединений HTTPS.

Для того, чтобы получить доступ к содержимому запросов, Скаут выступает в качестве прозрачного прокси для защищаемого Web-сервера. Соответствующий функционал реализуется в методе фильтрации Перехват SSL.

Прежде чем начать использовать метод Перехват SSL, необходимо выполнить предварительную настройку: включить возможность загрузки сертификатов в подсистему фильтрации трафика и загрузить в Скаут секретный ключ и соответствующий ему сертификат защищаемого Web-сервера.

Скаут поддерживает работу со следующими шифронаборами:

TLS_RSA_WITH_NULL_MD5 (0x0001)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_RSA_WITH_NULL_SHA (0x0002)	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)
TLS_RSA_WITH_RC4_128_MD5 (0x0004)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
TLS_RSA_WITH_RC4_128_SHA (0x0005)	TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
TLS_RSA_WITH_DES_CBC_SHA (0x0009)	TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)	TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)
TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)	TLS_ECDHE_ECDSA_WITH_NULL_SHA (0xc006)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_RSA_WITH_NULL_SHA (0xc010)
TLS_RSA_WITH_NULL_SHA256 (0x003b)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_DSS_WITH_RC4_128_SHA (0x0066)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	

6.1 Включение и отключение возможности загрузки SSL-сертификатов

Перед тем как загружать ключевую информацию в Скаут, необходимо разрешить работу подсистемы фильтрации трафика с SSL-сертификатами. Для это необходимо:

- перейти в меню Настройки › Подвление атак на вкладку Управление очистителями;
- перейти по ссылке Local Traffic Cleaner;
- активировать переключатель Загружать SSL сертификаты, чтобы включить возможность работы с ними или деактивировать переключатель в противном случае;
- нажать на кнопку Сохранить.

6.2 Управление SSL-сертификатами защищаемых web-серверов

Для управления SSL-сертификатами, необходимо перейти в меню Настройки › Подавление атак и выбрать вкладку Сертификаты SSL.

Для добавления новой пары сертификат/ключ необходимо:

- нажать на кнопку ✚ Добавить запись;
- в поле Описание ввести дополнительную информацию о сертификате и защищаемом ресурсе;
- в поле Сертификат нажать на кнопку Загрузить и указать на файл SSL-сертификата в формате PEM;
- в поле Ключ нажать на кнопку Загрузить и указать на файл секретного ключа, соответствующего SSL-сертификату в формате PEM;

- если секретный ключ защищен парольной фразой, её необходимо ввести в поле Пароль;

> ***Примечание:*** *Парольная фраза не хранится в* Скауте*. Она используется только во время загрузки ключа в защищенное хранилище.*

- в поле Домены ввести список доменных имен защищаемых web-серверов или использовать список, который прописан в сертификате, активировав переключатель Использовать домены из сертификата;
- указать префиксы защищаемых ресурсов, использующие сертификат;
- нажать на кнопку Сохранить.

В таблице используемых SSL-сертификатов в поле Применение на очистителях отражается статус загрузки: зеленый индикатор означает успешную загрузку, а красный - ошибку.

Для изменения конфигурационных параметров, связанных с загруженными сертификатами, необходимо выделить одну строку в таблице SSL-сертификатов и нажать на кнопку Редактировать в панели инструментов.

Для удаления SSL-сертификата необходимо выделить одну строку в таблице SSL-сертификатов и нажать на кнопку Удалить в панели инструментов.

6.3 Включение и отключение перехвата SSL-сессий

Активация функции перехвата SSL-сессий производится в методе фильтрации Перехват SSL для каждого задания подавления независимо. Для включения перехвата в задании подавления необходимо:

- перейти в меню Подавление атак на вкладку Задания;
- найти задание подавления, в котором необходимо изменить параметры, и нажать на мини-график для перехода к статусу задания;
- перейти в режим редактирования параметров методов фильтрации, нажав на кнопку Режим редактирования в панели управления;
- в разделе Методы активировать переключатель Перехват SSL;
- при необходимости, раскрыть секцию метода Перехват SSL и настроить параметры:

Порты - список tcp-портов защищаемых ресурсов, для которых производится перехват SSL-сессий;

Примечание: *Порты, на которых происходит перехват, должны также присутствовать в разделе Порты контрмер секции Настройки.*

Не учитывать домены SSL сертификатов:

- в выключенном состоянии:
  - перехватываются только запросы с именами серверов и IP-адресами, указанными в загруженных сертификатах;
  - запросы по заданным IP-адресам без имени сервера или с неизвестным именем пропускаются без обработки;
- во включенном состоянии:
  - перехватывается весь трафик по IP-адресам, указанным в загруженных сертификатах;
  - перехватываются запросы, идущие на доменные имена, не присутствующие в сертификате;
  - блокируется трафик web-серверов, для которых не загружены сертификаты на IP-адресах, указанных в загруженных сертификатах;

Блокировать не TLS трафик - параметр не пропускает на указанные в методе порты трафик, который не может быть перехвачен/не является шифрованным.

6.4 Получение статистики по работе метода Перехват SSL

Суммарный блокируемые методом трафик отображается на графике прямого трафика в секции Графики.

Дополнительная информация о работе метода Перехват SSL представлена графиками и таблицей, расположенными ниже параметров метода. На графиках отображается информация об отброшенном, пропущенном без обработки и перехваченном трафике. В таблице представлена статистика по текущим активным TLS-сессиям, а также число выявленных TLS-сессий за интервал просмотра детальной статистики.

7 Подавление в облаке

«Подавление в облаке» – это возможность Скаута запрашивать дополнительную поддержку при подавлении атаки путем фильтрации трафика на стороне операторского комплекса Периметр, установленного у вышестоящего провайдера.

Основной принцип работы заключается в том, что на стороне Скаута устанавливается устройство (локальная система) с возможностью очистки трафика меньшей чем на сети оператора связи (центральная система). Скаут может быть установлен в разрыв канала связи и осуществлять защиту от атак на уровень приложения или защищаемого сервиса. Получение как прямого, так и обратного потока данных позволяет использовать методы, основанные на проксировании соединений, в том числе расшифровку TLS-соединений и применение методов очистки к проксируемому HTTPS-трафику. При возникновении ситуации, когда атака превышает производительность входящих каналов связи клиента или возможности по очистке трафика локальной системы, производится запрос к операторскому комплексу Периметр (центральной системе) на перевод трафика на очистку мощностями операторского комплекса (центральной системы).

Запрос очистки на центральной системе осуществляется по протоколу UDP, что позволяет произвести отправку несмотря на загруженность каналов связи. Кроме того, Скаут может загружать на операторский комплекс черный и белый списки адресов. Эти списки будут использоваться при подавлении атаки средствами операторского комплекса.

7.1 Настройка подключения к операторскому комплексу

Скаут работает в режиме локальной системы. В ней настраиваются параметры доступа к центральной системе, параметры отправки запроса на очистку, а также передаваемые на очистку префиксы. Кроме того, локальная система позволяет загружать на центральную систему черный и белый списки, которые будут применяться в задании подавления на центральной системе.

Для настройки параметров, необходимо:

- перейти в меню Подавление атак на вкладку Облако;
- в разделе Параметры выбрать вариант Локальная система;

- если необходимо, чтобы поддержка со стороны центральной системы подключалась автоматически, если объём трафика, проходящего через Скаут, превысит определенное значение, то активировать переключатель Автоматический режим и указать порог по трафику в соответствующем поле;
- нажать на кнопку «Сохранить».

Для настройки параметров подключения к центральной системе необходимо:

- нажать на кнопку Редактировать в разделе Центральная система и заполнить форму ввода:
  - активировать переключатель Активно;
  - ввести IP-адрес центральной системы и кодовое слово в соответствующие поля
  - нажать на кнопку «Сохранить».

Состояние подключения к центральной системе, с которой осуществляется взаимодействие отображается в разделе Центральная система в поле Статус устройства.

Секция Фильтрация в облаке управлять процессом подключения и отключения защиты на центральной системе, а также загружать на неё пользовательские списки.

Кнопка Запустить позволяет отправить запрос на запуск фильтрации трафика на центральную систему. Если от центральной системы получено подтверждение, что задание подавления работает, кнопка Остановить позволяет отправить запрос на остановку фильтрации на центральной системе.

Состояние задания подавления, работающего на центральной системе, отображается в поле Статус в разделе Фильтрация в облаке.

Кнопка Редактировать позволяет изменить набор защищаемых на центральной системе префиксов.

Примечание: *Если префиксы не указаны, то на защиту на центральной системе переводятся все префиксы, разрешенные для локальной системы. Указываемые на локальной системе префиксы должны выходить в эти диапазоны разрешенных префиксов, в противном случае они будут проигнорированы.*
Количество передаваемых префиксов не может превышать 30.

Для загрузки пользовательских черного и белого списка на центральную систему необходимо нажать на кнопку Загрузить в соответствующем поле и указать файл со списком префиксов.

> ***Примечание:*** *Администратор центральной системы может заблокировать возможность загрузки пользовательских списков.*
> *Списки загружаются в режиме замены.*

Если активирован автоматический режим, то запрос на включение подавления в облаке отправляется, если трафик превышает заданный порог 80% времени на 5 минутном интервале, а автоматическая остановка подавления - если трафик не превышает заданный порог 80% времени на 10-минутном интервале.

8 Детектирование DoS-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:

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

Выявление DoS-атаки приводит к активизации механизма сбора детализированной статистики по трафику атаки, что позволяет выделять общие критерии, необходимые для успешного её подавления.

8.1 Глобальные настройки детектирования

Основными методом выявления DoS-атак в Скауте является детектирование превышения порогов трафика 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. Для того, чтобы добавить или изменить конфигурацию шаблонных пакетов, необходимо:

- перейти в меню Настройки › Детекция и выбрать вкладку Глобальные настройки;
- в разделе Шаблонные пакеты активировать переключатель Настройки для хостов наблюдаемых объектов, если он не активирован;
- нажать на кнопку Редактировать;

- для добавления нового шаблонного пакета:
  - нажать на кнопку + Добавить сигнатуру;
  - в поле Название ввести понятное имя для шаблонного пакета (будет отображаться при выявлении вектора атаки, соответствующего шаблонному пакету);
  - в поле Текущее правило ввести параметры шаблонного пакета (сигнатуру DoS-атаки);
  - нажать на кнопку Применить для добавления шаблонного пакета и возврата в список или на кнопку Отменить для возврата в список без добавления нового шаблонного пакета;
- для изменения параметров шаблонного пакета или его удаления:
  - перейти по ссылке в поле Название (доступна для изменяемых шаблонных пакетов) и изменить значения параметров, если это необходимо;
  - если необходимо удалить шаблонный пакет, нажать на кнопку Удалить;
  - если необходимо подтвердить изменения параметров, нажать на кнопку Применить;

Пороговые значения задаются индивидуально для каждого шаблонного пакета. Для получения детальной информации по управлению порогами обратитесь к разделу Пороги по трафику. Кроме пороговых значений, для каждого шаблонного пакета можно определить набор методов подавления, которые будут активироваться при выявлении вектора атаки.Управление параметрами контрмер в этом случае аналогично изменению контрмер в заданиях подавления. Для получения детальной информации обратитесь к разделу Корректировка параметров контрмер в задании подавления. Методы подавления, указанные в глобальных настройках шаблонных пакетов, применяются для всех наблюдаемых объектов, при условии, что для них не определены индивидуальные настройки подавления.

8.2 Пороги по трафику

Список шаблонных пакетов содержит информацию об используемых порогах по трафику. Выявление вектора атаки происходит при превышении заданного порога и выполнении дополнительных условий, задаваемых настройками детектирования:

- Отсрочка обнаружения — время в секундах, в течении которого трафик должен превышать пороговое значение;
- Отсрочка закрытия — время в секундах, в течении которого вектор атаки продолжает считаться открытым, даже при отсутствии превышения порога;
- Быстрое обнаружение — если трафик превышает порог в заданное количество раз, то параметр Отсрочка обнаружения игнорируется и сразу происходит выявление вектора атаки.

Для получения доступа к управлению порогами, необходимо щелкнуть на строке шаблонного пакета, для которого необходимо изменить настройки. В результате будет развернута форма с элементами управления, соответствующим полям таблицы шаблонных пакетов

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:

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

Выбор способа задания порога осуществляется путем изменения значения выпадающего списка в соответствующей группе элементов управления:

- Порог — используются статические пороги;
- Автопорог — используются автоматически рассчитываемые пороги;
- Выключено — детектирование не производится.

При необходимости анализа и детектирования векторов атак на трафике, исходящем от наблюдаемого объекта (защищаемого ресурса), необходимо активировать переключатель Мониторинг исходящего трафика.

Статические пороги

Включение использования статических порогов производится путем указания значения Порог в выпадающем списке. 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.

Динамические пороги

Включение использования динамических порогов производится путем указания значения Автопорог в выпадающем списке. В режиме динамических порогов доступна ссылка ⚙ Настроить, перейдя по которой можно настроить статистические параметры определения динамических порогов:

- 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).

При просмотре или установке индивидуальных порогов в настройках наблюдаемого объекта, в окне настроек отображается график максимальных значений трафика, что позволяет оценить характер трафика и величину рассчитываемого порога и оперативно изменить параметры при необходимости..

8.3 Шаблоны настроек детектирования

Скаут позволяет хранить настройки детекторов по шаблонным пакетам и профилям поведения в виде шаблонов настроек детектирования. Для управления шаблонами необходимо перейти в меню Настройки › Детекция на вкладку Шаблоны настроек детектирования.

