Работа системы «MITIGATOR»

Система «MITIGATOR» предназначена для защиты от сетевых атак типа DDoS. Механизмы борьбы с атаками различного типа реализованы в системе в виде модулей, называемых ***контрмерами***.

Все защищаемые сервисы обладают собственной спецификой работы. Из-за этого на каждый из них могут осуществляться атаки разного типа. Способы отражения будут так же различными.

Поэтому существует задача индивидуального конфигурирования контрмер для разных сервисов. Эта задача решается разделением общего потока трафика на отдельные ветки обработки – ***политики защиты***. Политика объединяет в себе набор контрмер, которые могут быть индивидуально настроены. За распределение по политикам отвечают ***правила маршрутизации трафика***.

Порядок обработки сетевого трафика

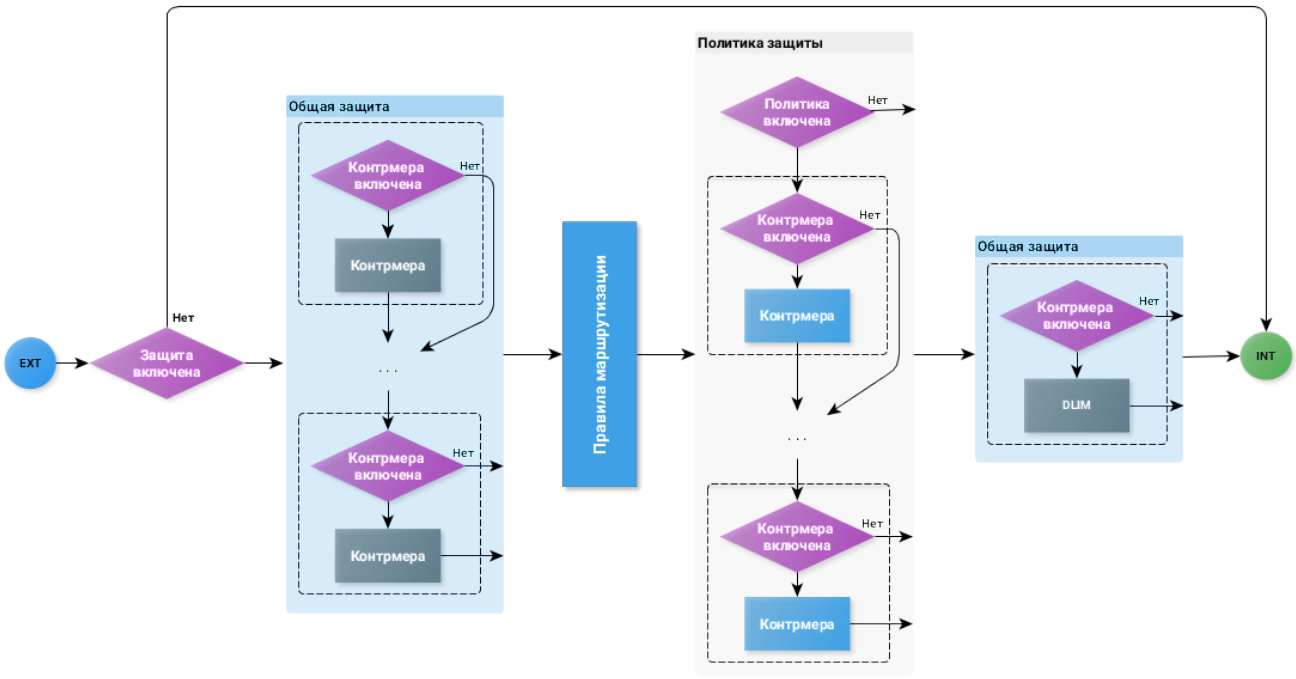
Система «MITIGATOR» обрабатывает трафик протокола IP четвертой версии (IPv4). Трафик других протоколов сетевого уровня модели OSI пропускается без обработки всегда. Элементарной обрабатываемой единицей является сетевой пакет протокола IPv4. Весь поступающий трафик может быть пропущен без обработки, если система защиты не активирована.

В первую очередь, после попадания трафика в систему, если система защиты включена, то для всех пакетов обязательно проводится валидация заголовков протокола IPv4.

Далее весь трафик сначала обрабатывается глобальными контрмерами, которые должны быть применены на весь сетевой трафик. После прохождения глобальных контрмер, трафик распределяется на разные политики защиты, где обрабатывается в соответствии с индивидуальными настройками политики. Для распределения применяются правила маршрутизации.

На выходе с политик весь трафик попадает на глобальную контрмеру *«Ограничение трафика на IP-адрес получателя».* Расположение данной контрмеры перед выходом системы позволяет предотвратить отказ защищаемого ресурса, если остальные контрмеры были отключены или оказались неэффективны.

Помимо главного переключателя активации системы защиты каждая политика и контрмера имеет собственные переключатели. Это позволяет более гибко настроить, какая обработка будет применена. Проще всего понять работу переключателей в системе, представив их как точку разветвления маршрутов следования пакетов. Активным является тот маршрут, на который указывает положение переключателя. Если переключатель находится в отключенном состоянии, то трафик идет по маршруту, на котором не производится обработка. Если переключатель находится во включенном состоянии, то трафик направляется по маршруту, на котором на него будет производиться воздействие контрмерами.



Изображение 1. Схема последовательности обработки сетевого трафика в системе.

Правила маршрутизации на политики защиты

Правила маршрутизации используются для распределения поступающего трафика на политики защиты.

Правила могут содержать пять параметров:

- протокол;
- префикс отправителя;
- порт отправителя;
- префикс получателя;
- порт получателя.

Правила разделены на три части:

1. Пред-правила;
2. Групповые правила;
3. Пост-правила.

Разделение необходимо для того, чтобы обеспечить ограничение доступа к правилам для пользователей с разными типами учетных записей.

Пред и пост-правила могут быть доступны только пользователям с системной ролью. Групповые правила могут быть доступны как пользователям с системной ролью, так и с групповой ролью. Пользователю с групповой ролью доступны только правила группы, в которой состоит пользователь.

Такое разграничение доступа позволяет на пред-правилах обработать трафик, который не должен попадать в группы. А весь трафик, который не был по каким-то причинам распределен групповыми правилами, будет обработан пост-правилами.

Порядок применения правил

Поступающие пакеты проверяются последовательно на соответствие каждому правилу. Если пакет удовлетворяет правилу, то он направляется на политику защиты, на которую указывает данное правило. Первыми отрабатывают пред-правила, потом групповые правила, затем пост-правила.

Групповое правило обязательно должно содержать префикс получателя. Поэтому для групповых правил не важен порядок следования групп. Но важен порядок следования правил внутри одной группы.

В пред и пост-правилах можно создать пустое правило не содержащее значений параметров. Тогда все пакеты, попавшие на это правило, будут направляться на указанную в правиле политику.

Если пакет не соответствует ни одному из заданных пользователями правил, тогда сработает правило по умолчанию, которое направит пакет на политику «По умолчанию». Правило по умолчанию не содержит значений ни одного из параметров, поэтому правилу удовлетворяет любой пакет. Правило по умолчанию всегда существует и находится в конце списка правил. Оно не может быть изменено.

Задание правил маршрутизации

В качестве значения протокола указываются номера протоколов транспортного уровня, инкапсулируемых в протокол IPv4. Диапазон допустимых значений от 0 до 255. Наиболее часто применяемы протоколы могут указываться по названию: tcp, udp, icmp.

Префикс отправителя или получателя могут содержать IP-адрес или подсеть в нотации CIDR.

Порт отправителя или получателя используются для указания номеров сетевых портов протоколов TCP и UDP. Диапазон допустимых значений от 0 до 65535.

Каждый параметр может содержать несколько значений.

Подсчет трафика

Многие контрмеры системы оперируют скоростью трафика в битах в секунду. Значения скорости трафика указываются в параметрах автодетектирования и отображается на графиках системы. Поэтому важно понимать, какие данные учитываются при подсчете скорости сетевого трафика. Хотя система обрабатывает только пакеты протокола IPv4, подсчет размера выполняется для всего Ethernet-кадра. Это удобно для сравнения со значениями трафика, получаемыми из других устройств в сети, работающих на уровне L2 модели OSI.

Подсчет размера происходит от начала заголовка Ethernet-кадра до начала FCS (Frame check sequence), не включая его. Заголовок GRE не учитывается, если он снят системой в процессе обработки.

Группы

Система может использоваться для защиты сервисов, принадлежащих разным клиентам. Для обеспечения этой возможности применяется разделение на группы внутри системы. Определяющим параметром группы является список префиксов получателя. Группа может иметь доступ и влиять только на трафик с указанными префиксами. Поэтому в групповых правилах префикс получателя является обязательным полем.

Группу может создавать и настраивать пользователь с системной ролью, обладающей соответствующими правами создания и редактирования групп.

Каждая группа обладает набором персональных сущностей, которые должны быть доступны только пользователям данной группы:

- политики защиты;
- правила маршрутизации;
- учетные записи пользователей.

Персональные сущности группы недоступны другим группам.

Права

Права определяют возможность доступа к функциям и сущностям системы. Права могут иметь три состояния:

- право отсутствует;
- чтение;
- запись – включает возможности изменения и создание.

Права могут иметь до трех уровней вложенности. Если роль обладает правом, то она будет обладать всеми вложенными правами нижестоящих уровней. Если же у роли нет хотя бы одного из вложенных прав, то не будет вышестоящего права. Например, в право на политики защиты вложены права на все контрмеры политик. В право на контрмеру вложены права на переключение состояния контрмеры и ее параметры. Если выдать права на политики защиты, появляются права на все контрмеры политики (на переключение и параметры). Если снять право на доступ к параметрам любой из контрмер, то будет снято право на эту контрмеру и право на политики защиты. Права на все остальные контрмеры политики при этом сохранятся.

Роли

Роли объединяют в себе набор прав. И служат удобству поиска и назначения типовых наборов прав учетным записям пользователей.

Типы ролей

В системе присутствует три типа ролей:

- Системная привилегированная роль – доступны все функции системы. Роль предназначена для управления настройками системы, администрирования других ролей, заведения новых учетных записей.
- Системные роли – могут обладать всеми теми же возможностями, что и системная привилегированная роль. Но набор возможностей определяется назначенными правами. Такие роли используются для ограниченного доступа только к определенным функциям системы.
- Групповые роли – имеют доступ только к сущностям, используемым группами. Назначаются учетным записям групповых пользователей. Такие роли могут обладать правами администратора группы – могут создавать новые правила, политики, регистрировать новых пользователей.

