Positive Technologies Система Определения и Предотвращения Телекоммуникационных Атак

Версия R2.5

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 05.11.2020

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию продукта "Система Определения и Предотвращения Телекоммуникационных Атак" (далее также — СОПТА). Руководство не содержит инструкций по установке СОПТА и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим СОПТА.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **ОК**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о СОПТА

Вы можете найти дополнительную информацию о СОПТА на сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 12).

2. О СОПТА

СОПТА — это решение, предназначенное для отделов информационной безопасности операторов мобильной связи. СОПТА устанавливается на границе операторской сети, собирает копию сигнального трафика, анализирует его и выявляет атаки.

В СОПТА реализованы следующие функции:

- сбор копии трафика сети сотовой связи;
- обнаружение атак в собранном трафике на основе сигнатур;
- присвоение атакам категории на основе классификации GSMA;
- классификация атак по уровню опасности и потенциальным последствиям;
- настройка отображения списка атак;
- создание статистических отчетов;
- выгрузка данных в формате JSON для дальнейшего анализа.

Примечание. Кроме того, может быть предоставлен Firewall, который позволяет СОПТА блокировать входящие запросы до того, как они достигнут сети оператора. Используя язык правил гибкого Firewall (см. раздел 8.4), можно указать параметры сообщений, которые будут заблокированы.

3. Логические компоненты СОПТА

СОПТА имеет модульную архитектуру, что позволяет устанавливать продукт на один или несколько серверов в зависимости от объема сетевого трафика, который надо обрабатывать, и необходимости распределять нагрузку между серверами.

СОПТА включает в себя следующие модули:

— Attack Discovery Engine. Модуль включает в себя два компонента:

  • Correlator проверяет сообщения, полученные от Sensor, на соответствие сигнатурам атак. Если сообщение или последовательность из сообщений соответствует сигнатуре, регистрируется атака. Обнаруженные атаки сохраняются в модуле Database.

— Firewall. На основе правил Firewall модуль фильтрует входящие запросы, прежде чем они попадут в сеть оператора. Правила Firewall настраиваются администратором СОПТА. Если сообщение не подходит под правило, оно разрешается (правило по умолчанию).

— Database. Модуль является централизованной системой хранения в СОПТА, основанной на транзакционной системе управления базами данных (PostgreSQL). В модуле Database хранится следующая информация.

  • Конфигурационные параметры Correlator.

  • Префиксы стран и операторов.

  • Пользовательские настройки: группы адресов, фильтры, настройки отображения атак.

— Backend. Модуль обрабатывает данные из модуля Database для предоставления модулю UI информации о зарегистрированных атаках. Модуль выполняет следующие функции.

  • Аутентификация и авторизация пользователей.

  • Обработка пользовательских настроек (групп адресов, фильтров, настроек отображения атак) и сохранение их в модуле Database.

  • Поиск, агрегация и фильтрация данных на основе пользовательских настроек.

  • Экспорт подробной информации об атаках в виде JSON-файлов, доступных для скачивания из интерфейса.

  • Создание статистических отчетов в формате ODS, доступных для скачивания из интерфейса.

— UI. Модуль представляет собой веб-сервер (nginx), обеспечивающий возможность работы в веб-интерфейсе.

4. Развертывание СОПТА

Трафик может обрабатываться двумя компонентами СОПТА:

— Модуль Attack Discovery Engine анализирует копию трафика и регистрирует атаки.

Если используются оба компонента, вы можете развернуть СОПТА по одной из двух схем в зависимости от того, какой из компонентов первым обрабатывает трафик.

В этом разделе

4.1. Схемы развертывания СОПТА

СОПТА может быть развернут по одной из двух схем:

— Модуль Attack Discovery Engine обеспечивает анализ трафика до его проверки в модуле Firewall в соответствии с правилами Firewall. В этой схеме атаки, обнаруженные модулем обнаружения атак, могут впоследствии блокироваться Firewall.

— Модуль Attack Discovery Engine может анализировать трафик после его проверки по Firewall в соответствии с правилами Firewall. В этой схеме только трафик, который не был заблокирован Firewall, проверяется по сигнатурам СОПТА.

В этом разделе описаны этапы проверки трафика в обеих схемах развертывания.