Для добавления нового шаблона необходимо нажать на кнопку ✚ Добавить шаблон и выбрать тип создаваемого шаблона:

- По профилю поведения — используется в одноименном разделе настроек детектирования наблюдаемого объекта или в глобальных настройках детектирования атак;
- По шаблонным пакетам для хостов наблюдаемых объектов — используется в одноименном разделе настроек детектирования наблюдаемого объекта или в глобальных настройках детектирования атак;
- По шаблонным пакетам для хостов, не относящихся к наблюдаемым объектам — используется в одноименном разделе глобальных настроек детектирования атак.

Настройки для детектирования по шаблонным пакетам подразумевают установку пороговых значений. Детальная информация об установке порогов по трафику представлена в разделе Пороги по трафику.

Шаблон настроек детектирования может быть применен к наблюдаемому объекту. Детальная информация о связывании шаблона настроек детектирования и наблюдаемого объекта приведена в разделе Создание профиля.

Примечание: *Загрузка настроек из шаблона создает связь между шаблоном и профилем. Изменения, сделанные в шаблоне будут применены ко всем связанным профилям. Связь будет действовать до тех пор, пока вручную не будет внесено хотя бы одно изменение в настройки параметров детектирования в профиле.*
Методы подавления не входят в шаблон настроек детектирования и определяются на глобальном уровне или на уровне индивидуального профиля. В шаблоне присутствует возможность разрешить или запретить автоматическое подавление выявленного вектора атаки, используя переключатель Разрешить подавление.

Для совершения действий с существующим шаблонами, необходимо отметить флагом в ловом столбце одну или несколько строк. Возможные действия отображаются в виде кнопок над таблицей:

- Редактировать — изменить параметры шаблона;
- Копировать — создать новый шаблон на основе выделенного;
- Удалить — удалить выделенные шаблоны из базы данных;
- Редактировать группу шаблонов — задать параметры для выделенных шаблонов.

Доступ к форме редактирования шаблона осуществляется также путем перехода по ссылке в столбце Название.

8.4 Профили

Для того, чтобы выделить из всего трафика необходимую часть, например, выделить трафик защищаемого ресурса или нескольких ресурсов, используются наблюдаемые объекты (далее Профили). К каждому профилю могут быть применены индивидуальные настройки детектирования Dos-атак, либо профиль может использовать настройки заданные глобально. Для профиля может быть определен индивидуальный шаблон подавления атак, учитывающий особенности трафика, соответствующего профилю. Профиль можно поставить в соответствие группе пользователей с ограниченными правами, организовав, таким образом, личные кабинеты пользователей.

8.4.1 Создание профиля

Для создания наблюдаемого объекта Профиль, необходимо:

- перейти в меню Настройки › Мониторинг и выбрать вкладку Наблюдаемые объекты › Профили;
- нажать на кнопку ✚ Добавить объект, расположенную в правой части над таблицей профилей;
- на вкладке Описание ввести наименование профиля в поле Название;
- на вкладке Конфигурация:
  - выбрать в выпадающем списке Фильтр1 значение IP-префиксы;
  - в поле Значение фильтра ввести IP-префиксы защищаемых ресурсов;
- на вкладке Детекция в разделе Настройки детектирования в выпадающем списке По шаблонным пакетам выбрать вариант Всегда

включено для задания индивидуальных настроек детектирования атак, либо вариант По умолчанию (использовать глобальные настройки), если детектирование будет осуществляться согласно настройкам для хостов наблюдаемых объектов секции Шаблонные пакеты, расположенным на вкладке Глобальные настройки меню Настройки › Детекция;

- если выбран вариант Всегда включено:
  - нажать на кнопку Редактировать для перехода к настройке профиля детектирования атак;
  - выбрать профиль детектирования, нажав на кнопку Загрузить из шаблона выбрав в выпадающем списке один из шаблонов настройки методов;

Примечание: *Загрузка настроек из шаблона создает связь между шаблоном и профилем. Изменения, сделанные в шаблоне будут применены ко всем связанным профилям. Связь будет действовать до тех пор, пока вручную не будет внесено хотя бы одно изменение в настройки параметров детектирования в профиле.*

По умолчанию, для каждого вида шаблонных пакетов предусмотрены методы подавления, определенные на глобальном уровне. Эти методы будут действовать сразу после включения детектирования и разрешения подавления атаки с помощью переключателя Методы подавления, расположенного в одноименном поле.

  - при необходимости, внести изменения в настройки профиля детектирования, например, изменить пороговые значения или включить/отключить детектирование для какой-либо сигнатуры DoS-атак;
  - добавить индивидуальные настройки подавления атак в разделе Методы подавления, используя кнопку Настроить;

Примечание: *Настроенные методы будут автоматически подключаться при выявлении атаки с выбранным вектором, если такое подключение разрешено в шаблоне настроек методов, используемом в задании подавления.*

  - нажать на кнопку Сохранить для выхода из режима редактирования настроек детектирования по шаблонным пакетам с сохранением сделанных изменений и возврата к настройкам профиля;
  - перейти на вкладку Подавление атак:

1. выбрать Шаблон настроек подключения очистителей, используя соответствующую кнопку;
2. нажать на кнопку ✚ Выбрать в поле Шаблон методов фильтрации и выбрать из списка политику защиты, которая будет применяться при создании нового автоматического задания подавления;
3. если необходимо подключать дополнительные методы защиты при выявлении атаки или автоматически создавать задания подавления, активировать переключатели Разрешить автоматическое подавление атак и Объединять атаки в одно задание фильтрации;
   - нажать на кнопку Сохранить для применения изменений.

8.4.2 Удаление профиля

Для удаления наблюдаемого объекта, необходимо перейти в меню Настройки › Мониторинг на вкладку Наблюдаемые объекты › Профили, отметить профили, которые необходимо удалить, с помощью флагов и нажать на кнопку 🗑 Удалить. Для подтверждения удаления необходимо нажать на кнопку Продолжить.

8.5 Просмотр выявленных DoS-атак

Выявленные Скаутом DoS-атаки сохраняются в меню Аномалии. Активные атаки отображаются на вкладке Текущие DoS-атаки, а завершенные - на вкладке Прошедшие DoS-атаки.

В верхней части вкладки располагается блок параметров фильтрации, ограничивающий список отображающихся атак. При изменении фильтра обновление списка атак происходит автоматически.

Список DoS-атак представляет собой таблицу, содержащую основные параметры атаки. Таблица имеет настраиваемое с помощью кнопки ☰ содержимое:

ID:	уникальный числовой идентификатор атаки для быстрого поиска и идентификации;
Трафик:	схематичное графическое представление трафика атаки (мини-график);
Ресурс:	атакуемый профиль и(или) IP-адрес;
Влияние:	сумма входящего и исходящего трафика профиля во время атаки;

Класс опасности:	тег, присваиваемый системой в зависимости от относительной величины превышения текущего трафика над пороговым значением (может быть изменен пользователем);
Время создания:	дата и время выявления атаки;
Длительность:	время активности атаки;
DoS-сигнатуры:	выявленные векторы атаки и максимальные значения трафика по ним в абсолютных и относительных величинах.

Для просмотра детализированной статистики, необходимо выполнить щелчок левой кнопки мыши на значение в поле ID или на мини-графике. При этом, кроме указанной выше информации, становится доступен детализированный график трафика во время атаки в разрезе выявленных векторов, а также расширенная статистика по каждому вектору атаки, включающая следующие характеристики:

Источники:	IP-адреса источников, вносящих наибольший вес в трафик;
Получатели:	IP-адреса получателей, на которых направлен трафик;
Страны источника:	страны, которые вносят наибольший вес в трафик;
Страны получателя:	страны, в которых направлен трафик;
Размеры пакетов:	наиболее часто встречающиеся размеры пакетов (усредненные значения);
Протокол/порт источника:	наименование или номер протоколов транспортного уровня, вносящих наибольший вес в трафик, а также номера портов, с которых этот трафик отправлялся, если это применимо к протоколу;
Протокол/порт получателя:	наименование или номер протоколов транспортного уровня, вносящих наибольший вес в трафик, а также номера портов, на которые этот трафик отправлялся, если это применимо к протоколу;
BGP ASN источника:	origin ASN, вносящие наибольший вест в трафик;
BGP ASN получателя:	origin ASN, на которые направлен трафик с наибольшим весом;

TCP-флаги:	наборы флагов протокола TCP, наиболее часто встречающиеся в потоках данных;
Интерфейсы, входящие:	информация о сетевых интерфейсах, на которые приходит трафик атаки;
Интерфейсы, исходящие:	информация о сетевых интерфейсах, через которые выходит трафик атаки;

Примечание: *Если выявить отдельные элементы не удается, отображается одна строка Разные.*

Элементы, имеющие вес менее 10%, агрегируются и отображаются одной строкой Прочие.

Детализированная статистика по вектору атаки начинает собираться и накапливаться с момента выявления вектора атаки, поэтому она будет отсутствовать непосредственно после выявления атаки. Для коротких атак (меньше 3-х минут) или для импульсных атак, в которых векторы атаки активны короткий промежуток времени, она может отсутствовать даже после завершения атаки.

Во время атаки блоки детализированной статистики периодически обновляются и отображают актуальную информацию. После завершения атаки в блоках отображаются срезы с максимальным трафиком, зафиксированные во время атаки. Такие же срезы формируются каждый час для длительных атак.

Детализированный график позволяет просмотреть информацию о трафике в разрезе векторов атак при наведении на него курсора мыши.

Щелчок левой кнопкой мыши фиксирует момент времени, после чего в блоках детализированной статистики отображается информация на этот момент времени, если он присутствует в базе данных.

На основе детализированной статистики по атаке может быть сформирован отчет по запросу пользователя. Для получения отчета, необходим нажать на кнопку Экспорт отчета и выбрать один из предлагаемых форматов. Отчет будет сформирован и загружен в браузер.

Изменение характера трафика во время атаки приводит к появлению или закрытию векторов атак. Эти изменения, а также действия пользователя

журналируются в соответствующем разделе. Последние 10 записей журнала отображаются на экране.

9 Уведомления

Скаут имеет возможность отправлять уведомления о наступлении различных событий, например, выявлении DoS-атак, а также периодически информировать о состоянии защищаемых ресурсов путем отправки почтовых уведомлений, отправки сообщений на удаленный сервер, используя протокол syslog или в виде snmp trap.

9.1 Настройка параметров взаимодействия с почтовым сервером

Для настройки параметров почтового сервера, через который будет осуществляться отправка почтовых уведомлений, необходимо:

- перейти в меню Настройки › Уведомления;
- на вкладке Глобальные настройки заполнить следующие поля:

SMTP-сервер:	IPv4 адрес или FQDN сервера, через который будет отправляться электронная почта;
SMTP-адрес источника:	адрес электронной почты, от имени которого будут отправляться почтовые уведомления;
SMTP-имя пользователя:	логин пользователя для аутентификации на почтовом сервере;
Подпись	текст, добавляемый к отправляемому сообщению.

Примечание: *При использовании аутентификации с паролем на почтовом сервере, необходимо активировать переключатель Использовать SMTP-пароль. При этом становятся доступны поля SMTP-пароль и SMTP-подтверждение пароля, в которые необходимо ввести пароль пользователя, соответствующий логину на почтовом сервере.*

- подтвердить изменение настроек нажатием на кнопку Сохранить

9.2 Группы отправки почтовых сообщений

Уведомления могут быть направлены одному или более получателю. Список получателей составляет группу отправки почтовых сообщений.

Для управления группами отправки почтовых сообщений, необходимо перейти в меню Настройки › Уведомления на вкладку Группы. Скаут поставляется с одной группой отправки По умолчанию/Default, которая используется для отправки всех сообщений, включая системные.

Для добавления новой группы отправки сообщений, необходимо:

- нажать на кнопку ✚ Добавить группу;
- ввести название создаваемой группы в соответствующее поле;
- активировать переключатель Отправлять по e-mail;
- ввести в поле Адреса электронной почты список e-mail получателей сообщений, разделенных запятой;
- подтвердить добавление группы нажатием на кнопку Добавить группу.

Удаление и редактирование осуществляется путем выделения групп(ы) с помощью флага и выбора необходимой операции в панели инструментов над таблицей.

9.3 Правила отправки почтовых сообщений

Правила отправки почтовых сообщений определяют какая информация должна отправляться на адреса, указанные в группе уведомлений, и с какой периодичностью должна производится отправка сообщений. Для того, чтобы определить правила отправки почтовых сообщений, необходимо перейти в меню Настройки › Уведомления на вкладку Правила.

Для добавления нового правила, необходимо:

- нажать на кнопку ✚ Добавить запись;
- выбрать тип уведомления из списка Вид отчета:

Dos-отчет:	комплексный отчет об аномалиях, необходимо выбрать объект Профиль, информация которого будет включена в уведомление;
События:	информация о событиях (типы событий могут быть указаны в соответствующем поле) системы в целом или профиля (DoS-атаки не входят в отчет);
DoS-атаки:	информация о DoS-атаках, в зависимости от периода отправки может формироваться список атак за период или отправляться отдельное уведомление при начале и завершении атаки (период отправки «Мгновенно»);

Задание подавления:	информация о проходящем через подсистему очистки трафике и работе контрмер;
Отчет по трафику:	информация из аналитической подсистемы;

- настроить параметры фильтрации для выбранного типа отчета:

Наблюдаемый объект:	объект Профиль, для которого будет отправляться уведомление;
Тип:	типы и подтипы событий,которые будут включаться в уведомление;
Детальная статистика:	в отчеты DoS-атаки и(или) Задание подавления будет включена детализированная информация о трафике атаки или работе контрмер;

Примечание: *Одно правило уведомлений может содержать до 10 отчетов. Из них будет сформирован документ, содержащий все запрашиваемые отчеты. Для добавления и удаления отчетов в правило необходимо использовать соответствующие кнопки Добавить отчет и Удалить отчет.*

- выбрать используемую группу уведомлений, нажав на кнопку + Выбрать или создать новую группу, нажав на кнопку Добавить группу;
- выбрать формат отправляемых сообщений: html будет отправлен непосредственно в теле сообщения, а остальные форматы - в виде вложений;
- указать период отправки (типы отчетов DoS-отчет и Отчет по трафику не поддерживают вариант Мгновенно)
- установить переключатель Отправить пустой, если нужно отправлять периодические отчеты даже в том случае, если они не содержат информации;
- подтвердить создание правила, нажав на кнопку Добавить правило.