Тип существующей роли не может быть изменен.

Предустановленные роли

Сразу после установки в системе будет создано несколько ролей. При необходимости их можно изменить или удалить. Кроме роли «Администратор системы».

Название роли	Тип роли	Права на чтение	Права на запись
Администратор системы	Системная привилегированная роль	Полные	Полные
Пользователь системы	Системная роль	Включение защиты Мониторинг и состояние системы Политики защиты Правила маршрутизации Журнал событий Группы Роли Профили пользователей	Собственный профиль пользователя
Администратор группы	Групповая роль	Политики защиты Правила маршрутизации Журнал событий Группы Роли	Профили пользователей Собственный профиль пользователя
Пользователь группы	Групповая роль	Параметры политики Правила маршрутизации Журнал событий	Контрмеры политики Собственный профиль пользователя
Просмотр группы	Групповая роль	Политики защиты Правила маршрутизации Журнал событий Собственный профиль пользователя	

Обновление ролей

При обновлении у роли будут автоматически появляться права на новые функции, если до обновления у роли было вышестоящее право. Например, если у роли было право на политики защиты, то после обновления у роли будут права на новые контрмеры в политиках. Если же у роли были права только на некоторые контрмеры политики, то новая контрмера не будет доступна.

Предустановленные роли, созданные при установке системы, обновляются по такому же принципу.

Учетные записи пользователей

Пользователи, работающие с системой, осуществляют доступ к функциям системы с определенной учетной записью. Для каждой учетной записи обязательным являются имя и фамилия пользователя, логин, пароль и роль для аутентификации и авторизации пользователя.

Через роль учетной записи определяются права пользователя.

Запрещено изменение типа роли существующей учетной записи с системной на групповую и наоборот. Это означает, что учетной записи с системной ролью не может быть назначена групповая роль, а учетной записи с групповой ролью нельзя назначить системную роль.

Учетная запись группового пользователя не может быть перенесена из одной группы в другую.

Предустановленные учетные записи

После установки в системе будут присутствовать две предустановленные учетные записи.

Имя пользователя	Роль пользователя	Логин	Пароль
Администратор Системы	Администратор системы	admin	admin
Пользователь Системы	Пользователь системы	user	user

Функция определения политики по содержимому пакета

Если нужно понять, на какую политику защиты направят сетевой пакет правила маршрутизации, можно воспользоваться функцией определения политики по содержимому пакета. Для корректного определения политики нужно указать значения всех пяти параметров, по которым правила маршрутизации распределяют пакеты.

Функция захвата пакетов

Захват пакетов не является контрмерой и не предназначен для защиты. Функция захвата пакетов позволяет сохранить содержимое проходящих сетевых пакетов в файл для дальнейшего анализа.

Важно. Захват пакетов одновременно не может быть запущен несколькими пользователями. Если захват был запущен одним пользователем, то другие в это время смогут наблюдать индикацию процесса.

Взаимодействие по протоколу BGP

Система может установить соединение с несколькими BGP-соседями и анонсировать указанный пользователем список префиксов. Эта возможность будет полезна в случае интеграции «MITIGATOR» в сеть организации по схеме, когда трафик направляется на обработку только по необходимости. А в остальное время следует в обход системы.

Для реализации такого способа защиты предварительно нужно задать параметры и установить соединения с BGP-соседом. Это может быть маршрутизатор, отвечающий за распределение сетевых потоков во внутренней сети организации. Тогда в нужный момент по команде пользователя система будет анонсировать префиксы, трафик которых следует направлять на обработку.

Система способна получать от соседей и рассылать правила BGP Flow Specification (FlowSpec). Анонсирование префиксов, рассылка и получение FlowSpec-правил могут быть активированы независимо друг от друга.

Контрмеры валидации заголовков протоколов

Контрмера выполняет проверку заголовков пакетов протоколов IP, TCP, UDP, ICMP на соответствие стандартам RFC. Все пакеты, не соответствующие требованиям стандартов, безусловно сбрасываются.

Проверка IP-заголовков выполняется в первую очередь после попадания пакета в систему.

Заголовки протоколов TCP, UDP, ICMP проверяются на входе в политику защиты.

Контрмера «Блокировка по IP-адресу отправителя»

Контрмера предназначена для блокирования трафика, приходящего с заданных IP-адресов. При прохождении сетевого пакета через контрмеру выполняется проверка присутствия IP-адреса отправителя в списке блокировки. Если адрес есть в списке, то пакет направляется на сброс.

В качестве значений принимаются как отдельные IP-адреса, так и подсети в нотации CIDR. Заданные подсети разбираются контрмерой на IP-адреса, каждый адрес хранится во внутреннем представлении отдельно. Поэтому возможно сначала задать подсеть, после чего удалить отдельные адреса заданной ранее сети, сохранив остальные.

Важно. Контрмера *«Блокировка по IP-адресу отправителя»* в составе политик защиты может хранить ограниченное количество адресов. Максимально возможно указать 12582912 адресов.

Контрмера «Временная блокировка по IP-адресу отправителя»

Контрмера временно блокирует трафик, приходящий с заданного IP-адреса. В качестве значений принимаются как отдельные IP-адреса, так и подсети в нотации CIDR. Время блокировки указывается при занесении адресов в список. Если время не было указано явно, то адрес будет заблокирован на 300 секунд.

Контрмера всегда находится в активном состоянии. Поэтому блокирование трафика будет просисходить сразу после добавления адресов в список блокировки.

Адреса в список временной блокировки могут добавлять другие контрмеры. Критерии и время блокировки указывается в настройках той контрмеры, которая добавляет значения в список.

Контрмера «Фильтрация по странам»

Контрмера блокирует сетевой трафик по IP-адресу отправителя. Правила блокирования формируются на основании заданного пользователем списка стран и базы данных, которая хранит сопоставленный список стран и IP-адресов, выделенных для использования в этих странах.

В зависимости от настроек контрмера может либо пропускать трафик только из выбранных стран, либо сбрасывать трафик из этих стран.

Контрмера «Обработка фрагментированных пакетов»

Контрмера включена всегда, когда активирована защита. Потому что для корректной дальнейшей обработки фрагментированных пакетов необходимо выполнить пересборку этих пакетов. Контрмера позволяет выбрать три типа действий над фрагментированными пакетами: фрагменты могут быть пересобраны и направлены на дальнейшую обработку контрмерами системы; все фрагментированные пакеты могут быть сброшены; фрагментированные пакеты могут быть пропущены без обработки. В последнем случае, фрагментированные пакеты смогут быть обработаны только контрмерой *«Ограничение трафика на IP-адрес получателя»*.

Если применяется пересборка, то при получении IP-пакета с признаком фрагмента, контрмера сохраняет его. После получения всех фрагментов, выполняется пересборка исходного пакета. Пересобранный пакет направляется для обработки на следующие контрмеры.

Фрагменты хранятся ограниченное время. Если за это время не были получены все фрагменты исходного пакета, то хранимые фрагменты будут сброшены.

Для предотвращения атак фрагментированными пакетами применяется ограничение числа пропускаемых фрагментированных пакетов. Ограничение применяется независимо от выбранного типа действия над фрагментированными пакетами.

При включении пересборки, все фрагменты одного пакета будут обрабатываться контрмерами как одно целое. Но на всех счетчиках, графиках системы и при захвате пакетов каждый фрагмент будет учитываться отдельно.

Важно. Если исходный пакет разбит более чем на 4 фрагмента, то он не будет пересобран. Все фрагменты будут сброшены.

Контрмера «Фильтрация по правилам»

Контрмера фильтрует сетевые пакеты в соответствии с заданными правилами. Проверка пакетов на соответствие правилам происходит в порядке следования правил в списке.

Правила могут включать девять параметров:

- сетевой протокол (protocol);
- префикс отправителя (src);
- порт отправителя (sport);
- префикс получателя (dst);
- порт получателя (dport);
- ICMP-тип (icmp-type);
- ICMP-код (icmp-code);
- TCP-флаги (tcpflags);
- длина пакета (len).

Синтаксис правил фильтрации

```
acl ::= <entries>
entries ::= <entry> | <entry> "\n" <entries> "\n"
entry ::= <action> <components>
    action ::= "pass" | "drop"
    components ::= <> | <component> | <component> <components>
    component ::=
    "dst" <one-or-many prefix>
    | "src" <one-or-many prefix>
    | "protocol" <one-or-many protocol>
    | "port" <one-or-many port>
    | "dport" <one-or-many port>
    | "sport" <one-or-many port>
    | "icmp-type" <one-or-many icmp-type>
    | "icmp-code" <one-or-many icmp-code>
    | "tcpflags" <one-or-many tcp-flags>
    | "len" <one-or-many len>
    | "tcp"
    | "udp"
    | "icmp"

    prefix ::= <IP-адрес> | <IP-адрес с маской>
    protocol ::= "tcp" | "udp" | "icmp" | <range>
    port ::= <range>
    icmp-type ::= <range>
```

```
    icmp-code ::= <range>
    tcp-flags :: <flags>"/"<flags> | <>"/"<flags>
    len ::= <range>

    range ::= <число> | <число>"-"<число>
    flags ::= <flag> | <flag><flags>
    flag ::= "F" | "S" | "R" | "P" | "A" | "U" | "E" | "W"

    # Правила высшего порядка — это такие два правила, которые принимают аргументом другое правило:
    one-or-many C ::= C | "(" <many C> ")"
    many C ::= C | C " " <many C>
```

Пояснения:

- каждое правило – это действие «drop» или «pass» и набор компонентов;
- «component» – это одно из ключевых слов с последующим значением или несколькими значениями соответствующего типа;
- несколько значений записываются в скобках через пробел;
- диапазон пишется либо как одно число, либо как два числа через тире;
- «tcpflags» определяется двумя значениями – «флаги/маска», где «маска» задает набор проверяемых TCP-флагов, а «флаги» указывает, какие из них должны быть установлены (например: «S/SA» означает флаг SYN без флага ACK; «/A» означает проверку отсутствия флага ACK);
- есть три ключевых слова для обозначения protocol-ов – «tcp», «udp» и «icmp», которые могут употребляться как вместе с ключевым словом «protocol», так и без него;
- «len» – длина IP-пакета, включая IP-заголовки;
- при указании диапазона <range>, значение верхней границы диапазона должно быть больше значения нижней границы;
- для указания однострочного комментария используется символ «#»;
- формат записи правил регистронезависим.