Модуль Attack Discovery Engine перед модулем Firewall

Обработка трафика включает в себя следующие этапы:

1. Модуль Attack Discovery Engine анализирует копию трафика, прежде чем он достигнет пограничного STP-узла.
2. Модуль Firewall проверяет трафик, полученный от пограничного STP-узла, по правилам Firewall и отправляет обратно разрешенные сообщения.
3. Только разрешенные сообщения достигают сети оператора.

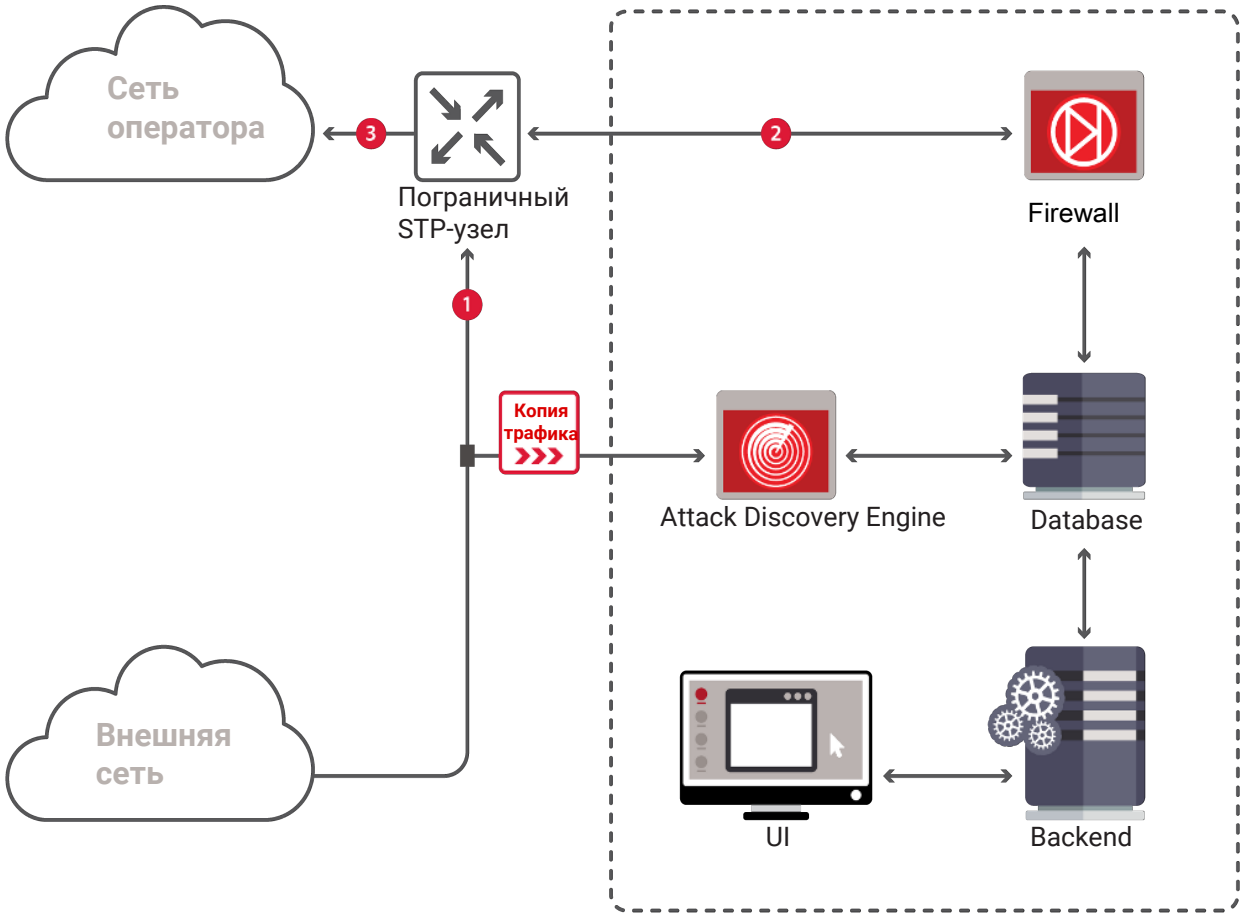


Рисунок 1. Схема развертывания СОПТА: Модуль Attack Discovery Engine перед модулем Firewall

В этой схеме модуль Attack Discovery Engine анализирует весь трафик, поступающий в сеть оператора, включая сообщения, которые могут быть заблокированы Firewall. Таким образом, СОПТА может обнаруживать атаки, которые не были бы обнаружены при блокировке соответствующих сообщений. Пользователи СОПТА могут проверять, какие из атак были заблокированы по правилам Firewall.