Для изменения параметров правила, необходимо отметить правило и нажать на кнопку Редактировать в панели инструментов.

После создания или изменения параметров правила, можно выполнить проверку отправки письма, используя кнопку Отправить сейчас.

9.4 Отправка сообщений на внешний syslog-сервер

Скаут может отправлять сообщения на внешние серверы, поддерживающие протокол syslog. Сообщения имеют стандартную нотацию CEF или LEEF, что позволяет принимать их в различных системах без необходимости подключения внешних коннекторов.

Для добавления правила отправки сообщений syslog необходимо:

- перейти в меню Настройки › Уведомления на вкладку Настройка серверов syslog;
- нажать на кнопку ✚ Добавить запись;
- заполнить обязательные параметры коллектора syslog-сообщений:

Имя коллектора:	наименование, использующееся для идентификации коллектора в Скауте;
IP-адрес:	IPv4 адрес коллектора, на который будут направляться сообщения;
Порт:	tcp/udp порт, на котором коллектор принимает сообщения (обычно используется порт по умолчанию 514);

- разрешить отправку сообщений, активировав переключатель Отправка;
- подтвердить создание правило, нажав на кнопку Применить.

Для изменения параметров правила отправки сообщений syslog, необходимо выделить правило и нажать на кнопку Редактировать, а для удаления правила - нажать на кнопку Удалить.

Для каждого правила можно задать список разрешенных к отправке сообщений, используя поле Список кодов сообщений для отправки. Значение Персональный, позволяет указать разрешенные коды сообщений, а значение Общий использует список разрешенных сообщений, определенный на уровне всей системы.

Для указания сообщений, разрешенных к отправке на уровне системы, необходимо нажать на кнопку Глобальный список кодов сообщений для отправки, находящуюся на вкладке Настройка серверов syslog в меню Настройки › Уведомления и переместить разрешенные типы сообщений в правое окно.

10 Безопасность и управление доступом

Скаут использует ролевую модель управления доступом к отдельным функциональным блокам, основанную на группах пользователей. Учетная запись пользователя входит в определенную группу. Для группы задаются параметры доступа к функциональным блокам Скаута.

10.1 Создание новой учетной записи и предоставление ей прав доступа

Перед созданием учетной записи пользователя, необходимо убедиться, что в Скауте существует группа пользователей с необходимым набором прав доступа. Если такой группы не существует, её необходимо создать и настроить в ней необходимые права доступа (см. разделы Группы пользователей и Настройка прав доступа для группы пользователей).

Для создания новой учетной записи пользователя, необходимо перейти в меню Настройки › Доступ и выбрать вкладку Пользователи. В форме Новый пользователь необходимо заполнить обязательные поля, отмеченные символом * и нажать на кнопку Сохранить.

Пароль для создаваемой учетной записи может быть введен вручную или сгенерирован системой при нажатии на кнопку Сгенерировать пароль. Если оставить поле пустым (не использовать кнопку Сгенерировать пароль и не заполнять поле вручную), то Скаут самостоятельно сгенерирует пароль.

Примечание: *Пароли, генерируемые системой автоматически, являются одноразовыми и отправляются на электронную почту пользователя, указанную в поле Адрес электронной почты. Одноразовый пароль должен быть изменен пользователем при первом входе в интерфейс управления.*

Пароли генерируемые по запросу пользователя или введенные вручную не являются одноразовыми и не отправляются на электронную почту пользователя.

10.2 Настройка прав доступа для группы пользователей

Каждой группе пользователей можно представить доступ, используя именованные наборы прав доступа. Каждый набор прав доступа в Скауте

определяет функциональные блоки, к которым будет иметь доступ группа пользователей. Для настройки прав доступа, необходимо:

- перейти в меню Настройки › Доступ на вкладку Права доступа;
- если необходимо отредактировать существующий набор прав, то выделить строку для редактирования в списке наборов прав доступа;
- если необходимо создать новый набор прав доступа, то нажать на кнопку ✚ Добавить, ввести название набора прав на русско и английском языках и нажать на кнопку Сохранить;
- отметить флагами функциональные блоки, которые должны быть доступны и снять флаги у тех функциональных блоков, к которым не должно быть доступа;
- нажать на кнопку Сохранить, расположенную ниже структуры функциональных блоков.

10.3 Группы пользователей

Группы пользователей вместе с наборами прав доступа формируют ролевую модель управления доступом в Скауте. Одну и ту же группу пользователей могут использовать множество учетных записей пользователей. В этом случае они получают одинаковый набор прав доступа.

Скаут поставляется с одной встроенной группой Администратор системы, пользователи которой имеют полный доступ ко всем функциям.

Администратор может создать произвольное число пользовательских групп и назначить для них необходимые права доступа.

Изменить настройки существующей группы или добавить новую группу можно на вкладке Группы в меню Настройки › Доступ.

Добавление группы пользователей

Для добавления новой группы пользователей, необходимо:

- нажать на кнопку ✚ Добавить группу;
- на вкладке Описание указать название группы в соответствующем поле;
- на вкладке Права: - указать максимальное число пользователей в группе, если это необходимо; - выбрать тип пользователей, которые будут включаться в группу:

Обычный:	пользователи имеют доступ ко всем объектам Скаута и только к тем функциональным блокам, которые определены в разрешенных к использованию наборах прав доступа;
Ограниченный:	пользователи имеют доступ только к указанному в настройках группы профилю, имеют ограниченные привилегии для использованию подсистемы очистки трафика и имеют доступ только к тем функциональным блокам, которые определены в разрешенных к использованию наборах прав доступа для групп ограниченных пользователей;

- отметить наборы прав доступа, которые будет использовать группа и установить дополнительные ограничения, если это необходимо;
- подтвердить создание группы, нажав на кнопку Сохранить.

Изменение параметров группы пользователей

Чтобы изменить параметры группы пользователей, необходимо:

- отметить строку с группой, параметры которой необходимо отредактировать;
- нажать на кнопку Редактировать в панели инструментов;
- внести необходимые правки и подтвердить изменение нажатием кнопки Сохранить.

Примечание: *Редактировать параметры встроенных групп пользователей нельзя.*

Удаление группы пользователей

Чтобы удалить существующую группу, необходимо:

- отметить строку с группой, параметры которой необходимо удалить;
- нажать на кнопку Удалить в панели инструментов; подтвердить удаление, нажав на кнопку Продолжить.

10.4 Ограничение доступа к интерфейсу управления

Доступ к веб-интерфейсу может быть ограничен на сетевом уровне. Для этого необходимо перейти на вкладку Сетевые подключения › Ограничение доступа к порталу в меню Настройки › Доступ.

В соответствующих полях ввода необходимо задать разрешенные и(или) запрещенные префиксы, доступ с которых будет разрешен или заблокирован.

Поддерживаются два режима управления доступом:

- Черный список — запрет доступа к графическому интерфейсу пользователя с IPv4 адресов, входящих в префиксы списка, при условии отсутствия более специфичного префикса в «белом списке»;
- Белый список — разрешение доступа к графическому интерфейсу пользователя с IPv4 адресов, входящих в префиксы списка, даже при условии присутствия менее специфичных префиксов в «черном списке».

Изменения, вносимые в список, необходимо в обязательном порядке подтверждать нажатием кнопки «Сохранить», находящейся в том же разделе страницы. В противном случае, они не будут применены.

Примечание: *В каждой строке списка после указания IP-префикса допустимо указывать однострочный комментарий, начинающийся с символа # и отделенный от IP-префикса как минимум одним пробелом.*

10.5 Контроль сетевых подключений

Скаут позволяет контролировать трафик на интерфейсе управления и создавать событие, если выявляется трафик, не соответствующий правилам. Это необходимо для выявления попыток несанкционированного доступа к Скауту.

Внимание: *Данная функциональность не связана с фильтрацией непосредственно сетевого трафика. Подключения, для которых нет правил заносятся в журнал и приводят к генерации аномалий. Пакеты не блокируются.*

Для создания правила, необходимо:

- перейти в меню Настройки › Доступ на вкладку Сетевые подключения -> Фильтры;

- нажать на кнопку ✚ Добавить запись;
- заполнить поля формы и нажать на кнопку Сохранить.

Для просмотра журнала соединений, необходимо перейти в меню Настройки › Доступ на кладку Сетевые подключения › Журнал. Если какие-то из подключений не нуждаются в логировании, можно создать правило, выделив строку таблицы и нажав на кнопку Создать правило.

11 Работа с аналитическими отчетами

Отчёты аналитической подсистемы Скаута обеспечивают пользователя информацией, позволяющей принимать обоснованные решения в вопросах подавления атак, управления пропускной способностью контролируемой СПД и т.д. Под термином "отчёт" подразумевается страница веб-интерфейса в меню Отчеты, содержащая необходимую статистическую информацию, собранную в процессе работы Скаут.

Минимальное разрешение отчетов аналитической подсистемы Скаута составляет 5 минут. Т.е. каждый 5 минут заполняются необходимые отчеты, в них появляется один новый временной отсчет.

Каждый отсчет в аналитическом отчете представляет собой ранжированный список данных определенной длины (количество строк списка, записываемый каждые 5 минут, разное и зависит от вида отчета). Т.о., в отчет всегда попадают только те данные, которые вносят наибольший вклад в отчет с точки зрения объема и количества трафика. Данные с небольшим объемом и количеством трафика могут не записываться в отчет из-за того, что они находятся слишком далеко от начала ранжированного списка и не входят в размер записываемого в отчет блока. Такое поведение связано с:

a) ограниченным размером подсистемы хранения аналитических отчетов;

b) необходимостью записать все данные в подсистему хранения аналитических отчетов за фиксированное время, которое не должно превышать разрешение в отчетах (5 минут).

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. Поэтому, отчет, построенный непосредственно после поступления данных в аналитическую подсистему, будет иметь значительно большее разрешение (детализацию), чем тот же самый отчет за тот же самый временной интервал, но построенный, например, через месяц от момента построения первоначального отчета.

Элементы управления на страницах отчётов

Вид и параметры выводимого отчёта могут быть настроены пользователем.

На странице отчёта выделяют следующие элементы управления:

- инструменты выбора данных для отчёта;

- графическое отображение отчетной информации;
- табличное представление отчетной информации;
- дополнительные элементы управление.

Примечание: *в случае возникновения непонимания по предоставляемой информации в отчете - необходимо обратиться к разделу подсказки, расположенному в верхней части страницы.*

Меню выбора отчета

Собираемые 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).

Каждая группа представлена отдельным пунктом выпадающего меню, расположенного в верхней части рабочей области экрана, для доступа к которому необходимо перейти в меню Отчеты.

Для доступа к конкретному отчету, необходимо открыть выпадающее меню и выбрать интересующий пункт. Отчеты разделены на следующие 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;
- По объектам › Профили – входящий и исходящий трафик с разбивкой по наблюдаемым объектам (профилям);
- Размер пакетов – входящий и исходящий трафик с разбивкой по размерам IP-пакетов;
- Протоколы – входящий и исходящий трафик с разбивкой по протоколам транспортного уровня;
- QoS – входящий и исходящий трафик с разбивкой по типам сервиса в различных нотациях (TOS, DTRM, IP Precedence, DSCP);
- География IP – трафик с разбивкой по географическим признакам источника и получателя (Страны, Регионы, Города);

- 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).

Панель информации об отчете

Информационная панель, расположенная в верхней части рабочей области непосредственно под меню выбора отчета кроме названия выбранного отчета содержит расширенную информацию об отчете. Для получения этой информации, необходимо подвести курсор мыши к пиктограмме  и дождаться появления всплывающей подсказки.

Пиктограмма  позволяет добавить отчет в список избранных отчетов, который доступен пользователю после перехода по ссылке Избранные, расположенной справа от пиктограммы. Избранные отчеты отображаются во всплывающем окне.

В панели также присутствует кнопка Экспорт отчета. Щелчок левой кнопкой мыши открывает всплывающее окно выбора формата экспорта:

- PDF;
- CSF;
- Excel;
- XML;
- Отправлять на e-mail.

Вариант отправки на электронную почту подразумевает подписку пользователя не периодическую рассылку отчета с выбранными на момент подписки параметрами. Отчеты высылается на адрес электронной почты пользователя. Подписки могут быть отменены в том же меню с помощью кнопки Отписаться. Для немедленной отправки отчета, необходимо воспользоваться кнопкой Отправить сейчас.

Панель информации содержит также переключатель вида макета отчета:

- табличный вид — графическая и табличная часть отчета располагаются рядом в одной строке;
- вид списка — табличная часть отчета располагается ниже графической части.

Примечание: *Вид макета влияет только на отображение отчета в веб-интерфейсе. При экспорте вид макета не учитывается.*

Панель выбора параметров отчёта

Панель Фильтры предоставляет пользователю средства управления параметрами выводимого отчёта. Пользователь определяет единицы измерения трафика в отчёте, период выводимых данных, а также дополнительные критерии фильтрации. Панель Фильтры отображается в верхней части рабочей области страницы отчёта.