Допустимые диапазоны <range> для различных компонент правила:

- port: 0-65535;
- protocol: 0-255;
- icmp-type: 0-255;
- icmp-code: 0-255;
- len: 0-65535.

Примеры правил фильтрации

```
PASS dst (1.1.1.1 22.22.22.22 205.12.12.1/30)
PASS protocol (udp 27 tcp 30-32)
DROP dport 80-2000 sport (4000 4001 5555)
DROP tcp tcpflags (S/SA A/FA) len 512-610
DROP icmp icmp-type (0-2 8) icmp-code 0
DROP dst 1.1.1.1 src 3.3.3.3/16 protocol tcp dport 80 sport 4000 tcpflags S/SA len 512
# следующее правило сбрасывает любые IP-пакеты
DROP
```

Контрмера «Фильтрация по FlowSpec-правилам»

Контрмера применяет для фильтрации проходящего трафика FlowSpec-правила, получаемые по протоколу BGP от BGP-соседей.

Синтаксис правил аналогичен синтаксису контрмеры *«Фильтрация по правилам»*.

Контрмера «Фильтрация по регулярным выражениям»

Контрмера выполняет фильтрацию сетевого трафика по регулярному выражению в формате PCRE (Perl-compatible regular expressions). Пакет будет сброшен, если в теле пакета (в payload протоколов TCP, UDP, ICMP) найдена строка, удовлетворяющая одному из заданных регулярных выражений.

Синтаксис правил фильтрации

Контрмера позволяет указать три типа действий над пакетами, удовлетворяющими заданному регулярному выражению:

- PASS – пропустить;
- DROP – сбросить;
- BLOCK – сбросить пакет и добавить IP-адрес отправителя в список блокировки контрмеры «Временная блокировка по IP-адресу отправителя».

Для действия BLOCK можно указать значение времени в секундах, на которое нужно заблокировать IP-адрес. Если время не указано, то адрес будет заблокирован на 300 секунд.

Если тип действия не указан, то будет применяться DROP.

Если содержимое пакета удовлетворяет регулярным выражениям из нескольких правил, то сработает правило с менее специфичным регулярным выражением.

Примеры регулярных выражений

Блокировка на 10 минут IP-адресов, с которых осуществляется атака на переполнение буфера IMAP-сервера:

```
BLOCK 600 \sLOGIN\s[^\n]{100}
```

Блокировка запросов от Android-устройств:

```
DROP ^User-Agent\x3a[^\r\n]*android
```

Блокировка попыток подключения к роутеру с паролем по умолчанию:

```
^Authorization\x3a(\s*|\s*\r?\n\s+)Basic\s+OmFkbWlu
```

Контрмера «Ограничение трафика»

Контрмера ограничивает скорость проходящего через нее сетевого трафика. Ограничение может быть задано отдельно в пакетах в секунду и в битах в секунду. Или одновременно обоими способами. Такая возможность позволяет гибко подстраивать контрмеру под особенности работы защищаемого сервиса и адаптировать защиту под специфику атаки.

Контрмера «Ограничение трафика на IP-адрес получателя»

Контрмера позволяет задать ограничение скорости проходящего трафика, адресованного на конкретный IP-адрес получателя. Ограничения могут быть заданы на скорость в пакетах в секунду и битах в секунду или одновременно двумя способами. В качестве параметров контрмера принимает список значений, состоящих из IP-адреса получателя и одного или двух значений ограничений.

Контрмера «Защита от атак на протокол TCP»

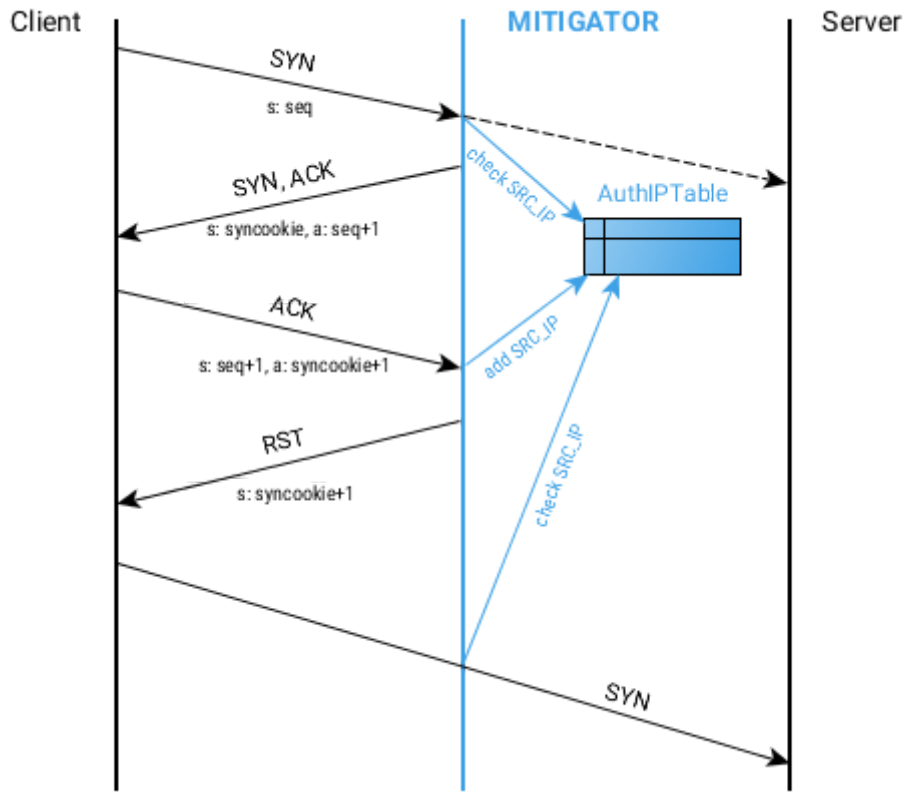
Контрмера предназначена для защиты от атак, основанных на особенностях работы протокола TCP. В первую очередь защищает от различного рода атак типа flood с подменой IP-адреса отправителя сетевого пакета. Для этого контрмера, используя проверки, наполняет таблицу аутентифицированных IP-адресов.

В усиленном режиме контрмера хранит, помимо IP-адреса отправителя, ещё и TCP-порт. Это позволяет защищаться от атак, когда злоумышленник каким-либо образом выяснил IP-адреса реальных клиентов, и подставляет их в атакующие пакеты. Если включен усиленный режим, то не следует устанавливать режим защиты от SYN flood атак *Проверять сбросом TCP-сессии*.

Защита от SYN flood атак

При включенной защите от SYN flood атак система проверяет все входящие пакеты, содержащие TCP-флаг SYN. Если IP-адрес отправителя пакета содержится в таблице аутентифицированных адресов, то пакет пропускается. Иначе выполняется проверка на то, что отправитель пакета существует и является легитимным пользователем. Метод проверки зависит от выбранного режима защиты от SYN flood атак.

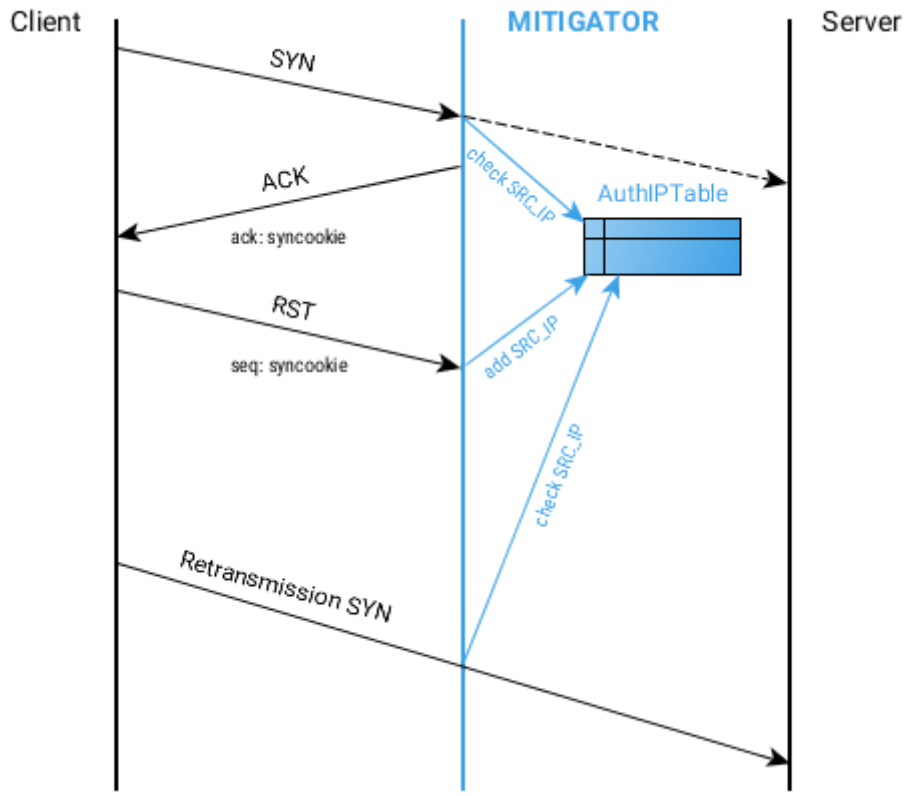
Если используется режим *«Проверять сбросом TCP-сессии»*, от лица сервера выполняется установление TCP-сессии, подтверждение cookie, вносится запись в таблицу аутентифицированных IP-адресов. После удачной аутентификации пользователя, ему направляется пакет с флагом RST. Что приводит к сбросу установленной TCP-сессии. При таком способе аутентификации пользовательское программное обеспечение должно поддерживать повторную установку TCP-соединения, иначе пользователю придется инициировать соединение заново своими действиями.