Модуль Attack Discovery Engine после Firewall

Обработка трафика включает в себя следующие этапы:

1. Трафик поступает на пограничный STP-узел.
2. Модуль Firewall проверяет трафик, полученный от пограничного STP-узла, по правилам Firewall и отправляет обратно разрешенные сообщения.
3. Только разрешенные сообщения достигают сети оператора. Модуль Attack Discovery Engine анализирует копию трафика, которая не содержит сообщения, заблокированные модулем Firewall.

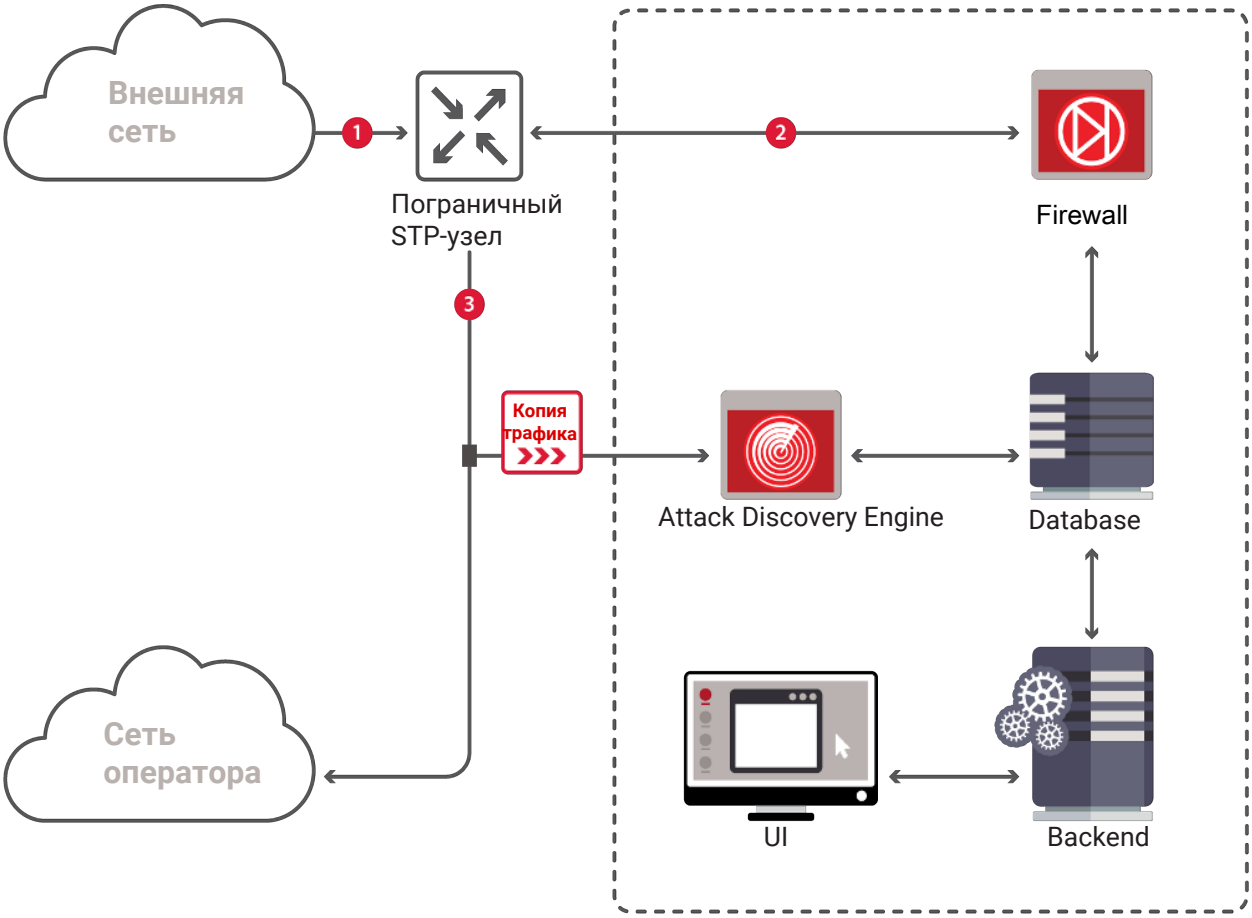


Рисунок 2. Схема развертывания СОПТА: Модуль Attack Discovery Engine после Firewall