Панель фильтров содержит параметр Автоматический поиск при изменении фильтра, расположенный в разделе Параметры поиска (кнопка ☰). Если флаг не активен, то после задания нужных параметров на панели Фильтры, необходимо нажать на кнопку Найти для отправки запроса на построение отчета. В противном случае, запрос на построение отчета отправляется сразу после изменения одного из параметров на панели Фильтры, а кнопка Найти на экране не отображается.

Установленный фильтр может быть отменен нажатием на кнопку Сбросить фильтр.

Примечание: *Набор доступных элементов управления параметрами отчёта зависит от выбранного отчёта и может отличаться в зависимости от выбранного отчета.*

Выбор типа усреднения данных

Во многих отчетах существует возможность отображения данных в таблице с различным усреднением:

- Текущий - отображается трафик последнего записанного в аналитическую подсистему отсчета;
- Средний - отображается усредненный по методу среднего арифметического трафик за выбранный интервал;
- Максимальный - отображается максимальный трафик на выбранном интервале;
- PCT95 - отображается трафик, соответствующий 95-му процентилю на выбранном интервале.

Выбор типа усреднения производится путем указания необходимого варианта в выпадающем списке, расположенном над таблицей с данными о трафике.

Работа с графиком

Графическое представление трафика в отчете позволяет оценить распределение трафика по времени на заданном в параметрах отчета интервале.

Данные для отображения на графике берутся из таблицы отчета. Каждая строка таблицы соответствует двум рядам данных на графике (входящий и исходящий трафик) для всех отчетов за исключением суммарных. На суммарных отчетах каждая строка таблицы соответствует одному ряду данных на графике.

На график можно добавить до 20 строк таблицы. Отображаемые ряды данных переносятся в верхнюю таблицу и строке присваивается маркер, цвет которого соответствует цвету на графике.

Чтобы добавить или удалить строку с графика, необходимо щелкнуть левой кнопкой мыши по строке таблицы, которую необходимо удалить или добавить.

На графике можно быстро просмотреть отдельный ряд данных. Для этого необходимо навести курсор мыши на описание ряда данных в легенде. Ряд будет выделен заливкой, а остальные ряды данных будут отображаться без заливки.

На графике можно временно отключить отображение отдельных рядов данных. Для этого необходимо щелкнуть левой кнопкой мыши на описании ряда данных в легенде. Описание в легенде для выключенных рядов данных будет отмечено серым цветом. повторный щелчок приведет к отображению ряда данных на графике.

Управление масштабированием доступно посредством соответствующих пиктограмм или путем выделения части графика мышью.

11.1 Группа отчетов Состояние сети

Группа отчетов Состояние сети содержит отчеты по всему трафику, проходящему через Систему.

Общая информация об аналитических отчетах приведена в разделе Работа с аналитическими отчетами.

Суммарный отчет

Отчёт показывает трафик, проходящий через Систему за выбранный интервал времени, с разбивкой по типам: входящий, исходящий, отброшенный, multicast и суммарное количество трафика проходящего через Систему (Всего).

Для каждого типа трафика в таблице показывается текущее, среднее и максимальное значения, а также значение 95-го процентиля за интервал построения отчета.

Приложения › Все

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по приложениям. Под приложением понимается порт tcp/udp или код и тип сообщения icmp.

Существует возможность ограничить список отображаемых портов в блоке фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › ICMP

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по парам ICMP-типов и ICMP-кодов, формирующих ICMP-сообщение.

Существует возможность ограничить список отображаемых ICMP-сообщений в блоке расширенной фильтрации, указав перечисление или диапазон числовых идентификаторов типов ICMP, либо указав текстовое наименование ICMP-сообщения (например, echo или echo reply), а также дополнительно ограничить версию протокола ICMP (ICMPv4 или ICMPv6).

Приложения › TCP

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по IPv4 TCP-приложениям. Под приложением понимается порт tcp.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › UDP

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по IPv4 UDP-приложениям. Под приложением понимается порт udp.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › IPv6 › TCP

Отчёт показывает входящий и исходящий IPv6-трафик, проходящий через Систему, с разбивкой по TCP IPv6-приложениям. Под приложением понимается порт tcp.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › IPv6 › UDP

Отчёт показывает входящий и исходящий IPv6-трафик, проходящий через Систему, с разбивкой по UDP IPv6-приложениям. Под приложением понимается порт udp.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

По объектам › Профили

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по наблюдаемым объектам (профилям). Направление трафика в отчете относится к Системе: входящий трафик – это трафик, прошедший через Систему в прямом направлении, а исходящий – в обратном направлении.

Существует возможность ограничить список отображаемых профилей в блоке расширенной фильтрации, выбрав необходимые профили через соответствующий селектор наблюдаемых объектов.

Размеры пакетов

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по размерам пакетов.

Существует возможность ограничить список отображаемых размеров пакетов в блоке расширенной фильтрации, указав перечисление или диапазон размеров пакетов.

Протоколы

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по протоколам.

Существует возможность ограничить список отображаемых протоколов в блоке расширенной фильтрации, указав перечисление или диапазон протоколов. При перечислении допускается использовать символические обозначения протоколов: tcp, udp, icmp и т.д.

QoS › Тип сервиса

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по типам обслуживания (ToS).

Существует возможность ограничить список отображаемых кодов ToS в блоке расширенной фильтрации, указав их перечисление или задав диапазон.

QoS › Тип сервиса (DTRM)

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по типам обслуживания в нотации DTRM (3-6 биты поля ToS). Нотация DTRM определяет следующие типы сервиса:

D - минимальная задержка;

T - максимальная пропускная способность;

R - максимальная надежность;

M - минимальная стоимость.

Существует возможность ограничить список отображаемых кодов ToS в блоке расширенной фильтрации, указав их перечисление или задав диапазон. допускается использование символов D, T, R, M при перечислении.

QoS › IP Precedence

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по важности датаграммы (IP Precedence).

Существует возможность ограничить список отображаемых кодов IP Precedence в блоке расширенной фильтрации, указав их перечисление (десятичные значения) или задав диапазон.

QoS › DSCP

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по значениям DSCP.

Существует возможность ограничить список отображаемых значений DSCP в блоке расширенной фильтрации, указав их перечисление (десятичные значения) или задав диапазон.

Суммарный отчет IPv6

Отчёт показывает трафик протокола IPv6, проходящий через Систему за выбранный интервал времени, с разбивкой по типам: входящий, исходящий, отброшенный, multicast и суммарное количество трафика проходящего через Систему (Всего).

Для каждого типа трафика в таблице показывается текущее, среднее и максимальное значения за интервал построения отчета.

Прогноз IPv6

Отчет показывает трафик протокола IPv6, проходящий через Систему, и прогноз (линейный тренд) по трафику протокола IPv6 на заданный период времени. Отчет содержит таблицу с информацией о текущем, среднем и максимальном трафике, а также оценку трафика через 1 год, 2 года и 5 лет.

География IP › Страны

Отчет показывает трафик, проходящий через Систему, с разбивкой по странам источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются страны для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по странам:

- В страну в сеть – страна получателя трафика, трафик в сторону защищаемых ресурсов;
- В страну из сети – страна получателя трафика, трафик исходящий со стороны защищаемых ресурсов;
- Из страны в сеть – страна источника трафика. трафик в сторону защищаемых ресурсов;
- Из страны из сети – страна источника трафика, трафик исходящий со стороны защищаемых ресурсов.

Существует возможность ограничить список отображаемых стран в блоке расширенной фильтрации, выбрав необходимые страны через соответствующий селектор.

География IP › Регионы

Отчет показывает трафик, проходящий через Систему, с разбивкой по паре страна и регион источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются регионы для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по регионам:

- В регион в сеть – страна и регион получателя трафика, трафик в сторону защищаемых ресурсов;
- В регион из сети – страна и регион получателя трафика, трафик исходящий со стороны защищаемых ресурсов;
- Из региона в сеть – страна и регион источника трафика. трафик в сторону защищаемых ресурсов;
- Из региона из сети – страна и регион источника трафика, трафик исходящий со стороны защищаемых ресурсов.

Существует возможность ограничить список отображаемых стран и(или) регионов в блоке расширенной фильтрации, выбрав необходимые параметры через соответствующие селекторы.

География IP › Города

Отчет показывает трафик, проходящий через Систему, с разбивкой по составному ключу, состоящему из страны, региона и города источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются города для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по городам:

- В город в сеть – страна, регион и город получателя трафика, трафик в сторону защищаемых ресурсов;
- В город из сети – страна, регион и город получателя трафика, трафик исходящий со стороны защищаемых ресурсов;
- Из города в сеть – страна, регион и город источника трафика. трафик в сторону защищаемых ресурсов;
- Из города из сети – страна, регион и город источника трафика, трафик исходящий со стороны защищаемых ресурсов.

Существует возможность ограничить список отображаемых стран, регионов и(или) городов в блоке расширенной фильтрации, выбрав необходимые параметры через соответствующие селекторы.

11.2 Группа отчетов Профиль

Группа отчетов Профиль содержит отчеты по трафику, соответствующему наблюдаемому объекту (Профилю).

Трафик в группе отчетов Профиль всегда показывается по отношению к профилю: входящий трафик – это трафик, у которого адреса получателей соответствуют заданным в профиле, а исходящий трафик – это трафик, у которого адреса источников соответствуют профилю.

В некоторых случаях Профиль может быть определен как внешний по отношению к защищаемым ресурсам. В этом случае, входящий трафик в группе отчетов Состояние сети будет соответствовать исходящему трафику для профиля, а исходящий трафик в группе отчетов Состояние сети будет соответствовать входящему трафику для профиля.

Общая информация об аналитических отчетах приведена в разделе Работа с аналитическими отчетами.

Суммарный отчет › Сравнение профилей

Отчёт показывает трафик наблюдаемых объектов (Профилей) за выбранный интервал времени с разбивкой по Профилям.

Для каждого Профиля в таблице показывается входящий, исходящий и суммарный трафик.

Суммарный отчет › Профиль

Отчёт показывает информацию о суммарном трафике выбранного Профиля с разбивкой по типам: входящий, исходящий, отброшенный и суммарный (Всего).

Выбор профиля осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Для каждого типа трафика в таблице показывается текущее, среднее и максимальное значения, а также значение 95-го процентиля за интервал построения отчета.

Приложения › Все

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по приложениям. Под приложением понимается порт tcp/udp или код и тип сообщения icmp.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых портов в блоке фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › ICMP

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по парам ICMP-типов и ICMP-кодов, формирующих ICMP-сообщение.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых ICMP-сообщений в блоке расширенной фильтрации, указав перечисление или диапазон числовых

идентификаторов типов ICMP, либо указав текстовое наименование ICMP-сообщения (например, echo или echo reply), а также дополнительно ограничить версию протокола ICMP (ICMPv4 или ICMPv6).

Приложения › TCP

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по IPv4 TCP-приложениям. Под приложением понимается порт tcp.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › UDP

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по IPv4 UDP-приложениям. Под приложением понимается порт udp.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › IPv6 › TCP

Отчёт показывает входящий и исходящий IPv6-трафик выбранных Профилей с разбивкой по TCP IPv6-приложениям. Под приложением понимается порт tcp.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Приложения › IPv6 › UDP

Отчёт показывает входящий и исходящий IPv6-трафик выбранных Профилей с разбивкой по UDP IPv6-приложениям. Под приложением понимается порт udp.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых портов в блоке расширенной фильтрации, указав перечисление или диапазон портов, а также дополнительно ограничить тип порта (source или destination).

Размеры пакетов

Отчёт показывает входящий и исходящий трафик, проходящий через Систему, с разбивкой по размерам пакетов.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых размеров пакетов в блоке расширенной фильтрации, указав перечисление или диапазон размеров пакетов.

Пользовательские отчеты

Отчёт показывает информацию о суммарном входящем и исходящем трафике выбранного пользовательского отчета.

Выбор пользовательского отчета осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Для каждого типа трафика в таблице показывается текущее, среднее и максимальное значения, а также значение 95-го процентиля за интервал построения отчета.

Детальная информация о настройке пользовательских отчетов приведена в разделе Пользовательские отчеты.

Протоколы

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по протоколам.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых протоколов в блоке расширенной фильтрации, указав перечисление или диапазон протоколов. При перечислении допускается использовать символические обозначения протоколов: tcp, udp, icmp и т.д.

QoS › Тип сервиса

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по типам обслуживания (ToS).

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых кодов ToS в блоке расширенной фильтрации, указав их перечисление или задав диапазон.

QoS › Тип сервиса (DTRM)

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по типам обслуживания в нотации DTRM (3-6 биты поля ToS). Нотация DTRM определяет следующие типы сервиса:

D - минимальная задержка;

T - максимальная пропускная способность;

R - максимальная надежность;

M - минимальная стоимость.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых кодов ToS в блоке расширенной фильтрации, указав их перечисление или задав диапазон. допускается использование символов D, T, R, M при перечислении.

QoS › IP Precedence

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по важности датаграммы (IP Precedence).

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых кодов IP Precedence в блоке расширенной фильтрации, указав их перечисление (десятичные значения) или задав диапазон.

QoS › DSCP

Отчёт показывает входящий и исходящий трафик выбранных Профилей с разбивкой по значениям DSCP.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых значений DSCP в блоке расширенной фильтрации, указав их перечисление (десятичные значения) или задав диапазон.

Рейтинг по потреблению трафика › Внутренние IP-префиксы

Отчёт показывает ранжированный по пиковому трафику список из 100 IP-адресов, внутренних для Профиля (принадлежащих Профилю). Отчет предназначен для оценки хостов наблюдаемого объекта (Профиля), создающих или принимающих наибольший трафик.