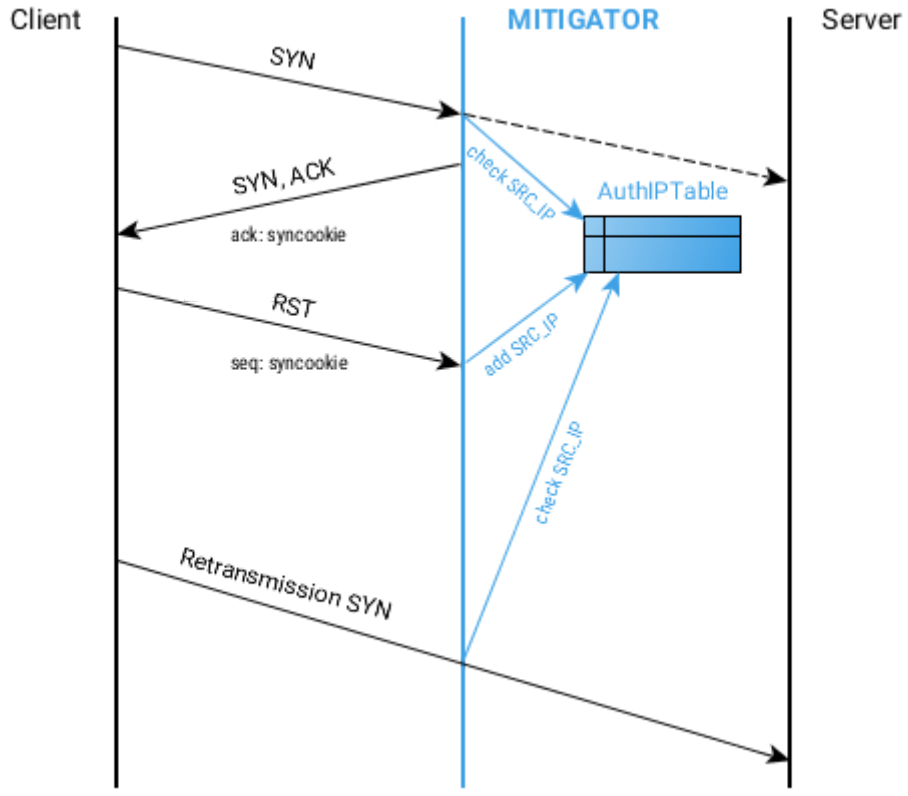
Изображение 2. Работа в режиме «Проверять сбросом TCP-сессии».

В основе работы других трех режимов лежит одинаковый принцип «проверки ответом». Принцип заключается в том, чтобы вынудить проверяемого пользователя прислать ответный пакет с флагом RST и подтверждением cookie в поле Sequence number. После чего легитимный пользователь должен выполнить повторную посылку пакета (согласно RFC 793 и его обновлениям), который уже будет пропущен системой. Разница в работе режимов заключается только в том, с каким набором TCP-флагов будет отправлен пакет в ответ на пришедший SYN-пакет. Соответственно для трех режимов работы ответный пакет будет содержать TCP-флаги: ACK; SYN и ACK; FIN и ACK.

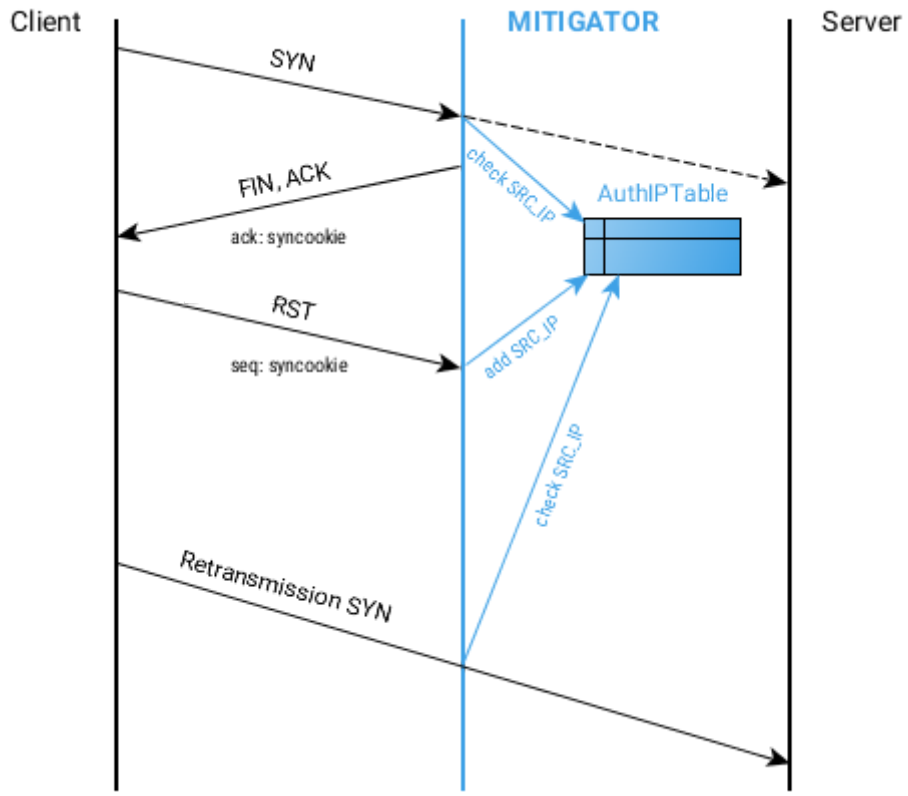
Существует способ обхода SYN flood защиты, когда сначала выполняется корректная аутентфикация. После чего генерируется SYN flood атака от лица аутентифицированного адреса. Для предотвращения обхода защиты таким способом существует ограничение количества SYN-пакетов, которое может быть пропущено. После достижения данного ограничения повторно выполняется процедура аутентификации.



Изображение 3. Работа в режиме «Проверять ответом на ACK».



Изображение 4. Работа в режиме «Проверять ответом на SYN+ACK».



Изображение 5. Работа в режиме «Проверять ответом на FIN+ACK».

Защита от SYN+ACK flood атак

Если контрмера включена, то безусловно проводится проверка пакетов, содержащих оба флага SYN и ACK. Если пакет пришел от неаутентифицированного адреса, то будет проведена проверка ответом на ACK-пакет.

Защита от ACK flood атак

Защита от ACK flood атак имеет три режима работы: *«Пропускать»*, *«Проверять»*, *«Проверять сбросом»*. В режиме *«Пропускать»* сетевые пакеты, содержащие TCP-флаг ACK будут пропущены без проверки. При включении механизма защиты от ACK flood атак в режиме *«Проверять»* входящие пакеты, содержащие флаг ACK (кроме SYN+ACK пакетов) начинают проверяться по таблице аутентифицированных адресов. Пакеты, IP-адрес отправителя которых отсутствует в таблице, сбрасываются. Поэтому механизм защиты от ACK flood атак может работать только совместно с защитой от SYN flood атак. Иначе включение защиты от ACK flood приведет к сбросу всех существующих сессий в момент включения механизма. Так как, если механизм SYN flood защиты не использовался до включения ACK flood защиты, то таблица аутентифицированных адресов пуста. Чтобы этого не происходило, после включения ACK flood защиты заданное количество времени механизм должен работать в режиме *«Проверять сбросом»*. В этом режиме, все приходящие пакеты, содержащие флаг ACK, и IP-адрес отправителя которых не обнаружен в таблице аутентифицированных адресов, дополнительно проверяются. Первый пришедший ACK-пакет запоминается и сбрасывается. Если повторно приходит точно такой же ACK-пакет, то он будет пропущен, а IP-адрес отправителя добавлен в таблицу аутентифицированных адресов с нулевым значением счетчика SYN-пакетов. Таким образом выполняется дополнительная проверка существования реального отправителя и TCP-сессии.

Защита от RST flood атак

Защита от RST flood атак имеет три режима работы. В режиме *«Пропускать»* сетевые пакеты, содержащие TCP-флаг RST будут пропущены без проверки. Режим *«Проверять»* подразумевает проверку наличия IP-адреса отправителя в таблице аутентифицированных адресов. Если адрес присутствует в таблице, то пакет пропускается, иначе сбрасывается. В режиме *«Сбрасывать»* все RST-пакеты будут безусловно сброшены.

Действия механизма защиты от RST flood атак не распространяется на RST-пакеты, которые являются ответами на отправленные пакеты в режиме «проверка ответом» и содержат cookie.

Контрмера «Защита от Slowloris атак»

Атаки Slowloris направлены на исчерпание всех свободных соединений на атакуемом сервере. Достигается это удержанием открытых соединений максимально долгое время за счет отправки фрагментированных HTTP-заголовков.

Для борьбы с атакой контрмера отслеживает соединения на указанные TCP-порты и проверяет по двум критериям: 1. число фрагментов HTTP-заголовка не превышает заданное значение; 2. задержки между фрагментами не превышают заданное значение.

Если число фрагментов превысило допустимое, то IP-адрес направляется на блокировку в контрмеру *«Временная блокировка по IP-адресу отправителя»*, а все соединения с этого адреса закрываются, отправкой на сервер TCP-пакета с флагом RST.

Если обнаружено, что для соединений с какого-либо IP-адреса слишком часто возникает задержка более допустимой между фрагментами запроса, то IP-адрес направляется на блокировку в контрмеру «Временная блокировка по IP-адресу отправителя».

Контрмера «Защита от HTTP flood атак»

Контрмера предназначена для защиты от атак типа flood на протокол прикладного уровня HTTP. Если контрмера включена, то выполняется HTTP-аутентификация отправителя запроса. Если отправитель удачно проходит аутентификацию, то его адрес добавляется в таблицу аутентифицированных адресов для механизма HTTP flood зашиты. И дальнейшие запросы с этого адреса будут пропущены.

Для выполнения HTTP-аутентификации, после получения HTTP-запроса, контрмера отсылает специально сформированный ответ. Если на него от клиента приходит ожидаемый ответ, то аутентификация считается пройденной, а клиент перенаправляется на адрес исходного запроса.

Механизм контрмеры учитывает каждый TCP SYN-пакет, пришедший с аутентифицированного адреса. После достижения счетчиком заданного значения, отправителю снова потребуется пройти процедуру аутентификации.

Контрмера «Защита TLS методом аутентификации»

Контрмера обрабатывает TCP-трафик, приходящий с заданных сетевых портов. По умолчанию задан порт 443.

Защита может работать в двух режимах:

- Пассивный;
- Активный.

В пассивном режиме контрмера проверяет, что каждый приходящий пакет является пакетом протокола TLS. Если пакет не удовлетворяет критериям проверки, он сбрасывается.

В активном режиме выполняется аутентификация пользователей.

Все приходящие TCP-пакеты проверяются по таблице аутентифицированных адресов. Если адрес присутствует в таблице, то пакет будет пропущен.