В этой схеме модуль Attack Discovery Engine анализирует только те сообщения, которые не были заблокированы модулем Firewall. Таким образом можно проверять эффективность модуля СОПТА Firewall (или используемого решения стороннего производителя): обнаружение «заблокированной» атаки означает, что механизм блокировки не сработал.

4.2. Схемы развертывания SS7 Firewall

Этот раздел содержит описание схем развертывания модуля Firewall и конфигурации маршрутизации пограничного STP-узла, необходимой для отказоустойчивой передачи трафика.

Развертывание без избыточности

Модуль Firewall может быть использован как единственный M3UA-сервер приложений с собственным кодом сигнальной точки (PC 4 на рисунке ниже). В этой схеме пограничный STP-узел (PC 2) при получении внешнего сетевого трафика (1) перенаправляет его в модуль Firewall (2). Модуль Firewall отправляет сообщения (3), которые не были заблокированы, обратно на STP-узел. STP-узел передает такие сообщения во внутреннюю сеть (4).

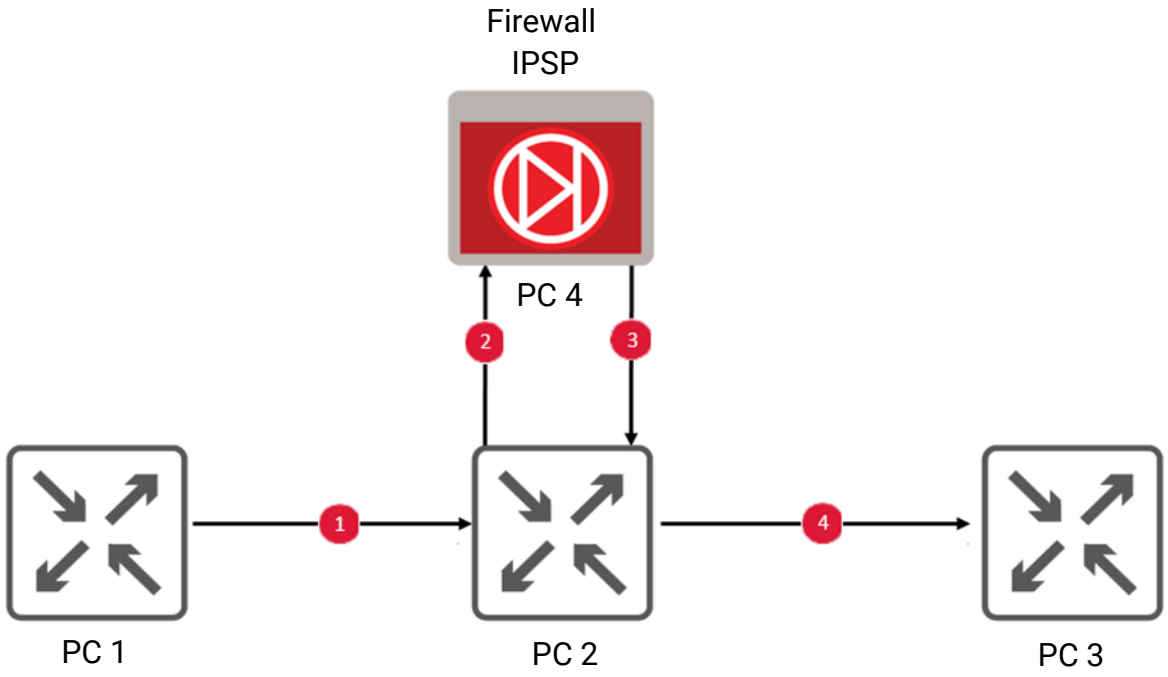


Рисунок 3. Развертывание без избыточности

Поскольку в этой схеме отсутствует избыточность, в случае недоступности модуля Firewall настройки STP-узла должны обеспечивать передачу трафика напрямую во внутреннюю сеть.