В дополнение к линейному графику распределения трафика по времени и таблице хостов отчет содержит гистограмму: распределение трафика по пиковым значениям трафика. Диаграмма позволяет визуально оценить соотношение пикового трафика хостов без привязки ко времени.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Рейтинг по потреблению трафика › Внешние IP-префиксы

Отчёт показывает ранжированный по пиковому трафику список из 100 IP-адресов, внешних для Профиля (не принадлежащих Профилю). Отчет предназначен для оценки хостов, создающих наибольший трафик, направленный на хосты входящие

в Профиль, или принимающих наибольший трафик, создаваемый хостами входящими в Профиль.

В дополнение к линейному графику распределения трафика по времени и таблице хостов отчет содержит гистограмму: распределение трафика по пиковым значениям трафика. Диаграмма позволяет визуально оценить соотношение пикового трафика хостов без привязки ко времени.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

География IP › Страны

Отчет показывает трафик выбранных Профилей с разбивкой по странам источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются страны для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по странам:

- В страну в профиль – страна получателя трафика, входящий трафик для наблюдаемого объекта;
- В страну из профиля – страна получателя трафика, исходящий трафик для наблюдаемого объекта;
- Из страны в профиль – страна источника трафика. входящий трафика для наблюдаемого объекта;
- Из страны из профиля – страна источника трафика, исходящий трафик для наблюдаемого объекта.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых стран в блоке расширенной фильтрации, выбрав необходимые страны через соответствующий селектор.

География IP › Регионы

Отчет показывает трафик выбранных Профилей с разбивкой паре страна и регион источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются регионы для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по регионам:

- В регион в профиль – страна и регион получателя трафика, входящий трафик для наблюдаемого объекта;
- В регион из профиля – страна и регион получателя трафика, исходящий трафик для наблюдаемого объекта;
- Из региона в профиль – страна и регион источника трафика. входящий трафика для наблюдаемого объекта;
- Из региона из профиля – страна и регион источника трафика, исходящий трафик для наблюдаемого объекта.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых стран и(или) регионов в блоке расширенной фильтрации, выбрав необходимые параметры через соответствующие селекторы.

География IP › Города

Отчет показывает трафик выбранных Профилей с разбивкой по составному ключу, состоящему из страны, региона и города источника и получателя.

Существует два направления трафика (входящий и исходящий). Для каждого направления определяются города для источника и получателя трафика. Т.о., существует четыре варианта распределения трафика по городам:

- В город в профиль – страна, регион и город получателя трафика, входящий трафик для наблюдаемого объекта;
- В город из профиля – страна, регион и город получателя трафика, исходящий трафик для наблюдаемого объекта;
- Из город в профиль – страна, регион и город источника трафика. входящий трафика для наблюдаемого объекта;
- Из город из профиля – страна, регион и город источника трафика, исходящий трафик для наблюдаемого объекта.

Выбор профилей осуществляется с помощью селектора в соответствующем поле блока фильтрации.

Существует возможность ограничить список отображаемых стран, регионов и(или) городов в блоке расширенной фильтрации, выбрав необходимые параметры через соответствующие селекторы.

11.3 Пользовательские отчеты

Скаут содержит большой набор собираемых аналитических отчетов по трафику. Однако, в некоторых случая может потребоваться собирать специфичные отчеты по трафику для отдельных наблюдаемых объектов (Профилей).

Скаут позволяет определить пользовательские отчеты, в которых будет отображаться суммарный трафик наблюдаемого объекта с учетом дополнительных ограничений, задаваемых с помощью языка описания синатур трафика gfcap (описание языка сигнатур приведено в разделе Критерии в наблюдаемых объектах).

Сбор данных для отчета начинается сразу после определения параметров пользовательского отчета.

Для добавления нового пользовательского отчета необходимо перейти в меню Настройки › Мониторинг на вкладку Пользовательские отчеты и нажать на кнопку + Добавить запись. В открывшемся окне необходимо выбрать наблюдаемый объект, для которого создается дополнительный пользовательский отчет, указать название этого отчета и составить сигнатуру отчета, используя мастер или введя сигнатуру трафика в формате gfcap вручную.

Изменение сигнатуры трафика производится путем перехода по ссылке в поле Название таблицы пользовательских отчетов.

Для удаления пользовательских отчетов необходимо отметить удаляемые строки флагом и нажать на кнопку Удалить в панели инструментов.

Для просмотра пользовательских отчетов необходимо перейти в меню Отчеты, выбрать вкладку Профиль › Пользовательские отчеты, а затем выбрать пользовательский отчет в соответствующем параметре в блоке фильтрации. Наполнение отчета совпадает с суммарным отчетом по профилю.

12 Информация о трафике (flow-записи)

Для детектирования DoS-атак и аномалий по трафику, Скаут собирает и использует информацию о трафике, совместимую со стандартным протоколом netflow и его аналогами. Информация о трафике может поступать от подсистемы очистки трафика Скаута или от маршрутизаторов СПД.

Скаут позволяет выполнять просмотр поступаемой информации о трафике, либо выполнять ретроспективный анализ по накопленным в базе flow-записей данным.

12.1 Сбор поступаемой информации о трафике

Скаут позволяет собирать и отображать информацию о трафике, поступаемую для обработки. Эта функциональность необходима для проверки правильности поступления flow-записей, особенно в случае, если информация о трафике поступает от маршрутизаторов СПД. Функциональность позволяет оценить правильность классификации интерфейсов маршрутизаторов в Скаут, если информация о трафике поступает от маршрутизаторов СПД и корректность использования netflow sampling при автоматическом его определении.

Для того, чтобы получить информацию о трафике, поступающую в Скаут, необходимо:

- перейти в меню Система на вкладку Сырой NetFlow → Дамп;
- если необходимо собрать только часть поступающих данных, ввести сигнатуру трафика для сбора в поле Введите сигнатуру трафика для сбора пакетов вручную с клавиатуры или воспользовавшись мастером созданий сигнатур, который доступен при нажатии на кнопку Добавить правило с помощью мастера;
- при необходимости, изменить значения полей Максимальное время дампа и Максимальное кол-во NetFlow-записей;
- нажать на кнопку Старт.

Собранные flow-записи отображаются в таблице. Допускается настройка отображаемых в таблице полей, используя переключатели в разделах Метаданные, NetFlow и Производные.

12.2 Хранилище flow-записей

Скаут имеет возможность хранения ограниченного объема приходящих flow-записей в специализированной базе данных. Сохраняемые flow-записи

обогащаются дополнительной информацией об объектах мониторинга и сигнатурах DoS-атак, которым соответствует flow-запись.

Для работы с хранилищем необходимо перейти в меню Система на вкладку Сырой NetFlow › Хранилище

Информация о flow-записях представлена в виде графика и таблицы. Отчет работает в двух режимах:

- переключатель **С группировкой** активен - в этом режиме данные группируются по выбранным полям, на графике отображаются ряды сгруппированных данных;
- переключатель **С группировкой** не активен - в этом режиме в таблице представлены отдельные flow-записи без группировки, а не графике показан один ряд: распределение трафика по времени.

Блок фильтров в верхней части позволяет настраивать отбираемые из БД данные. Для построения сложных условий необходимо переключить фильтр в режим Расширенный фильтр или воспользоваться кнопкой ☰ для выбора параметров фильтрации. Для начала выполнения запроса необходимо нажать на кнопку Найти.

Кнопка Скачать дает возможность скачать flow-записи в виде файла в формате csv.

13 Дополнительные возможности

13.1 Управление АПК через REST API

Программный интерфейс удалённого администрирования (API) позволяет управлять работой и осуществлять настройку Скаута удалённо по протоколу HTTPS с применением RESTful запросов.

Запросы к REST API могут выполнять только аутентифицированные и авторизованные пользователи. API поддерживает метод аутентификации с использованием токена доступа (apikey). Доступ к API разрешён активным учётным записям, в настройках прав доступа которых установлен флаг Разрешить доступ к API.

Функциональность REST API описана в схемах, соответствующих формату openapi 3.0. Схемы доступны для загрузки на страницах описания API, к которым можно обратиться, открыв одноименный раздел электронной версии документации. Схемы также доступны в виде документов в формате PDF.

Поддерживается API версии 3, которая доступна по пути /api/v3/.

13.1.1 REST API Управление комплексом

Скаут предоставляет полнофункциональный API управления Комплексом.

API управления позволяет выполнять следующие действия:

- создавать, изменять параметры и удалять пользователей Комплекса;
- создавать, изменять параметры и удалять группы безопасности;
- изменять параметры настроек прав доступа;
- изменять общие настройки Комплекса, а также его отдельных подсистем;
- создавать, изменять параметры и удалять наблюдаемые объекты;
- создавать, изменять параметры и удалять правила уведомления и группы уведомлений;
- создавать, изменять параметры и удалять DoS-сигнатуры атак, настройки детектирования, включая управление порогами, а также настройку параметров подавления для DoS-сигнатур атак;
- создавать, изменять параметры и удалять шаблоны подавления атак всех типов;
- создавать, изменять параметры и удалять задания подавления, а также управлять планировщиком заданий;

- получать информацию о текущих и прошедших DoS-атаках, событиях и аномалиях, зафиксированных Комплексом;
- получать детальную статистику по каждой DoS-атаке;
- получать детальную статистику по каждому заданию подавления.

Все запросы, отправляемые посредством REST API, проходят аутентификацию, авторизацию и валидацию. В случае не прохождения какого-либо из этапов, возвращается соответствующий код ошибки:

401:	не пройдена аутентификация или авторизация;
40X:	в запросе указаны некорректные параметры.

В случае успешного выполнения запроса возвращаются коды успешного завершения и запрашиваемая информация:

200:	запрос успешно выполнен, запрошенная информация находится в теле ответа;
204:	запрос успешно, выполнен, информация для передачи отсутствует.

Запросы могут быть отправлены из любого ПО, совместимого со стандартом HTTP(S), при этом для управления используются методы GET,PUT,PATCH и DELETE.

Например, для получения списка текущих DoS-атак можно выполнить следующий запрос:

```
curl -X GET "https://scout.server/api/v3/anomalies/attacks?
ongoing=true&limit=10" -H "accept: application/json"
```

Поскольку в запросе не присутствует аутентификационная информация, в результате будет получен ответ о необходимости аутентификации:

```
HTTP/1.1 401 Unauthorized

{"error":"Authentication required"}
```

Дополним запрос информацией об аутентификации по ключу (apikey):

```
curl -X GET "https://scout.server/api/v3/anomalies/attacks?
ongoing=true&limit=10" \
  -H "accept: application/json" \
  -H "APIKEY: insert_your_apikey_here"
```

Если указанный ключ прошел проверки, в запросе будет присутствовать информация о первых 10 текущих атаках из списка атак в формате json:


```
{
  "total": 2,
  "start": 0,
  "limit": 10,
  "entry": [
    {
      "id": 6135772,
      "managed_object": {
        "name": "117 all",
        "description": "test 2"
      },
      "protected_ip": "192.168.117.100",
      "start_time": "2019-06-03T13:03:55+03:00",
      "duration": "0:0:1",
      "vectors": [
        {
        "id": 8,
        "name": "UDP (вх)",
        "bps_severity": 36400,
        "bps_threshold": 0,
        "pps_severity": 0,
        "pps_threshold": 0
        },
        {
        "id": 1,
        "name": "Total (вх)",
        "bps_severity": 36400,
        "bps_threshold": 0,
        "pps_severity": 0,
        "pps_threshold": 0
        }
      ]
    },
    {
      "id": 6135770,
      "managed_object": {
        "name": "117 all",
```

```
        "description": "test 2"
      },
      "protected_ip": "192.168.117.161",
      "start_time": "2019-06-03T13:03:40+03:00",
      "duration": "0:0:1",
      "vectors": [
        {
        "id": 7,
        "name": "TCP ACK (вх)",
        "bps_severity": 16600,
        "bps_threshold": 0,
        "pps_severity": 0,
        "pps_threshold": 0,
        "stop_time": "2019-06-03T13:04:55+03:00"
        },
        {
        "id": 1,
        "name": "Total (вх)",
        "bps_severity": 16600,
        "bps_threshold": 0,
        "pps_severity": 0,
        "pps_threshold": 0,
        "stop_time": "2019-06-03T13:04:55+03:00"
        }
      ]
    }
  ]
}
```


13.1.2 REST API Отчеты по трафику

Скаут предоставляет полнофункциональный API выгрузки аналитической информации о трафике для интеграции с внешними системами. Вся информация выгружается в формате json. Информация для построения графиков выгружается в виде kv-пар.

API отчетов по трафику позволяет выполнять следующие действия:

- получать список всех доступных отчетов, а также доступных отчетов по каждой категории (отчеты по сети, отчеты по наблюдаемым объектам, отчеты по маршрутизаторам и т.д.);

- получать информацию о форматах предоставляемой в отчете информации (таблица, график);
- получать данные о трафике в формате json с учетом заданных в запросе ограничений;
- получать данные для построения графиков в формате json в виде kv-пар.

API отчетов по трафику повторяет структуру данных отчетов по трафику графического интерфейса пользователя Скаут, делая возможность выгрузки данных по любому отчету во внешние системы.

Например, необходимо получить данные по трафику Клиента в разрезе приложений (портов) протокола tcp. Запрос:

```
curl -X GET
"http://scout.server/api/v3/reports/mo/customer/app/tcp" -H
"accept: application/json" -H "APIKEY: insert_your_apikey_here"
```

предоставит информацию о том, какие типы отчетной информации доступны для запрашиваемого отчета:

```
{
 "_links": [
   {
     "href": "/api/v3/reports/mo/customer/app/tcp/chart",
     "rel": "child",
     "name": "Chart item link"
   },
   {
     "href": "/api/v3/reports/mo/customer/app/tcp/table",
     "rel": "child",
     "name": "Table link"
   }
 ]
}
```

Как видно из результата запроса, отчет представляет собой один график и одну таблицу.