Если адрес отправителя пакета отсутствует в таблице и пакет содержит флаг SYN, то в ответ будет отправлен пакет с флагами SYN+ACK, содержащий cookie. Ожидается, что легитимный клиент в ответ пришлет пустой пакет с флагом ACK – этот пакет будет сброшен.

После чего клиент должен прислать ACK-пакет с данными, содержащий «ClientHello» для начала установления TLS-соединения.

При получении ACK-пакета с данными от неаутентифицированного адреса, контрмера выполнит проверку cookie. После этого проверит, что в данных пакета содержится «ClientHello» протокола TLS, и добавит IP-адрес в таблицу аутентифицирвоанных клиентов.

Если адрес прошел аутентификацию механизмом активной защиты, то при добавлении в таблицу аутентифицированных адресов будет поставлен признак того, что адрес считается аутентифицированным для контрмеры *«Защита TCP»*.

Если в момент добавления в таблицу, окажется что адрес уже присутствует в таблице – был занесен другими механизмами, то счетчик числа запрососв до повторной аутентификации будет увеличен. К текущему значению, хранящемуся в таблице, будет добавлено значение, заданное в настройках контрмеры.

Контрмера «Защита TLS методом оценки интервалов»

Контрмера предназначена для борьбы с атаками типа flood внутри зашифрованного TLS-соединения, когда атакующий после корректной установки TLS-соединения начинает слать большое количество запросов. Борьба с такими атаками осложнена тем, что нет возможности проанализировать трафик внутри зашифрованного соединения без расшифровывания. Поэтому контрмера анализирует равномерность временных интервалов между пакетами каждого соединения. Основываясь на том, что межпакетные интервалы в соединении атакующего равны с большой точностью, вычисляются IP-адреса таких соединений, и добавляются в список контрмеры *«Временная блокировка по IP-адресу отправителя»*. Но в некоторых случаях и соединения легитимных клиентов могут вести себя подобным образом. Поэтому имеется ряд механизмов защиты от ложных срабатываний. Некоторыми из которых может управлять пользователь системы, изменяя параметры.

Для работы контрмеры необходимо задать значения параметров, характерных для трафика защищаемого ресурса. Пользователю трудно подобрать корректные параметры контрмеры без тщательного анализа трафика защищаемого сервиса. Поэтому контрмера имеет функцию обучения.

Обучение

В процессе обучения анализируется проходящий трафик. Контрмера включена, но в это время она не выполняет функцию защиты. В результате успешного прохождения обучения будут предложены оптимальные параметры контрмеры для проанализированного трафика.

Обучение следует проводить на легитимном трафике клиентов защищаемого сервиса в наиболее загруженные часы работы сервиса. Если характер трафика защищаемого ресурса изменится, то следует повторно выполнить подбор параметров.

Контрмера «Защита игровых серверов»

Контрмера обрабатывает трафик протокола UDP, приходящий только с портов диапазона 27000 – 28000 на порты того диапазона 27000 – 28000.

Контрмера предназначена для защиты игровых серверов для игр:

- Counter-Strike 1.6;
- Counter-Strike Source;
- Counter-Strike GO;
- Left 4 Dead 2;
- GTA San Andreas Multiplayer;
- Team Fortress 2.

Защита основана на особенностях игровых протоколов. Система проводит аутентификацию клиентов при попытке установления соединения.

При получении от клиента запроса на соединение с сервером, система отправляет в ответ специально сформированное значение. Если клиент в следующем пакете присылает это значение, то IP-адрес клиента заносится в таблицу аутентифицированных адресов. Не получив ответ от сервера, клиент повторит попытку установления соединения с сервером и будет пропущен системой.

Отдельно обрабатываются запросы на поиск серверов. Так как на такой тип запроса не происходит установка соединения между клиентом и сервером. Поэтому контрмера ограничивает количество таких запросов в секунду.

Контрмера «Защита от DNS flood атак»

Контрмера предназначена для защиты от атак на DNS-сервера и учитывает особенности работы протокола DNS.

Сначала все поступающие DNS-запросы проходят валидацию. Некорректные и пустые запросы сбрасываются.

Если DNS-запрос поступает по протоколу UDP, то выполняется проверка присутствия IP-адреса отправителя в таблице аутентифицированных контрмерой адресов. Если адрес ранее аутентифицирован, то запрос будет пропущен. Иначе отсылается ответ с установленным флагом Truncated (TC) в заголовке протокола DNS. Это означает, что отправитель должен повторить свой DNS-запрос по протоколу TCP.

Когда DNS-запрос поступает по протоколу TCP, на этапе установления TCP-соединения выполняется проверка присутствия адреса отправителя в таблице аутентифицированных контрмерой адресов. Если адрес присутствует, то запрос пропускается. Иначе выполняется процедура аутентификации по тем же алгоритмам, которые применяются механизмом *«Защита от SYN flood атак»*. После успешного прохождения процедуры аутентификации адрес считается аутентифицированным контрмерой.

Каждый TCP SYN-пакет и каждый UDP DNS-запрос с аутентифицированного адреса, проходящий через контрмеру, учитывается счетчиком. После достижения счетчиком заданного значения, отправителю снова потребуется пройти процедуру аутентификации.

Если адрес уже внесен в таблицу аутентифицированных адресов контрмерой *«Защита от атак на протокол TCP»*, то аутентификации считается пройденной и для контрмеры *«Защита от DNS flood атак»*.

Контрмера «Блокировка при превышении порогов»

Контрмера блокирует прохождение сетевых пакетов с IP-адреса, если трафик с этого адреса превышает заданный порог пакетов или бит в секунду. Блокировка происходит в момент, когда механизм контрмеры обнаруживает превышение порога. В зависимости от величины превышения может отличаться скорость срабатывания контрмеры. Блокировка сохраняется пока приходящий с адреса трафик превышает порог. Снимается блокировка, когда трафик опускается ниже порогового значения.

«GRE-туннель»

GRE-туннелирование может быть включено для трафика каждой политики защиты. Если туннелирование в политике включено, то трафик этой политики распаковывается перед попаданием в политику и запаковывается на выходе из политики.

GRE-туннелирование может быть включено даже если система защиты отключена, чтобы не нарушать работу клиентов, использующих туннелирование.

«GRE-туннель со сторонним сервисом»

Если организована предварительная обработка трафика защищаемого клиента удаленным сторонним сервисом, MITIGATOR позволяет реализовать доставку трафика от стороннего сервиса через GRE-туннель. В этом случае сторонний сервис анонсирует IP-адреса клиента, и получает его трафик. После обработки через GRE-туннель передает трафик на адрес MITIGATOR-а. MITIGATOR распаковывает полученный в туннеле трафик, выполняет дальнейшую обработку и отправку клиенту.

Обратный трафик от клиента может быть запакован и отправлен обратно через GRE-туннель на адрес внешнего сервиса. Для этого необходимо указать IP-адреса защищаемых клиентов, от которых трафик должен запаковываться в GRE-туннель.

«Ретрансляция syslog»

Получает от защищаемых клиентов данные журналов syslog на порт 2601 и выполняет пересылку на указанный внешний сервис, используя TLS-шифрование. Такая функция будет полезна, когда организована предварительная обработка трафика защищаемого клиента удаленным сторонним сервисом. Если сервис использует данные журналов с оборудования клиента для работы собственных алгоритмов обработки.

Управление системой через Web-интерфейс

В Web-интерфейсе системы экран разделен на три основные области: заголовок интерфейса сверху по ширине всего экрана; область меню слева; область страницы справа от меню. Заголовок и меню являются общими для всего интерфейса. В заголовке отображается название текущей страницы и справа индикаторы состояния подсистем. В области меню помимо пунктов меню находится кнопка выхода из Web-интерфейса и главный переключатель активации системы защиты *«Включить защиту»*.

В Web-интерфейсе каждая контрмера представлена собственной панелью. В каждой панели контрмеры есть переключатель состояния, позволяющий включить или отключить применение контрмеры к проходящему трафику. Сохранение состояния контрмеры происходит при нажатии на кнопку *«ПРИМЕНИТЬ»* в панели контрмеры.

Страница «Мониторинг»

На странице показаны графики входящего и исходящего трафика суммарно и на каждом сетевом порту устройства, графики трафика на очередях портов.

Порты, имеющие в названии префикс ***ext***, являются внешними портами, на которые должен поступать трафик, требующий очистки. Обработанный системой трафик отправляется через внутренние порты, имеющие в названии префикс ***int***. Обратный трафик по направлению от портов ***int*** к ***ext*** не подвергается обработке и его наличие не обязательно.

Графики очередей портов рисуются только в том случае, когда система по какой-то причине не успевает обработать весь поступающий трафик и сбрасывает часть пакетов на входе.

Страница «Общая защита»

На странице находятся элементы управления глобальными контрмерами, действие которых распространяется на весь проходящий трафик. Сетевые пакеты обрабатываются этими контрмерами до распределения по политикам защиты.

Панель «Рассылка BGP FlowSpec-правил»

Для выполнения рассылки FlowSpec-правил BGP-соседям предварительно необходимо задать собственные параметры системы в панели *«BGP-соединение»* и параметры подключения в панели *«BGP-соседи»* на странице *«Настройка системы»*.

Чекбоксы *«Устанавливать соединение»*, *«Отсылать FlowSpec»* и поля *«FlowSpec-правила»*, *«Community»* дублируют одноименные поля из панелей *«BGP-соединение»* и *«BGP-соседи»* на странице *«Настройка системы»*.

Правила могут быть предвариательно заданы в поле *«FlowSpec-правила»* и сохранены. Рассылка будет выполняться только после установки чекбокса *«Выполнять рассылку правил»*.

Панель «Захват пакетов»

В поле *«Число пакетов»* задается количество пакетов, которое необходимо захватить. После достижения заданного значения захват будет автоматически остановлен. Поле *«Семплирование»* используется для управления семплированием захвата. Значение 1 в этом поле означает, что будут захвачены все проходящие пакеты. Значение 100, что будет захвачен каждый сотый из проходящих пакетов.

После запуска захвата появится полоса индикации процесса со счетчиком уже захваченных пакетов. Захват можно остановить принудительно кнопкой «ОСТАНОВИТЬ» или дождаться автоматической остановки. После остановки, если были захвачены пакеты, появится ссылка для скачивания файла в формате PCAP.

Панель контрмеры «Блокировка по IP-адресу отправителя»

Панель содержит переключатель включения контрмеры, график сброшенного контрмерой трафика в пакетах и битах в секунду.