Отдельные серверы приложений

Экземпляры модуля Firewall могут использоваться как независимые M3UA-серверы приложений с собственным кодом сигнальной точки для каждого из них (PC 4 и PC 5 на рисунке ниже). В этой схеме пограничный STP (PC 2) должен быть настроен для маршрутизации трафика из одного из экземпляров Firewall (PC 4 или PC 5) во внутреннюю сеть.

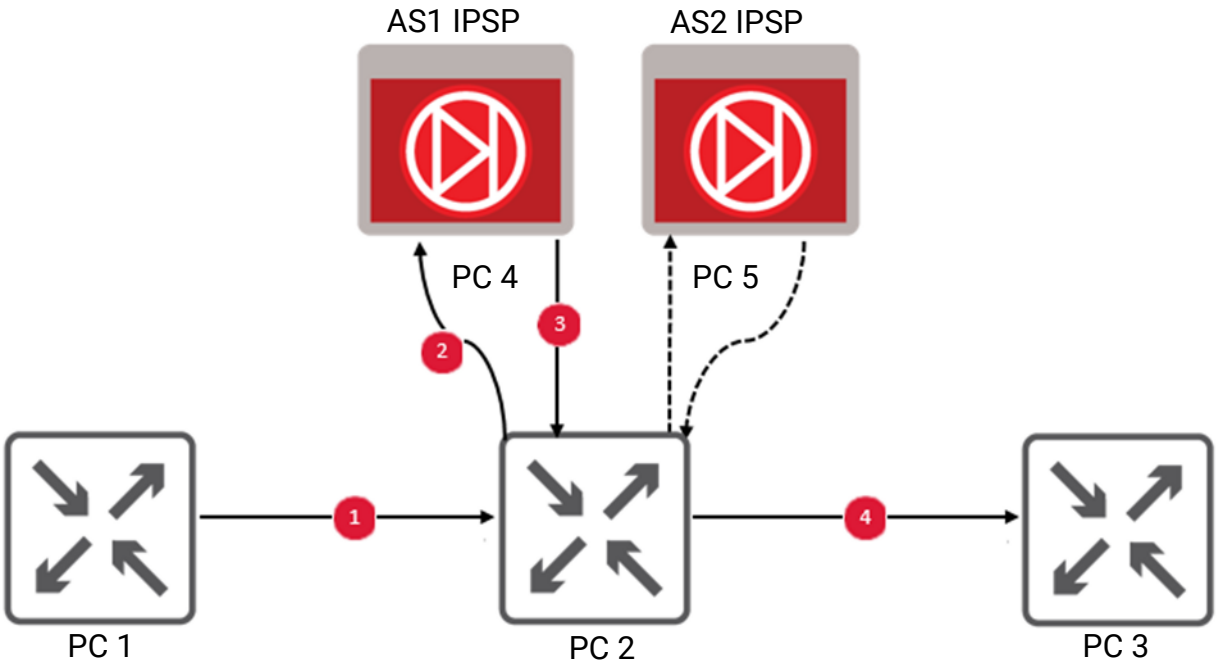


Рисунок 4. Отдельные серверы приложений

Если первый экземпляр модуля Firewall (PC 4) недоступен, трафик должен передаваться на второй экземпляр (PC 5) и с него. Возможность передавать трафик во внутреннюю сеть в случае недоступности обоих серверов приложений зависит от используемого оборудования.

Двойной модуль Firewall в рамках одного сервера приложений

Экземпляры модуля Firewall могут использоваться как отдельные процессы M3UA-серверов приложений в рамках одного сервера приложений с единым кодом сигнальной точки (PC 4 на рисунке ниже). Для корректной работы модуля Firewall рекомендуется использовать режим Loadshare для процессов серверов приложений.

Настройки пограничного STP-узла (PC 2) должны обеспечивать передачу трафика с этого кода сигнальной точки во внутреннюю сеть. Маршрутизация между двумя экземплярами модуля Firewall в рамках одного сервера приложений осуществляется на уровне протокола M3UA.