Получим данные в табличном формате средние значения трафика в bps за сутки для клиента с идентификационным номером 339 для приложения ssh:

```
curl -X GET
"http://scout.server/api/v3/reports/mo/customer/app/tcp/table?
```

```
func=avg&filter_customers=339&filter_units=bps&filter_period=da
y&filter_tcp-port=22" \
-H "accept: application/json" \
-H "APIKEY: insert_you_api_key_here"
```

В результате получаем массив данных в json формате:


```
{
 "entry": [
   {
     "port": 22,
     "port_type": "dst",
     "object_id": "339",
     "bps_in": 3764.5112,
     "bps_out": 0,
     "bps_total": 3764.5112,
     "name": "ssh",
     "object_name": "117 all",
     "in": 3764.5112,
     "out": 0,
     "total": 3764.5112,
     "_links": [
       {
         "href": "/api/v3/reports/mo/customer/app/tcp/chart?
filter_customers=339&filter_units=bps&filter_period=day&filter_
tcp-port=22&item=%7B%22direction%22%3A0%2C%22object_name%22%3A%
22117+all%22%2C%22name%22%3A%22ssh%22%2C%22port%22%3A22%2C%
22port_type%22%3A%22dst%22%2C%22object_id%22%3A%22339%22%7D",
         "rel": "child",
         "name": "Chart item link"
       },
       {
         "href": "/api/v3/reports/mo/customer/app/tcp/chart?
filter_customers=339&filter_units=bps&filter_period=day&filter_
tcp-port=22&item=%7B%22direction%22%3A1%2C%22object_name%22%3A%
22117+all%22%2C%22name%22%3A%22ssh%22%2C%22port%22%3A22%2C%
22port_type%22%3A%22dst%22%2C%22object_id%22%3A%22339%22%7D",
         "rel": "child",
         "name": "Chart item link"
       }
     ]
```

```
    },
  ]
}
```

В результате присутствует запрошенная информация в полях bps_in, bps_out, bps_total, а также присутствуют ссылки (поле _links) для запроса данных по временному ряду для построения графиков.

Запросим график:

```
curl -X GET
"http://scout.server/api/v2/reports/mo/customer/app/tcp/chart?
filter_customers=339&filter_units=bps&filter_period=day&filter_
tcp-port=22&item=%7B%22direction%22%3A0%2C%22object_name%22%3A%
22117%2Ball%22%2C%22name%22%3A%22ssh%22%2C%22port%22%3A22%2C%
22port_type%22%3A%22dst%22%2C%22object_id%22%3A%22339%22%7D" \
-H "accept: application/json" \
-H "APIKEY: insert_your_apikey_here"
```

В результате получим временной ряд, состоящий из значений key и value (kv-пара):

```
{
 "entry": [
   {
     "p": 1591102200,
     "value": -5848
   },
   {
     "p": 1591102800,
     "value": -1296
   },
   {
     "p": 1591103100,
     "value": -3960
   },
 ]
}
```

Параметр «p» представляет собой временную метку в формате unix timestamp, а «value» значение запрашиваемого параметра в этой точке в запрашиваемых единицах измерения (bps или pps).

13.1.3 Журнал API-запросов

Все запросы к API журналируются. Для просмотра информации о запросах через веб-интерфейс, необходимо перейти в меню Система › Запросы API. В журнале доступна следующая информация:

- дата и время запроса;
- пользователь, выполнивший запрос;
- IP адрес, с которого поступил запрос;
- запрашиваемый ресурс;
- время обработки запроса;
- информация об успешности выполнения запроса с указанием кода возврата HTTP.

Для поиска необходимой информации в верхней части экрана предусмотрен фильтр, позволяющий указать исследуемый временной диапазон, имя пользователя (или его часть с учетом регистра символов), метод, а также запрашиваемый ресурс или его часть.

Доступ к журналу запросов может быть получен также и с помощью API или CLI. В первом случае необходимо отправить запрос GET на ресурс */logs/security/audit*, при необходимости указав параметры фильтра (без указания параметров выводится информация за 1 сутки), а во втором случае, необходимо выполнить в интерактивном режиме *info*, либо с помощью утилиты syncli в пакетном режиме команду:

```
show logs security audit
```

13.1.4 restfull webhooks

Вебхук (webhook) - это определяемый пользователем обратный вызов, путем отправки запроса по протоколу HTTP(S). Его можно использовать, чтобы уведомлять внешнее приложение, о наступлении определенного события в формате, пригодном для обработки внешним приложением. Например, можно предупредить приложение, когда задание подавления запускается или останавливается, или когда выявляется DoS-атака на определенный наблюдаемый объект. Использование вебхуков позволяет внешнему приложению не опрашивая периодически Скаут через REST API, получать информацию о наступлении событий.

Для настройки вебхуков необходимо использовать REST API. Поддерживаются следующие виды запросов:

POST /system/webhooks:	создание нового вебхука
PATCH /system/webhooks/{webhook_id}:	изменение параметров вебхука
DELETE /system/webhooks/{webhook_id}:	удаление вебхука
GET /system/webhooks/{webhook_id}:	просмотр параметров вебхука
GET /system/webhooks:	просмотр списка вебхуков
GET /system/webhooktasks:	просмотр списка задач вебхуков

Для создания вебхука необходимо отправить POST запрос, содержащий следующие обязательные параметры в формате json (описание параметров приведено ниже):

resource:	ресурс Скаута, для которого создается вебхук
resource_params:	параметры вебхука для выбранного ресурса
enabled:	флаг активности вебхука
events:	события, для которых будет срабатывать вебхук
url:	ресурс, на который будет отправляться сообщение
method:	метод запроса (GET, POST и т.д.)
http_version:	версия протокола HTTP
headers:	коллекция заголовков запроса (например, для метода POST обязателен заголовок Content-Type)
options:	опции запроса: **verify** - флаг проверки TLS сертификата сервера ***Примечание:*** *Не рекомендуется отключать проверку сертификатов на не доверенных ресурсах.*
body:	шаблон тела запроса в формате, соответствующем заголовку Content-Type с применением подстановочных элементов TWIG
description:	текстовое описание вебхука

Пример сообщения json для создания вебхука отправки информации о запуске задания подавления в мессенджер телеграм:

```
{
  "resource":"/defense/mitigations",
  "resource_params":{
    "mo":[{"id":88333 }]
  },
  "url":"https://api.telegram.org/<BOT_ID>:<BOT_KEY>/sendMessag
e",
  "headers":["Content-Type: application/x-www-form-
urlencoded"],
  "body":"chat_id=-1001700067151&text=Задание для наблюдаемого
объекта 'Мой объект' {{event_type}}%0AПользователь:
{{user_name}}",
  "events":["update"],
  "enabled":true,
  "description":"telegram notification"
}
```

Вебхуки отправляют внешнему приложению HTTP-запрос, с телом запроса (body), сформированным на основе шаблона, задаваемого при создании вебхука. Шаблоны вебхуков поддерживают формат TWIG (https://twig.symfony.com), что позволяет формировать различные сообщения в зависимости от значений параметров сообщения, например, менять цвета в сообщении в зависимости от опасности DoS-атаки или включать в сообщение различную информацию в зависимости от того, какой наблюдаемый объект атакуется. Например, при использовании шаблона:

```
Ресурс {{resource}}/{{id}} был изменён в {{time\\|date('Y-m-d
H:i:s')}}
```

после подстановки параметров сформируется сообщение

```
Ресурс /defense/mitigations/123 был изменён в 2021-12-28
11:12:00
```

В шаблонах разрешено использовать:

теги:	if, for, apply

фильтры:	lower, upper, escape, capitalize, date, date_modify, default, format, format_number, join, json_encode, length, replace, round, slice, split, title, trim, url_encode, raw, striptags, json, json_pretty
функции:	date, max, min, random, range

Для всех ресурсов поддерживаются общие параметры в шаблонах сообщений:

{{id}}:	число, идентификатор ресурса
{{resource}}:	строка, тип ресурса
{{time}}:	число, время события в формате unixtime. Для вывода в сообщение нужно использовать фильтр date`
{{event}}:	строка, тип события: create, update, delete
{{user_id}}:	число, идентификатор пользователя. Для системного события имеет пустое значение
{{user_name}}:	строка, имя пользователя. Для системного события имеет значение «Система»

Скаут поддерживает создание вебхуков для следующих ресурсов:

- /defense/mitigations
  - параметры вебхука (формат описан в документации к API):

ids:	массив, список идентификаторов заданий подавления
mo:	массив, список наблюдаемых объектов
prefixes:	массив, список префиксов

  - дополнительные параметры шаблона сообщения:

{{comment}}:	строка, описание события
{{details}}:	массив, подробная информация об изменении. Для вывода в сообщение нужно использовать фильтры json, json_pretty, json_encode
{{event_type}}:	строка, тип события в рамках ресурса
{{mo_id}}:	число, идентификатор наблюдаемого объекта

{{prefixes}}:	массив, список префиксов

- /anomalies/attacks
  - параметры вебхука:

ids:	массив, список идентификаторов DoS-атак
mo:	массив, список наблюдаемых объектов
prefixes:	массив, список префиксов

  - дополнительные параметры шаблона сообщения:

{{comment}}:	строка, описание события
{{action}}:	строка, тип события в рамках ресурса
{{mo_id}}:	число, идентификатор наблюдаемого объекта
{{ip}}:	строка, атакуемый ip-адрес

При выполнении запроса, Скаут пытается два раза соединиться с внешним сервером и передать запрос.

История изменений ресурсов и выполнения задач хранится 1 сутки.

13.2 Управление АПК через интерфейс командной строки

Интерфейс командной строки (command line interface, CLI) позволяет управлять работой и осуществлять настройку Скаута удалённо по протоколу SSH в интерактивном режиме.

Включение доступа к интерфейсу командной строки осуществляется путем установки соответствующего флага в параметрах пользователя.

Для подключения к интерфейсу командной строки необходимо с помощью ssh-клиента, совместимого с протоколом ssh2, подключиться к Скауту, используя учетный данные пользователя, имеющего право доступа к интерфейсу командной строки. После успешного входа в систему на терминале отображается стартовый баннер, время последнего входа в систему и приглашение для ввода команд

```
****************************************
*            PERIMETER CLI             *
```

```
*                                          *
*      WARNING: Authorised Access Only     *
*******************************************

Welcome user_cli it is Mon Jun 22 12:31:44 MSK 2020
user_cli@scout#
```

Интерфейс командной строки представляет собой интерактивный терминал, позволяющий получать информацию о работе Скаута, управлять защитой, а также изменять настройки. Введя с клавиатуры команду ? (знак вопроса), можно получить информацию о доступных командах и(или) параметрах.

Меню верхнего уровня состоит из следующих пунктов:

configure:	переводит интерфейс в режим изменения конфигурации Скаута
exit:	завершает сеанс работы с интерфейсом командной строки
help:	позволяет получить расширенную информацию о работе с интерфейсом командной строки
history:	отображает на экране терминала историю используемых команд
info:	переводит интерфейс в режим просмотра конфигурации Скаута
logout:	завершает сеанс работы с интерфейсом командной строки
top:	возврат в меню верхнего уровня
utils:	диагностические утилиты ping, netstat, traceroute, nslookup

Режим info предоставляет доступ к команде show, с помощью которой осуществляется просмотр информации по всем категориям объектов Скаута. Например, для просмотра текущих DoS-атак, необходимо выполнять в режиме info следующую команду:

```
user_cli@scout info# show anomalies attacks --ongoing
```

Результат отобразится на экране терминала в формате JSON.

Режим configure предоставляет возможность управления Скаутом, включая изменение параметров наблюдаемых объектов, маршрутизаторов, пользователей и иных логических объектов; запуск, остановку и изменение параметров заданий подавления, а также управление правилами и группами оповещений. Например,

для включения в задании подавления с идентификатором 531990 метода TCP-аутентификации, необходимо выполнить следующую команду в режиме configure:

```
user_cli@scout configure-perimeter# update defense mitigations
mitigation_id parameters 531990
```

В открывшемся редакторе в секции tcp_auth установить для параметра tcp_host_auth_method значение OUT_OF_SEQUENCE и сохранить изменения (F10 или Esc с последующим подтверждением внесения изменений в параметры). В результате, при успешном изменении параметров на экране терминала отобразится идентификатор измененного объекта в формате JSON, а при некорректном задании параметров, сообщение об ошибке.

Для запуска задания подавления с идентификатором 531990 необходимо выполнить команду:

```
user_cli@scout configure-perimeter# add defense mitigations
mitigation_id start 531990
```

В результате, на экране терминала отобразится результат запрашиваемого действия в формате JSON, а при невозможности выполнения действия, сообщение об ошибке.

Основные команды, доступные в режиме configure:

add:	добавление логического объекта, отправка команды на выполнение какого-либо действия (например запуск задания подавления);
delete:	удаление логического объекта, очистка списка;
replace:	замена параметров логического объекта на заданные, при этом отсутствующие в запросе параметры принимают значения по умолчанию;
update:	обновление параметров логического объекта заданными, при этом отсутствующие в запросе параметры не изменяют свои значения.

Детальное описание команд, параметров и их значений приведено в документе «Скаут. Описание интерфейса командной строки.», а также в справочной системе man для утилиты syncli:

```
man syncli
```

13.3 Расширение GeoIP

Расширение GeoIP - это дополнение, вносимое в БД и изменяющее географическую принадлежность IP-префиксов и/или IP-адресов.

Функция расширения GeoIP оказывается чрезвычайно полезной, если пользователь располагает достоверными и точными данными о принадлежности IP-префиксов к некоторой географической области. Внесение этих данных в БД значительно повышает достоверность определения географической принадлежности.