В панели присутствует многострочные поля для добавления значений в список IP-адресов и удаления значений из списка. Для добавления значения вводятся на закладке *«Добавление»*. Для удаления IP-адресов из списка блокировки нужно переключиться на закладку *«Удаление»*. Возможно указать отдельные адреса и подсети, которые должны быть удалены, или сбросить весь заданные для контрмеры список блокировки, нажав кнопку *«СБРОСИТЬ ВСЕ»*.

В качестве значений могут указываться как отдельные IP-адреса, так и подсети в нотации CIDR. Каждое значение должно вводиться на новой строке.

Через поле *«Адрес»* можно проверить присутствует ли IP-адрес в списке блокировки.

Панель контрмеры «Обработка фрагментированных пакетов»

В панели отсутствует переключатель состояния контрмеры. Контрмера *«Обработка фрагментированных пакетов»* всегда включена.

График показывает количество пришедшего на контрмеру, пересобранного и сброшенного контрмерой фрагментированного трафика в пакетах и битах в секунду.

Панель контрмеры «Фильтрация по правилам»

Панель содержит переключатель включения контрмеры, график сброшенного контрмерой трафика.

Если указаны значения портов, то правило будет применяться, если в пакете совпадает с заданными хотя бы один из портов отправителя или получателя.

Панель контрмеры «Фильтрация по FlowSpec-правилам»

Панель *«Правила фильтрации»* отображает FlowSpec-правила, получаемые от BGP-соседей и применяемые в данный момент.

Панель контрмеры «Фильтрация по регулярным выражениям»

Панель содержит переключатель включения контрмеры, график сброшенного контрмерой трафика в пакетах и битах в секунду.

Правила фильтрации по регулярным выражениям задаются в многострочном поле ввода *«Правила фильтрации»*. Каждое регулярное выражение вводится на новой строке. Сохранение правил происходит после нажатия на кнопку *«ПРИМЕНИТЬ»*'. Если при сохранении будут обнаружены ошибки в правилах, то в подсказке к полю будет выведен список строк, содержащих ошибки. Красным цветом будут подсвечены номера строк и сами ошибочные значения. Если навести курсор на номер строки, то можно увидеть пояснение ошибки.

Панель контрмеры «Ограничение трафика на IP-адрес получателя»

Панель содержит переключатель включения контрмеры, график сброшенного контрмерой трафика в пакетах и битах в секунду.

Все заданные на текущий момент ограничения можно увидеть в таблице *«Список ограничений»*. Если какое-то из ограничений сработало и в данный момент происходит сброс трафика, то в столбце *«Состояние»* будет отображаться иконка в виде восклицательного знака. В столбце *«Время задания»* указывается момент времени, когда было задано или изменено ограничение. *«Период срабатывания»* показывает суммарную продолжительность действия ограничения (когда сбрасывался трафик) с момента задания или последнего изменения ограничения. *«Время последнего срабатывания»* отображает момент времени, когда прекратился сброс трафика в последний раз.

Для добавления новых значений в таблицу нужно нажать на кнопку *«ДОБАВИТЬ ОГРАНИЧЕНИЕ»*. После этого в конце списка на странице появится строка с полями для ввода значений. Для удаления или редактирования существующих записей нужно нажать на соответствующие иконки в конце строки. Нельзя изменить значение IP-адреса получателя для ранее созданных ограничений. Сохранение всех изменений происходит после нажатия на кнопку *«ПРИМЕНИТЬ ИЗМЕНЕНИЯ»*.

Страница «Политики защиты»

Страница содержит список настроенных политик защиты. В этом списке можно видеть название политики, состояние самой политики и контрмер, миниатюру общего графика политики.

Для удаления политики служит кнопка *«УДАЛИТЬ ПОЛИТИКУ»* на странице управления политикой защиты в панели *«Настройка политики»*.

Страница управления политикой защиты

Поступающий в политику трафик может быть обработан контрмерами политики или пропущен без обработки в зависимости от состояния политики. Переключатель состояния политики находится в панели *«Настройки политики»*.

В каждой панели контрмеры есть собственный переключатель состояния, позволяющий включить или отключить применение контрмеры к проходящему через политику трафику.

Контрмера *«Проверка заголовком протоколов»* не имеет собственной панели управления и включена всегда, если включена политика защиты. Сброшенные данной контрмерой пакеты будут отражаться на суммарном графике сброшенного трафика в панели *«Общий график»*.

Панель «Общий график»

Общий график отражает значения вошедшего трафика и вышедшего с политики защиты. Так же показывает суммарное значение трафика, сброшенного всеми контрмерами данной политики.

На закладке *«IP-адреса»* показана динамика наполнения таблиц аутентифицированных адресов для контрмер политики.

Панель «Настройка политики»

Панель содержит переключатель состояния политики. Если переключатель *«Включить защиту»* включен, значит политика защиты находится во включенном состоянии, и проходящий через нее трафик будет обрабатываться контрмерами политики. Если переключатель отключен, то трафик со входа политики будет перенаправляться сразу на выход политики.

В поле *«Название политики»* возможно изменить текущее название. По названию политику защиты можно идентифицировать в списке политик и при назначении правил маршрутизации. Название политики должно быть уникально. Если установлен чекбокс *«Автоматическое включение»*, то политика может быть включена по сигналу из syslog.

Под заголовком *«Правила маршрутизации на политику»* находится список ссылок на правила маршрутизации, указывающих на данную политику. По ссылкам происходит переход на страницу списка правил.

Политика *«По умолчанию»* не может быть удалена, ее название не может быть изменено.

Панель «Управление автодетектированием».

Панель содержит чекбоксы для включения механизма автодетектирования для всех контрмер, которые поддерживают автодетектирование. Ссылки *«Сбросить состояние»* могут быть применены для сброса накопленной статистики механизма автодетектирования.

В таблице ниже могут быть изменены и заданы специфичные параметры механизма автодетектирования.

Панель «Журнал событий»

Содержит список изменений параметров данной политики защиты.

Панель «Захват пакетов»

Панель полностью аналогична панели *«Захват пакетов»* на странице *«Общая защита»*.

Панель контрмеры «Блокировка по IP-адресу отправителя»

Панель управления контрмерой полностью аналогична панели контрмеры *«Блокировка по IP-адресу отправителя»* на странице *«Общая защита»*.

Панель контрмеры «Временная блокировка по IP-адресу отправителя»

Контрмера всегда находится в активном состоянии, поэтому не имеет переключателей для включения защиты.

Поле *«IP-адрес»* используется для того, чтобы проверить, занесен ли IP-адрес в список блокировки. Поле принимает в качестве значения только единичный IP-адрес.

Поле *«Заблокированный префикс»* применяется, когда нужно удалить значения из списка блокировки.

Для добавления адресов в список блокировки следует воспользоваться группой полей *«Добавление в список блокировки»*.

Весь список заблокированных адресов можно выгрузить в CSV-файл кнопкой *«Выгрузить»* или очистить кнопкой *«СБРОСИТЬ»*.

Панель контрмеры «Фильтрация по странам»

Пользователь в данной панели указывает перечень стран и действие, которое будет применено к трафику из указанных стран.

Важно. Для использования контрмеры сначала необходимо загрузить справочник стран на странице *«Настройка системы»* в панели *«Общие параметры контрмер»*.

Панель контрмеры «Фильтрация по правилам»

Панель управления контрмерой полностью аналогична панели контрмеры *«Фильтрация по правилам»* на странице *«Общая защита»*.

Панель контрмеры «Защита от атак на протокол TCP»

Панель содержит переключатель включения контрмеры. На графике отображается сброшенный трафик и сгенерированный контрмерой обратный трафик в пакетах и битах в секунду.

Под соответствующими заголовками в панели находятся элементы управления механизмами защиты от SYN flood, ACK flood, RST flood атак.

В поле *«Число SYN-пакетов до повторной аутентификации»* указывается значение числа SYN-пакетов, которое механизм пропустит до повторного выполнения процедуры аутентификации.

В поле *«Время работы в режиме CHECK (минут)»* задается время, которое механизм защиты от ACK flood будет работать в режиме *«CHECK»* до перехода в режим *«BLOCK»*.

Для проверки присутствия IP-адреса в таблице аутентифицированных адресов используется поле *«IP-адрес аутентифицированного клиента»* и кнопка *«ПРОВЕРИТЬ»*. При нажатии кнопки *«УДАЛИТЬ»* происходит удаление заданного в поле адреса из таблицы аутентифицированных адресов. Кнопка *«СБРОСИТЬ»* предназначена для удаления из таблицы аутентифицированных адресов всех IP-адресов, добавленных контрмерой *«Защита от атак на протокол TCP»* данной политики защиты.

Панель контрмеры «Защита от Slowloris атак»

Панель содержит переключатель включения контрмеры. На графике на вкладке *«Трафик»* отображается количество сбрасываемого трафика и отправляемого на сервер при закрытии соединения. На вкладке *«IP-адреса»* показано число уникальных IP-адресов, хранящихся в таблице отслеживаемых запросов.

Элемент интерфейса	Тип и диапазон значений	Описание
Число фрагментов	Целое 1 – 4294967295	Максимально допустимое число фрагментов HTTP-запроса.
Время ожидания	Целое 1 – 4294967295	Максимально допустимое время задержки между фрагментами запроса. Указывается в секундах.

Элемент интерфейса	Тип и диапазон значений	Описание
Допустимое число нарушений времени	Целое 1 – 4294967295	Максимально допустимое количество раз, когда обнаружены задержки между фрагментами запроса.
Длительность блокировки	Целое 1 – 2147483647	Время, на которое адрес будет заблокирован контрмерой *«Временная блокировка по IP-адресу отправителя»*.
Список портов HTTP	Список целых 0 – 65635	Список TCP-портов, трафик с которых анализирует контрмера.
Сбросить		Сбрасывает таблицу отслеживаемых соединений.

Панель контрмеры «Защита от HTTP flood атак»

Панель содержит переключатель включения контрмеры. На графике отображается сброшенный трафик и сгенерированный контрмерой обратный трафик в пакетах и битах в секунду.

В зависимости от положения переключателя *«Метод HTTP аутентификации»* изменяется содержимое ответов на запросы клиента. Шаблоны ответов можно видеть ниже в полях карточки. Применяется три разных шаблона. Первый шаблон применяется для ответа на GET-запрос клиента. Второй – для ответа на прочие типы HTTP-запросов. Третий шаблон используется для ответа клиенту после успешного прохождения им аутентификации. Если установить переключатель в положение *«Экспертный»*, то поля станут доступны для редактирования. Появится возможность прописать собственные шаблоны ответа.

При установке чекбокса *«Строгая аутентификация»* изменяется содержимое шаблона ответа на запросы отличные от GET.

В поле *«Список портов HTTP»* может быть задан список TCP-портов, на которых слушают защищаемые сервера, работающие по протоколу HTTP. Если в этом поле заданы значения, то контрмера будет обрабатывать только TCP-пакеты, у которых порт получателя равен заданным.

Панель контрмеры «Защита TLS методом аутентификации»

Панель содержит переключатель включения контрмеры и чекбокс активации автоматического детектирования. Если чекбокс установлен, то переключатель включения контрмеры становится неактивен. В таком состоянии пользователь не может управлять состоянием контрмеры, за это отвечает система автодетектирования.

В поле *«Список портов TLS»* указываются TCP-порты, страфик с которых следует обрабатывать.

Группа радиокнопок *«Метод TLS-аутентификации»* служит для переключения режимов работы контрмеры.

В поле *«Число запросов до повторной аутентификации»* указывается значение числа SYN-пакетов, которое механизм пропустит до повторного выполнения процедуры аутентификации.

Кнопка *«СБРОСИТЬ»* предназначена для удаления из таблицы аутентифицированных адресов всех IP-адресов, добавленных контрмерой.

Панель контрмеры «Защита TLS методом оценки интервалов»

Панель содержит переключатель включения контрмеры. На графике отображается количество сессий:

- всего отслеживаемых;
- признанных нелегитимными, IP-адреса которых направлены в блокировку;
- распознанных по признаку *«Не блокировать загрузку на сервер»*;
- распознанных по признаку *«Не блокировать при равных интервалах»*.

Элемент интерфейса	Тип и диапазон значений	Описание
Максимальное отклонение	Дробное 0.01 – 10	Порог числового показателя равномерности следования пакетов. Чем меньше показатель, тем более равномерен трафик соединения. Для легитимных клиентов показатель, как правило, не ниже 0,1. Если показатель для соединения меньше порога, IP-адрес отправителя блокируется.
Значимый межпакетный интервал	Целое 10 – 4294967296	Интервал следования пакетов, в котором они будут рассматриваться системой. Если пакеты следуют с большей задержкой, чем указанный интервал, то не будут учитываться в анализе. Поступление пакетов с высокой равномерностью и большой задержкой характерно, например, от систем мониторинга.
Время неактивности сессии	Целое 3 – 2147483647	Интервал неактивности сессии, после которого она перестает отслеживаться.
Список портов TLS	Список целых (до 8 значений) 0 – 65635	Список TCP-портов, трафик с которых анализирует контрмера.
Учитывать только пакеты с данными	Флаг	Признак указывает, что следует учитывать только пакеты TLS, содержащие данные (тип пакета Application Data по RFC 5246) и не учитывать служебные пакеты протокола TLS.
Не блокировать загрузку на сервер	Флаг	Признак, позволяющий не блокировать клиентов, ведущих загрузку данных на сервер. Потому что в момент передачи данных на сервер межпакетные интервалы имеют высокую равномерность.
Не блокировать при равных интервалах	Флаг	Признак, позволяющий не блокировать соединения, пакеты в которых следуют через интервалы, меньшие погрешности измерения. Такие соединения характерны для локальных клиентов – находящихся в том же сегменте сети, что и система защиты.
Длительность блокировки	Целое 1 – 2147483647	Время, на которое адрес будет заблокирован контрмерой *«Временная блокировка по IP-адресу отправителя»*.
Обучение		Раскрывает список рекомендованных параметров и элементы управления обучением. Если обучение не проводилось, рекомендованные значения будут отсутствовать.
Результаты обучения получены	Дата и время	Дата и время, когда было окончено последнее обучение и получены рекомендованные параметры.
Подобрать		Запускает обучение для подбора рекомендованных параметров.
Применить		Применяет параметры, подобранные при обучении.

Панель контрмеры «Защита игровых серверов»

Панель содержит переключатель включения контрмеры.

В поле *«Запросов на поиск серверов в секунду»* указывается допустимое число запросов данного типа.

Из выпадающего списка *«Тип сервера»* нужно выбрать название игры, сервера которой требуется защищать.

В зависимости от выбранной игры, для работы механизма может потребоваться указать значение *«Версия протокола»* – версия проткола, которую используют клиент и сервер. Протокол периодически обновляется разработчиками. Поэтому необходимо определить версию, которую использует защищаемый сервер. Для этого нужно запустить игровой сервер, открыть консоль нажатием клавиши «~». Ввести в консоли команду «version» и нажать «Enter». В результате выполнения команды, в консоли должно быть выведено целое число. Это число нужно вписать в поле *«Версия протокола»*.

Кнопка *«СБРОСИТЬ»* предназначена для удаления из таблицы аутентифицированных адресов всех IP-адресов, добавленных контрмерой

Панель контрмеры «Защита от DNS flood атак»

Панель содержит переключатель включения контрмеры и чекбокс активации автоматического детектирования. Если чекбокс установлен, то переключатель включения контрмеры становится неактивен. В таком состоянии пользователь не может управлять состоянием контрмеры, за это отвечет система автодетектирования. На графиках отображается отдельно трафик, сброшенный на этапе валидации, сброшенный контрмерой и сгенерированный контрмерой обратный трафик.

В поле *«Число запросов до повторной аутентификации»* указывается число DNS-запросов, которые механизм пропустит прежде чем потребует повторного выполнения процедуры аутентификации.

Панель контрмеры «Фильтрация по регулярным выражениям»

Панель содержит переключатель включения контрмеры, график сброшенного контрмерой трафика.

Если указаны значения портов, то правило будет применяться, если в пакете совпадает с заданными хотя бы один из портов отправителя или получателя.

Элемент интерфейса	Тип и диапазон значений	Описание
Правила фильтрации	Строка	Правила фильтрации. Каждое правило вводится на новой строке.
Остальные пакеты	Радиокнопка	Действие, которое будет применено для пакетов, не удовлетворяющих ни одному из правил.
Время блокировки по умолчанию(секунд):	Целое 1 – 1073741823	Время, на которое адрес будет заблокирован контрмерой «Временная блокировка по IP-адресу отправителя», если для правила «BLOCK» явно не указано время блокировки. Применяется так же для блокировки отправителей «остальных пакетов», если выбрано значение «Блокировать».

Элемент интерфейса	Тип и диапазон значений	Описание
Применять правила только для TCP-пакетов с портами: Порты отправителя	Список целых (до 16 значений) 0 – 65635	Список TCP-портов отправителя, для пакетов с которых будут применяться правила.
Применять правила только для TCP-пакетов с портами: Порты получателя	Список целых (до 16 значений) 0 – 65635	Список TCP-портов получателя, для пакетов на которые будут применяться правила.
Применять правила только для UDP-пакетов с портами: Порты отправителя	Список целых (до 16 значений) 0 – 65635	Список UDP-портов отправителя, для пакетов с которых будут применяться правила.
Применять правила только для UDP-пакетов с портами: Порты получателя	Список целых (до 16 значений) 0 – 65635	Список UDP-портов получателя, для пакетов на которые будут применяться правила.

Панель контрмеры «Блокировка при превышении порогов»

Контрмера позволяет отдельно управлять механизмами блокировок по превышению порога пакетов и порога бит. Поэтому в панели контрмеры представлены два набора элементов управления. Для каждого механизма блокировки имеется собственный переключатель включения и график сброшенного трафика. Для задания пороговых значений срабатывания механизмов используются соответственно поля *«Пакетов в секунду»*, *«Бит в секунду»*.

Механизмы могут быть включены по отдельности или одновременно оба.

Панель контрмеры «Ограничение трафика»

Контрмера позволяет отдельно управлять механизмами ограничения в пакетах и в битах. Поэтому в панели контрмеры представлены два набора элементов управления. Для каждого механизма ограничения имеется собственный переключатель включения и график сброшенного трафика. Для задания ограничений трафика используются соответственно поля *«Пакетов в секунду»*, *«Бит в секунду»*.

Механизмы могут быть включены по отдельности или одновременно оба.

Панель «GRE-туннель»

Панель содержит переключатель для включения туннелирования трафика данной политики.

Поля для указания IP-адресов участников, между которыми пересылается запакованный трафик.

Страница «Правила»

Страница содержит список всех правил маршрутизации сетевого трафика на политики защиты. Для каждого правила обязательно должна быть указана политика защиты, на которую отправляются пакеты, удовлетворяющие правилу.

Страница «Настройка системы»

На странице расположены элементы управления и параметры, влияющие на работу системы в целом, настройки интеграции системы в сетевую инфраструктуру организации, общие настройки контрмер, влияющие на все политики защиты.

Панель «Общие параметры контрмер»

В эту панель вынесены общие настройки контрмер всех политик защиты. Вносимые изменения будут влиять на контрмеры в каждой из используемых политик.

Чекбокс *«Использовать автодетектирование атак»* отвечает за включение системы автодетектирования. Если чекбокс снят, автоматическое включение и отключение контрмер не будет выполняться независимо от индивидуальных настроек автодетектирования контрмер.

Под заголовком *«Фильтрация по странам»* расположена кнопка для выбора и загрузки файла базы данных справочника стран GeoLite2. Скачать файл можно со страницы разработчика: http://dev.maxmind.com/geoip/geoip2/geolite2. Скачивать следует архив с базой стран в формате CSV. Данный файл архива загружается в систему как есть.

Под заголовком *«Защита от атак на протокол TCP»* находятся элементы управления одноименной контрмерой. Параметр *«Время жизни записи в таблице»* задает время хранения IP-адреса отправителя в таблице аутентифицированных IP-адресов. После истечения этого времени адрес будет удален из таблицы. Клиент должен будет снова пройти процедуру аутентификации.

Администратор системы может полностью очистить таблицу аутентифицированных IP-адресов, сбросив все значения кнопкой *«СБРОСИТЬ»*. Кнопка *«ВЫГРУЗИТЬ»* используется для получения содержимого таблицы аутентифицированных адресов в CSV-формате.

Важно. Очистка таблицы аутентифицированных IP-адресов приведет к разрыву уже установленных клиентских сессий, если используется режим *«BLOCK»* защиты от ACK flood атак.