Другим возможным применением функции может стать создание некоторой виртуальной области, объединяющей в себе, например, IP-адреса спутниковых провайдеров. Таким образом, отслеживать и анализировать их трафик становится значительно проще.

Доступ к странице расширений GeoIP осуществляется через меню Настройки › Общие настройки на вкладке Расширение GeoIP. Данные представлены в виде таблицы со следующими столбцами:

Часть света:	принадлежность к континенту;
Код страны:	Код административного деления, согласно ISO 3166-1 alpha-2 (https://www.iso.org/iso-3166-country-codes.html);
Страна:	наименование страны;
Код региона:	буквенно-цифровой код региона внутри страны;
Город:	наименование города;
IP-префикс:	IP-префикс, для которого устанавливается географическая принадлежность;
Редактировать:	нажатие кнопки активирует режим редактирования расширения;
Удалить:	нажатие кнопки приводит к удалению расширения.

В верхней части рабочей области страницы содержится фильтр строк таблицы. Чтобы отфильтровать строки таблицы, заполните нужные поля фильтра. Таблица будет содержать только строки, значения которых совпадают с заданными критериями фильтра.

Скаут позволяет выполнить экспорт и импорт данные по расширению БД из файла. Экспорт всех изменений, внесённых в географические данные БД анализатора, осуществляется нажатием кнопки Получить файл конфигурации, а импорт данных - нажатием кнопки Загрузить файл конфигурации.

Примечание: *Загружаемый файл должен содержать в себе все необходимые расширения БД geoIP, загрузка происходит в режиме замены. Поэтому, рекомендуется сначала выполнить экспорт в файл, затем внести изменения и загрузить измененный файл.*

Пересечения префиксов в загружаемом файле не допускаются.

Максимальная длина одного префикса - /24. Загрузка более длинных префиксов приведет к ошибке.

13.3.1 Добавление GeoIP-расширения

Для того, чтобы добавить расширение GeoIP в БД анализатора необходимо:

- перейти в меню Настройки › Общие настройки на вкладку Расширение GeoIP;
- нажать кнопку ✚ Добавить запись;
- заполнить поля:
  - Часть света;
  - Код страны;
  - Страна;
  - Код региона;
  - Город;
  - IP-префикс.
- нажать кнопку Сохранить.

Примечание: *При настройке параметров метода очистки Географический фильтр учитываются расширения БД GeoIP по странам.*

13.3.2 Редактирование GeoIP-расширения

Чтобы отредактировать расширение GeoIP необходимо:

- перейти на страницу интерфейса Администрирование › Общие настройки › Расширение GeoIP;

- найти запись, требующую изменения, используя фильтр или визуальный поиск;
- перейти на форму редактирования, выделив строку таблицы и нажав на кнопку Редактировать в панели инструментов;
- изменить значения параметров расширения;
- нажать кнопку Сохранить.

13.3.3 Удаление GeoIP-расширения

Чтобы удалить расширение GeoIP необходимо:

- перейти на страницу интерфейса Администрирование › Общие настройки › Расширение GeoIP;
- выделить строки, которые необходимо удалить;
- нажать кнопку Удалить в панели инструментов.

13.4 Резервное копирование

Для обеспечения возможности восстановления системы в случае программного или аппаратного сбоя, приведшего к потере или повреждению данных, необходимо организовать создание резервных архивных копий.

Система позволяет создавать резервные копии следующими способами:

- архивирование только конфигурации — резервная копия будет содержать только конфигурационную информацию (настройки и параметры), расположенную в базе данных и не будет содержать аномалии, в т.ч. и DoS-атаки и отчеты по трафику;
- архивирование полной базы данных — резервная копия будет содержать параметры конфигурации и накопленную статистическую информацию (отчеты, статистика по аномалиям и т.п.);
- инкрементальный архив — резервные копии образуют архивное хранилище, содержащее параметры конфигурации и накопленную статистическую информацию, хранящиеся в базе данных; первый архив содержит полную копию базы данных, а каждый последующий содержит только изменения относительно полного архива.

Для создания резервных копий вручную, просмотра журнала последней операции архивирования и изменения параметров планировщика задач архивирования, необходимо перейти в меню Настройки › Общие настройки и выбрать вкладку Архивирование.

Блок Журнал архивирования содержит информацию о последней задаче создания резервной копии.

В блоке Запустить архивирование находятся кнопки ручного создания резервных копий.

Блок Параметры архивирования содержит настройки планировщика задач архивирования. После изменения параметров, необходимо подтвердить внесение изменений нажатием кнопки Сохранить.

Созданные резервные копии располагаются на специально выделенном разделе дисковой подсистемы и доступны по пути /var/dbbackup.

Резервные копии могут копироваться на внешний sftp-сервер. Активировать копирование можно с помощью переключателя Отправлять по sftp. При этом, необходимо заполнить параметры подключения к sftp-серверу:

- Адрес — fqdn или IP-адрес sftp-сервера;
- Логин — имя пользователя, которое будет использовано для аутентификации на sftp-сервере;
- Sftp-пароль — пароль, который будет использован для аутентификации на sftp-сервере.

Примечание: *необходимо предоставить пользователю на sftp-сервере права на создание файлов и каталогов (для каждого типа архивной копии создается свой каталог на sftp-сервере).*

14 ПРИЛОЖЕНИЕ Б - Сигнатуры - описание языка

14.1 Общие сведения

Язык сигнатур – декларативный язык описания потоков данных, передаваемых через контролируемую СПД.

Созданные пользователем сигнатуры представляют собой наборы специфических признаков, характеризующих как обычный, так и аномальный трафик.

При помощи сигнатур система выделяет из всего объема трафика, передаваемого через СПД, те его составляющие, которые требуют внимания. В качестве характерных особенностей трафика, содержащихся в сигнатурах, могут выступать IP-адреса или IP-префиксы источников и/или получателей пакетов данных, протоколы, используемые при передаче трафика, TCP-флаги, содержащиеся в передаваемых пакетах, маршрутизаторы, участвующие в передаче данных, и ряд других признаков.

Использование сигнатур позволяет точно выделять из общей массы трафика ту его часть, которую требуется перенаправить на очиститель или классифицируемую системой как трафик одного из наблюдаемых объектов.

Сигнатуры являются удобным инструментом характеризации аномалий. Аномальным считается трафик, параметры которого совпадают с характерными признаками, указанными в его сигнатуре.

Обмен сигнатурами, налаженный между анализаторами, позволяет расширить спектр выявляемых аномалий и предотвращаемых угроз.

14.2 Элементы языка

Сигнатура представляет собой строку текста (выражение), состоящую из одного или нескольких маркеров, характеризующих трафик. Маркер – это условное обозначение того или иного параметра потока данных. В строке сигнатуры кроме маркеров присутствуют также логические операторы и символы, определяющие порядок разбора выражения. Регистр символов у маркеров и логических операторов не имеет значения, например, маркеры rtr и RTR равнозначны. В качестве разделителя компонентов выражения (маркеров и логических операторов) используется пробел.

При разборе сигнатуры программа разбирает выражение слева-направо. Логические операторы порядок разбора не изменяют. Порядок разбора можно

изменить, воспользовавшись круглыми скобками (символы «(» и «)»). Текст, заключённый в скобки, разбирается первым. Сигнатуры с синтаксическими ошибками системой не воспринимаются.

Синтаксис языка различается в зависимости от цели использования сигнатуры. Синтаксис языка сигнатур, используемых при задании критериев наблюдаемых объектов, несколько более сложен, чем язык сигнатур, используемых при создании заданий очистки. Этим различием обеспечивается оперативность считывания сигнатур системой.

14.2.1 Критерии в наблюдаемых объектах

Для выражения сигнатур используются следующие маркеры:

Маркер	Значение	Пример
rtr	маршрутизатор, участвующий в передаче трафика	rtr 192.168.0.1
iface	интерфейс, через который передается трафик	iface 23453
net или host	хост, участвующий в передаче трафика	net 192.168.0.1 или host 192.168.1.1/24
proto	протокол, используемый при передаче трафика	proto tcp или proto 34
tflags	TCP-флаги в пакетах трафика	tflags S/S
icmptype	ICMP-тип трафика	icmptype icmp-echoreply
icmpcode	ICMP-код трафика	icmpcode 4
bpp	размер пакета трафика	bpp 1 или bpp 1..4

Маркер	Значение	Пример
bytes	суммарный трафик в байтах	bytes 4 или bytes 2..5
packets	суммарное количество пакетов трафика	packets 4 или packets 2..5
bps	мгновенная скорость трафика в байтах в секунду	bps 4 или bps 2..5
pps	мгновенная скорость трафика в пакетах в секунду	pps 4 или pps 2..5
src	источник	src net 192.168.0.1 или src host 192.168.10.5/16
dst	получатель	dst host 192.168.5.13 или dst net 192.168.10.5/16

Атрибуты маркеров должны следовать сразу после маркера. Например, bps 4 или host 192.168.10.5/16.

В качестве атрибутов маркеров src и dst выступают другие маркеры. Например, строку «src host 192.168.0.1» программа интерпретирует как трафик, источником которого является хост с IP-адресом 192.168.0.1.

Атрибуты маркера «tflags» задают следующим образом: указывают первые буквы обозначений TCP-флагов, наличие которых отслеживается в пакетах трафика, затем после косой черты («/») повторяют обозначения флагов, указанных перед чертой, и первой буквой названия указывают флаги, которых в пакетах трафика быть не должно. Например, строка «tflags S/SP» интерпретируется как TCP-трафик, в пакетах которого содержится флаг SYN, и отсутствует флаг PUSH.

Существуют следующие TCP-флаги:

- SYN;
- ACK;
- URG;
- FIN;
- PUSH;
- URG;
- ECE;
- CWR.

Диапазоны значений задаются с помощью двух чисел, соответствующих началу и концу диапазона, разделённых символом «..» или «-». Например, строки «pps 2..5» и «pps 2-5» являются корректными и интерпретируются как трафик, мгновенная скорость передачи пакетов которого находится в диапазоне от 2 до 5 пакетов в секунду.

Маркер icmptype недопустимо употреблять без следующего за ним через пробел одного из нижеперечисленных атрибутов, указывающих на конкретный ICMP-тип:

- icmp-echoreply;
- icmp-unreach;
- icmp-sourcequench;
- icmp-redirect;
- icmp-echo;
- icmp-routeradvert;
- icmp-routersolicit;
- icmp-timxceed;
- icmp-paramprob;
- icmp-tstamp;
- icmp-tstampreply;
- icmp-ireq;
- icmp-ireqreply;
- icmp-maskreq;
- icmp-maskreply.

Например, строка icmptype icmp-echoreply интерпретируется программой как ICMP-трафик с типом echoreply.

Использование в выражениях для сигнатур логических операторов AND, OR и NOT позволяет получать сложные синтаксические конструкции, порядок считывания и разбора которых указывается круглыми скобками.

Синтаксис языка предполагает следующие логические операторы:

Логическая операция	Оператор	Оператор (альтернативный)	Пример
Умножение (Оба выражения должны быть истинны)	AND	&&	(dst host 192.168.5.13) && (tflags F/SF)
Сложение (Одно из выражений должно быть истинно)	OR	||	(dst net 192.168.5.13) || (tflags F/SF)
Отрицание (Выражение должно быть ложным)	NOT	!	!(dst net 192.168.5.13)

Маркеры, объединённые логическим оператором OR, могут включать сразу несколько атрибутов, каждый из которых записывается через запятую. Например, (dst host 192.168.5.13) OR (dst host 192.168.5.11, dst host 192.168.5.12), интерпретируется системой как трафик, направляемый на IP-адреса 192.168.5.13 или 192.168.5.11, или 192.168.5.12.

Логическое отрицание может использоваться в паре с другими логическими операторами. Например, NOT (dst host 192.168.5.13 OR dst host 192.168.5.11), эта сигнатура интерпретируется как трафик, ненаправляемый на IP-адреса 192.168.5.13 и 192.168.5.11.

14.2.2 Критерии в заданиях очистки

В методах очистки используется расширенная версия языка сигнатур (gfcap), которая в общем виде представляет собой выражение:

```
[action] expression [CR] LF
```

где:

- action - действие для методов Глобальный фильтр и фильтр задания очистки; может принимать значения:

- drop - отбросить;
- pass - пропустить без обработки;
- cont или continue - пропустить и передать на обработку последующим методам;

Примечание. Рекомендуется группировать правила в следующем порядке: сначала все правила с действием pass, затем все правила с действием continue, а затем все правила с действием drop. Чередование правил с различным действием не запрещено, оно может быть необходимо в отдельных случаях. Однако, предпочтение следует отдавать написанию сгруппированных по виду действия правил.

- eexpression - логическое выражение, описывающее трафик;
- [CR] LF - перевод строки с необязательным символом возврата каретки.

Выражение expression представляет собой совокупность предикатов (параметров) и их значений, объединенных с помощью логических операторов или операторов изменения порядка вычисления.

Предикаты описывают параметры заголовков трафика, по которым осуществляется фильтрация:

- proto или protocol - коллекция протоколов транспортного уровня заголовка IP:

  protocol tcp,udp

  proto = tcp,1..5,47,35-78

  proto 17

  udp,tcp

- port - коллекция портов протоколов tcp или udp, с указанием необязательного значения src - порт источника или dst - порт назначения (если src и dst отсутствуют, то выражение определяет, как порт источника, так и порт получателя):

  dst port 443

  dst port = 443

  src port 123,389,3389,1433

  port 53, что эквивалетно выражению(src port 53) or (dst port 53)

- ttl - диапазоны параметра время жизни пакета:

  ttl 1,5..10,100-150

ttl = 1,5..10,100-150

- tos - тип сервиса (QoS):

  tos 1,5..10,100-150

  tos = 1,5..10,100-150

- frag или ipfrag - установлен флаг фрагментации IP заголовка;
- net или host - IP префикс или адрес с указанием необязательного атрибута src или dst:

  src host 1.2.3.4 или src 1.2.3.4

  src host 1.2.3.0/24

  dst net = 5.6.0.0/16

  8.8.8.8, что эквивалентно выражению (src 8.8.8.8) or (dst 8.8.8.8)

- bytes или bpp - диапазоны длин IP пакета;
- tflags - флаги TCP в нотации УСТАНОВЛЕННЫЕ/АНАЛИЗИРУЕМЫЕ:

  tflags S/S пакеты с установленным SYN, например, SYN или SYN+ACK

  tflags = S/SA пакеты с установленным SYN и отсутствующим ACK

- icmptype - коллекция типов протокола icmp;
- icmpcode - коллекция кодов протокола icmp;
- icmp6type - коллекция типов протокола icmp6;
- icmp6code - коллекция кодов протокола icmp6;
- countrylist - коллекция кодов стран (в виде двухбуквенного кода, либо кода с префиксом "country_"), с указанием необязательного значения src - страна источника пакета или dst - страна назначения пакета:

  src countrylist RU,CN

  dst countrylist = (RU,country_CN)

  countrylist RU, что эквивалентно выражению (src countrylist RU) or (dst countrylist RU)

- ethernet - последовательность шестнадцатиричных значений, начиная с заданного смещению кадра ethernet:

  Ethernet[12] = 0x5F3D7A65

  Ethernet[12] 0x5F3D7A65

Предикаты объединяются с помощью логических выражений, имеющих следующий приоритет (в порядке уменьшения приоритета):

- not или ! - логическое отрицание (унарный оператор);
- and или && - логическое И (бинарный оператор);
- or или || - логическое ИЛИ (бинарный оператор).

Для изменения порядок вычисления, необходимо заключить выражение в круглые скобки. Заключенные в скобки выражения могут объединяться с помощью бинарных операторов.

Предикаты без явного указания направления всегда раскрываются в выражения, использующие предикаты с направлением:

- 8.8.8.8 - раскрывается в ((src 8.8.8.8) or (dst 8.8.8.8))
- port 80, 443 - раскрывается в (src port 80 or dst port 80 or src port 443 or dst port 443)
- countrylist RU, CH - раскрывается в (src countrylist RU or dst countrylist RU or src countrylist CH or dst countrylist CH)

Особенности использования оператора NOT

При использовании оператора NOT, необходимо помнить, что отрицание отсутствующего в пакете атрибута является истиной, например:

- not tflags S/S для пакета ICMP - истинное выражение, т.к. в пакете ICMP нет заголовка TCP с флагами;
- not port 443 для не первого IP фрагмента - истинное выражение, т.к. только в первом фрагменте есть информация о портах транспортного протокола, а в последующих фрагментах заголовок транспортного протокола и, как следствие, информация о портах, отсутствует;
- not icmptype icmp-echo для UDP пакета - истинное выражение, т.к. в UDP пакете отсутствуют заголовок протокола ICMP и, как следствие, информация о типе ICMP;
- not 10.10.10.10 для пакета IPv6 - истинное выражение, т.к. заголовок IPv4 и, как следствие, информация об IPv4 адресах, отсутствует в пакете IPv6.

Отрицание предикатов без явного указания направления port, host/net и countrylist приводит сначала к раскрытию выражения до использующего предикаты с направлением, объединенные через OR, а затем к применению отрицания по правилам Булевой алгебры:

- not 1.2.3.4 - раскрывается в not ((src host 1.2.3.4) or (dst host 1.2.3.4)), что эквивалентно not src host 1.2.3.4 AND not dst host 1.2.3.4;
- not tcp - раскрывается в not ((src port tcp) or (dst port tcp)), что эквивалентно not src port tcp AND not dst port tcp;
- not countrylist RU, CH - раскрывается в not src countrylist RU and not dst countrylist RU and not src countrylist CH and not dst countrylist CH.

Полное описание языка описания сигнатур gfcap в нотации ABNF приведено ниже.

```
;GFCAP grammar ABNF v1.2.0

acted_expression        = [action] expression [CR] LF
action                  = action_pass / action_drop /
    action_cont ; only makes sense for global and mitigation
    filter
action_pass             = "pass" ; forward packet
action_drop             = "drop" ; discard packet
action_cont             = "cont" / "continue" ; pass packet
    to the next mitigation method

expression              = disjunction
disjunction             = conjunction [logic_or conjunction]
logic_or                = "or" / "||"
conjunction             = (predicate / bracketed / negated)
    [logic_and (predicate / bracketed / negated)]
logic_and               = "and" / "&&"
bracketed               = "(" expression ")"
negated                 = negation (predicate / bracketed)
negation                = "not" / "!"

predicate               = predicate_proto /
                          predicate_port /
                          predicate_ttl /
                          predicate_tos /
                          predicate_frag /
```

```
                        predicate_net /
                        predicate_bytes /
                        predicate_tflags /
                        predicate_icmptype /
                        predicate_icmpcode /
                        predicate_icmp6type /
                        predicate_icmp6code /
                        predicate_countrylist /
                        predicate_ethernet /
                        predicate_filterid /
                        predicate_filteracion /
                        predicate_origin

direction               = dir_src / dir_dst
dir_src                 = "src"
dir_dst                 = "dst"

predicate_proto         = [attr_proto] ["="] values_proto
attr_proto              = "proto" / "protocol"
values_proto            = value_proto [1*("," value_proto)]
value_proto             = (uint8_val / protocol_name) [(".."
    / "-") (uint8_val / protocol_name)]

predicate_port          = [direction] attr_port ["="]
    values_port
attr_port               = "port"
values_port             = value_port [1*("," value_port)]
value_port              = (uint16_val / port_name) [(".." /
    "-") (uint16_val / port_name)]

predicate_ttl           = attr_ttl ["="] value_ttl
attr_ttl                = "ttl"
value_ttl               = uint8_list
```

```
predicate_tos           = attr_tos ["="] value_tos
attr_tos                = "tos"
value_tos               = uint8_list

predicate_frag          = attr_frag
attr_tos                = "frag" / "ipfrag"

predicate_net           = [direction] [attr_net] ["="]
    value_net
attr_net                = "net" / "host"
value_net               = (ipv4_addr ["/" ipv4_masklen]) /
                          (ipv6_addr ["/" ipv6_masklen])

predicate_bytes         = attr_bytes ["="] value_bytes ;
    packet size
attr_bytes              = "bytes" / "bpp"
value_bytes             = uint16_list

predicate_tflags        = attr_tflags ["="] value_tflags
attr_tflags             = "tflags" / "tcpflags"
value_tflags            = [tflags_to_match] "/"
    tflags_to_test ; flags-to-match MUST be a subset of
    flags-to-test
tflags_to_match         = tflags_str
tflags_to_test          = tflags_str
tflags_str              = ["S"] ["A"] ["F"] ["R"] ["P"]
    ["U"] ["E"] ["W"] ; [S]YN [A]CK [U]RG [F]IN [P]USH [R]ST
    [E]CE c[W]R

predicate_icmptype      = attr_icmptype ["="]
    values_icmptype
attr_icmptype           = "icmptype"
values_icmptype         = value_icmptype [1*(","
    value_icmptype)]
```

```
value_icmptype          = (icmptype_name / uint8_val) [(".."
    / "-") (icmptype_name / uint8_val)]

predicate_icmpcode      = attr_icmpcode ["="] value_icmpcode
attr_icmpcode           = "icmpcode"
value_icmpcode          = uint8_list

predicate_icmp6type     = attr_icmp6type ["="]
    values_icmp6type
attr_icmp6type          = "icmp6type"
values_icmp6type        = value_icmp6type [1*(","
    value_icmp6type)]
value_icmp6type         = (icmp6type_name / uint8_val)
    [(".." / "-") (icmp6type_name / uint8_val)]

predicate_icmp6code     = attr_icmp6code ["="]
    value_icmp6code
attr_icmp6code          = "icmp6code"
value_icmp6code         = uint8_list

predicate_countrylist   = [direction] attr_countylist ["="]
    value_countrylist ; list of matching countries
attr_countrylist        = "countrylist"
value_countrylist       = country_list /
    bracketed_country_list
bracketed_country_list  = "(" country_list ")"
country_list            = country_name [1*(","
    country_name)]
country_name            = ["country_"] country_code ; e.g.
    country_RU
country_code            = 2(ALPHA / DIGIT)

predicate_ethernet      = attr_ethernet value_ethernet ;
    matches bytes sequence (16 octets at max)
```

```
                                                                ; at
    specific (one-based) offset,
                                                                ;
    e.g. ethernet [10] 0xFE0A
attr_ethernet           = "ethernet"
value_ethernet          = "[" eth_offset "]" ["="] eth_seq
eth_offset              = uint16_val ; zero is not allowed
eth_seq                 = ["0"] "x" 1*16(2HEXDIGIT)

predicate_filterid      = attr_filterid ["="] value_filterid
    ; triggered mitigation method id (raw dump only)
attr_filterid           = "filterid"
value_filterid          = uint8_list

predicate_filteraction  = attr_filteraction ["="]
    value_filteraction ; applied action by mitigation method
    (raw dump only)
attr_filteraction       = "filteraction"
value_filteraction      = "drop" / "pass" / "term"

predicate_origin        = attr_origin ["="] value_origin ;
    packet origin (raw dump only)
attr_origin             = "origin"
value_origin            = "nic" / "tc"

uint8_list              = uint8_range [1*("," uint8_range)]
uint8_range             = uint8_val [(".." / "-") uint8_val]
uint16_list             = uint16_range [1*(","
    uint16_range)]
uint16_range            = uint16_val [(".." / "-")
    uint16_val]
```

14.2.3 Критерии в шаблонных пакетах

При создании сигнатур DoS-атак используется синтаксис, используемый при задании критериев наблюдаемых объектов. Дополнительно могут быть

использованы следующие маркеры:

Маркер	Значение	Пример
dpi slow	детектирование медленных атак по превышению количества простаивающих соединений	dpi slow and dst port 443
dpi httpreq	детектирование атак по превышению количества http запросов	dpi httpreq and proto tcp and dst port 80
dpi l4con	детектирование атак по превышению количества L4 соединений (tcp подключений и udp сессий)	dpi l4con and proto udp
dpi tlshandshake	детектирование атак по превышению количества устанавливаемых соединений TLS	dpi tlshandshake and port 8443
mo {object_id}	детектирование трафика, соответствующего заданному идентификатором {object_id} наблюдаемому объекту	(mo 755 or mo 667) and proto udp

Маркер dpi может быть использован в сигнатуре DoS-атаки только один раз. Счетчики соединений учитываются отдельно для каждой комбинации dst ip + dst port + protocol, поэтому маркеры dpi должны применяться только совместно с маркерами dst host, dst port и proto.

Маркер mo позволяет отслеживать трафик, соответствующий определенным наблюдаемым объектам комплекса. Например, можно детектировать аномальный трафик от хостов ботсетей, определяемых наблюдаемыми объектами с критерием сопоставления "ботсеть".

14.3 Примеры

Для того, чтобы облегчить понимание синтаксиса и принципов обработки декларативного языка сигнатур, ниже приведены некоторые примеры использования языка.

При задании сигнатур:

Характерный признак	Выражение для сигнатуры
трафик, исходящий от хостов из подсети с IP-префиксом 198.168.1.0/24	src net 198.168.1.0/24
трафик, направляемый на порт 22	dst port 22
трафик, исходящий от или направляемый на IP-адрес 1.2.3.4, порт 22	host 1.2.3.4 and port 22
трафик, направляемый на IP-адрес 1.2.3.4, порт 22 или 80	dst host 1.2.3.4 and (port 22 or port www)
TCP-трафик, пакеты которого содержат флаг SYN	proto tcp and tflags S/S
TCP-трафик, пакеты которого содержат флаг SYN и не содержат флаг ACK	proto tcp and (tflags S/SA) или proto tcp and (tflags S/S) and !(tflags SA/SA)
трафик, размер пакетов которого лежит в диапазоне от 500 до 1000 байт	bpp 500..1000

При определении заданий очистителю:

Задание	Выражение для задания
пропускать TCP-трафик	pass proto tcp
пропускать трафик, направляемый из подсети с IP-префиксом 1.1.1.0/24 или 2.2.0.0/16	pass src net 1.1.1.0/24 or src net 2.2.0.0/16
блокировать трафик, не исходящий от IP-адреса 1.1.1.1 или 2.2.2.2	drop not (src host 1.1.1.1 or src host 2.2.2.2)

Задание	Выражение для задания
блокировать трафик, исходящий от подсети с IP-префиксом 0.0.0.0/0, и пропускать трафик, исходящий от подсети с IP-префиксом 1.1.0.0/16	drop src net 0.0.0.0/0 and not src net 1.1.0.0/16
блокировать трафик, исходящий от порта 10	drop src port 10
блокировать трафик, источником которого являются хосты с IP-адресами 1.1.1.1 или 2.2.2.2.	drop not (src host 1.1.1.1 or src host 2.2.2.2)
пропускать весь TCP- и UDP-трафик	pass proto tcp,udp
пропускать трафик, исходящий от хостов с IP-префиксами 1.1.1.0/24 или 2.2.0.0/16	pass src net 1.1.1.0/24 or src net 2.2.0.0/16
пропускать IP-фрагменты UDP-трафика, источником которого является сеть 1.1.0.0/16 или хост 2.2.2.2	pass ipfrag and (src net 1.1.1.0/24 or src host 2.2.2.2)
блокировать TCP-трафик, исходящий от хостов с IP-префиксом 0.0.0.0/0	drop src net 0.0.0.0/0 and proto tcp