Панель «BGP-соединение»

В данной панели задаются собственный параметры системы для установления BGP-соединения. Параметры BGP-соседей настраиваются в отдельной панели.

Чекбокс *«Устанавливать BGP-соединение»* отвечает за включение взаимодействия по протоколу BGP. Если чекбокс не установлен, то не будет выполняться установления соединения ни с одним из BGP-соседей.

Так же в данной панели задаются *«Анонсируемые префиксы»* и *«FlowSpec-правила»*, которые могут отсылаться каждому из BGP-соседей.

Синтаксис FlowSpec-правил аналогичен синтаксису контрмеры *«Фильтрация по правилам»*.

Панель «BGP-соседи»

Для создания нового BGP-соседа нужно нажать на иконку добавления справа от выпадающего списка *«BGP-сосед»*.

Чекбокс *«Устанавливать соединение»* определяет, будет ли выполняться установка соединения с данным BGP-соседом. Текущие состояние соединения отображает индикатор в панели справа.

Чекбоксы *«Принимать FlowSpec»*, *«Анонсировать префиксы»*, *«Отсылать FlowSpec»* определяют, какие виды взаимодействия с данным BGP-соседом будут применяться. Анонсируемые префиксы и FlowSpec-правила одинаковы для всех соседей и задаются в панели *«BGP-соединение»*.

Управлять соединением с BGP-соседом и рассылкой FlowSpec-правил можно так же из панели *«Рассылка BGP FlowSpec-правил»* на странице *«Общая защита»*.

Панель «Настройка интерфейса управления»

Настройки включают четыре поля: *«IP-адрес интерфейса»*, *«Маска подсети»* для указанного адреса, *«Шлюз по умолчанию»*, *«Сервер DNS»*.

После нажатия на кнопку *«СОХРАНИТЬ ПАРАМЕТРЫ»* указанные будут отправлены на сервер. В случае удачного применения настроек, Web-интерфейс системы будет доступен на новом адресе.

Важно. Заданные значения проверяются только на соответствие формату записи IP-адреса протокола IPv4. Поэтому на администратора системы ложится обязанность задания значений в соответствии с принятой в организации схемой маршрутизации. В случае указания некорректных настроек, это может привести к тому, что административный интерфейс системы будет недоступен. На этот случай предусмотрено наличие второго интерфейса управления. Настройки которого нельзя изменить.

Панель «Рассылка сообщений по Email»

Для того чтобы пользователям системы рассылались уведомления о событиях системы, необходимо задать параметры подключения к почтовому серверу.

Адреса рассылки уведомлений задаются для каждого пользователя системы на странице управления параметрами учетной записи пользователя.

Панель «Рассылка сообщений через syslog»

Система позволяет выполнять отправку сообщений о событиях одновременно на несколько syslog-серверов. Для того чтобы настроить отправку сообщений на определенный syslog-сервер, нужно создать «рассылку» с параметрами этого сервера.

Для создания новой рассылки нужно нажать на кнопку создания рассылки справа от поля *«Рассылки»*. Для сохранения каждой новой рассылки или применения изменений требуется нажать на кнопку *«СОХРАНИТЬ ПАРАМЕТРЫ»*.

Переключатель «Выполнять рассылку» позволяет включать или отключать отправку сообщений. Если рассылка создана, но переключатель *«Выполнять рассылку»* находится в выключенном состоянии, то отправка сообщений этой рассылки не будет происходить.

Панель «Настройка времени системы»

С помощью данной панели можно устанавливать значение времени и часовой пояс места расположения системы.

Время возможно задавать двумя взаимоисключающими способами. Для того, чтобы задать значение даты и времени явно, нужно заполнить поле *«Задать время»*. Или можно настроить периодическую синхронизацию с сервером точного времени. Для этого следует установить

чекбокс *«Выполнять синхронизацию с NTP-сервером»* и ввести IP-адрес или доменное имя в поле *«Адрес NTP-сервера»*.

Применение всех новых настроек и обновление времени произойдет после нажатия на кнопку *«СОХРАНИТЬ ПАРАМЕТРЫ»*

Панель «Обновление системы»

В панели отображается текущая используемая версия системы.

Для выполнения обновления, нужно выбрать файл архива обновления. И нажать кнопку *«УСТАНОВИТЬ ОБНОВЛЕНИЕ»*. После этого откроется диалоговое окно, отображающие процесс загрузки файла на сервер. Процесс можно прервать кнопкой *«ОТМЕНА»*. Как только файл будет полностью загружен, автоматически начнется установка новой версии. Некоторое время будет недоступен Web-интерфейс, будет приостановлено прохождение сетевого трафика через систему.

Панель «Управление системой»

После нажатия кнопки напротив пункта *«Сбросить настройки»* будет инициирован сброс всех параметров системы, которые были заданы пользователями в процессе эксплуатации. Будут удалены все созданные политики защиты, правила маршрутизации, пользователи системы. Сброшены будут все индивидуальные настройки системы кроме настроек интерфейса управления и параметров синхронизации с сервером точного времени. После сброса войти в интерфейс системы можно будет под учетной записью по умолчанию. При нажатии кнопки напротив пункта *«Перезагрузить систему»* будет выполнена перезагрузка оборудования, на котором развернута система. При нажатии кнопки напротив пункта *«Выключить электропитание»* будет выключено оборудование, на котором развернута система.

Панель «Установка SSL-сертификата»

Web-интерфейс системы взаимодействует с сервером системы через защищенное соединение по протоколу HTTPS. Для установления защищенного соединения используется пара из закрытого ключа и SSL-сертификата. В систему разработчиком загружены пара из ключа и самоподписанного SSL-сертификата.

Администратор системы может установить собственную ключевую пару. Для этого нужно выбрать соответствующие файлы и нажать кнопку *«УСТАНОВИТЬ»*. Если установка пройдет упешно, то серверам сразу будет применена новая ключевая пара. Если администратор системы в дальнейшем загрузит другую ключевую пару, то текущая будет удалена.

При выполнения сброса настроек системы в панели *«Управление системой»* установленная администратором ключевая пара будет удалена. Будут восстановлены ключ и SSL-сертификат разработчика.

Страница «Состояние системы»

На странице приведены графики, отражающие загрузку ресурсов системы.

Страница «Пользователи»

На странице приведена таблица со списком учетных записей всех пользователей системы.

В таблице возможен поиск по основным полям, идентифицирующим владельца учетной записи. Если нажать на кнопку редактирования учетной записи (иконка в виде карандаша), то происходит переход на страницу управления параметрами учетной записи.

Для добавления нового пользователя следует нажать на кнопку «ДОБАВИТЬ ПОЛЬЗОВАТЕЛЯ» в правом нижнем углу страницы.

Страница и пункт меню *«Пользователи»* не будут показаны, если вход произведен под учетной записью с ролью отличной от *«Администратор»*.

Страница управления параметрами учетной записи

Панель «Основная информация»

Панель содержит набор полей, необходимых для идентификации владельца учетной записи. Ссылка *«Сменить логин или пароль»* раскрывает форму задания логина и пароля учетной записи. Поля *«Новый пароль»* и *«Новый пароль повторно»* становятся обязательными только если хотя бы в одно из них внесены изменения.

Панель «Рассылка уведомлений»

Поле *«Уведомлять по Email о событиях»* предназначено для выбора списка событий системы, о которых на электронную почту пользователя будут отсылаться уведомления. Для работы рассылки должен быть указан электронный адрес в поле *«Email»* панели *«Основная информация»*.

Страница «Журнал событий»

Содержит список всех событий, которые записываются в журнал. На данной странице можно видеть как общие события системы, так события изменения параметров каждой политики защиты.

Страница журнала отображает шесть полей для описания каждого события: *«Событие»*, *«Политика защиты»*, *«Контрмера»*, *«Поле»*, *«Пользователь»*, *«Время»*. В столбце *«Поле»* будет указано название параметра контрмеры, который был отредактирован. В зависимости от типа события некоторые поля могут оставаться пустыми.

Для того чтобы применить фильтрацию, нужно ввести искомый текст в поле названия столбца. Регистр не имеет значения, фильтрация может выполняться по нескольким столбцам одновременно.

По умолчанию события отсортированы так, что самые последние события находятся вверху списка. Чтобы отсортировать список в обратном порядке, нужно нажать на стрелку слева от заголовка *«Время»*.

Страница «Помощь»

Содержит описание работы системы.

Используемые термины

Администратор – пользователь системы «MITIGATOR» с ролью *«Администратор системы»*, имеющий доступ ко всем функциям системы через Web-интрефейс.

Глобальные контрмеры – контрмеры, применяемые на весь проходящий через систему трафик до распределения его по политикам защиты.

Контрмера – модуль системы, предназначенный для противодействия определенному типу DDoS-атак.

Панель – под панелью понимается визуально обособленный элемент Web-интерфейса, расположенные на странице интерфейса и имеющий собственный заголовок. В панели может находиться график, элементы управления контрмерой или элементы управления функциями системы.

Политика защиты (политика)– совокупность контрмер, объединенных в отдельную ветвь обработки трафика. Политика защиты имеет название, уникальное в рамках системы. Для распределения трафика на политики защиты используются правила маршрутизации трафика.

Правило маршрутизации трафика (правило) – совокупность из пяти параметров, задающих значения полей заголовка пакета протокола IPv4.

Префикс – собирательное определение, применяющееся тогда, когда в качестве значения допустимо использовать или один IP-адрес в точечно-десятичной нотации (например *198.51.100.1*), или список IP-адресов подсети в нотации CIDR (например *198.51.100.1/32* или *198.51.100.0/24*).

Протокол IPv4 – четвертая версия интернет протокола IP.

Сетевой пакет (пакет) – сетевой пакет протокола IPv4.

Сетевой трафик (трафик) – в общем понимании вся совокупность кадров канального уровня модели OSI, поступающих на сетевые контроллеры устройства системы «MITIGATOR». Или отдельная часть этого трафика, вычлененная из общей совокупности по какому-либо признаку в процессе обработки системой.

Система – система защиты от DDoS атак «MITIGATOR»

CIDR нотация – формат записи для задания логической подсети протокола IPv4 в формате, где адрес сети задается в точечно-десятичной нотации, а число битов маски подсети через символ слеш (например *198.51.100.0/24*). В системе применяется для задания диапазона IP-адресов, входящих в указанную таким образом подсеть.

Web-интерфейс – визуальный интерфейс управления системой «MITIGATOR», реализованный в виде одностраничного Web-приложения.