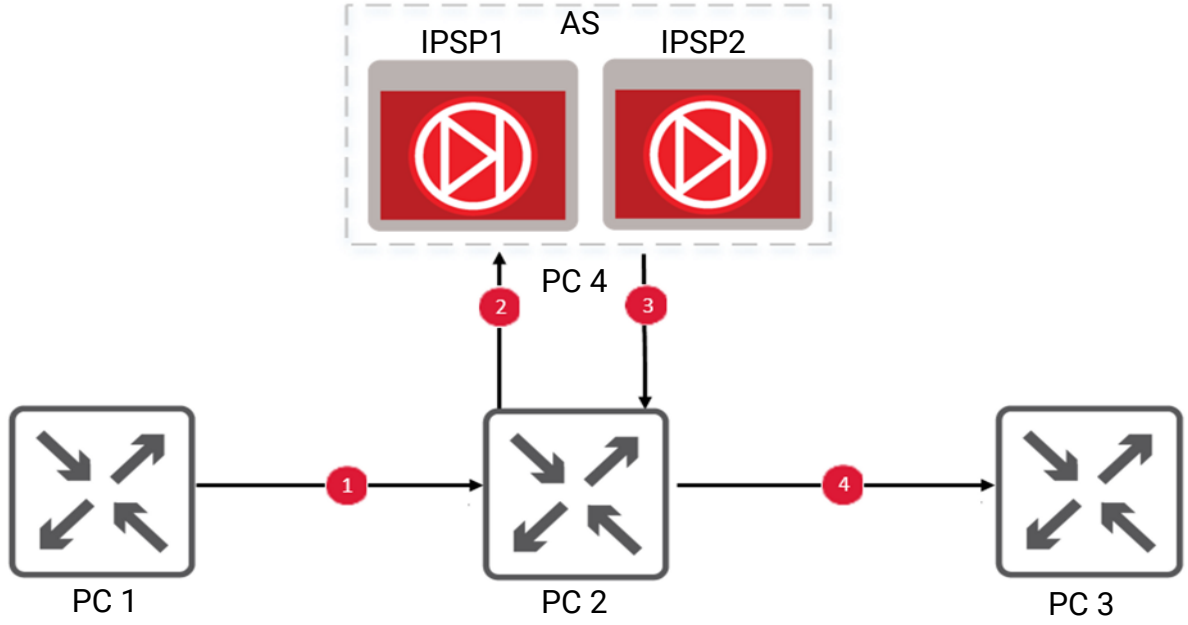


Рисунок 5. Избыточность в рамках одного сервера приложений

Если первый экземпляр модуля Firewall (IPSP1) недоступен, трафик должен передаваться на второй экземпляр (IPSP2) и с него. Если второй экземпляр также недоступен, трафик должен передаваться напрямую во внутреннюю сеть. В этой схеме обеспечивается наиболее высокая отказоустойчивость, так как трафик достигает внутренней сети, даже если оба процесса серверов приложений недоступны. Эта схема также обеспечивает наибольшую простоту настройки, так как оба процесса серверов приложений имеют единый код сигнальной точки.

4.3. Режимы сбора трафика в СОПТА

Модуль Attack Discovery Engine собирает мобильный сетевой трафик протоколов SCTP, M3UA, M2PA, MTP3, SCCP, TCAP, MAP, CAP, Diameter и GTP-C. В зависимости от потребностей заказчика модуль Attack Discovery Engine может получать трафик в следующих режимах:

— От пограничного элемента сети, который может быть STP-узлом (в сетях SS7), DEA-узлом (в протоколе Diameter) или IP-шлюзом (в протоколе GTP). Модуль Attack Discovery Engine получает копию трафика с внешнего интерфейса для обнаружения атак на сеть оператора.

Рисунок 6. Получение трафика от пограничного STP/DEA-узла

— От узла агрегации. Модуль Attack Discovery Engine получает копию трафика от узла, который агрегирует данные от элементов внутренней сети.

Рисунок 7. Получение трафика от узла агрегации

— Непосредственно перед элементами сети. Модуль Attack Discovery Engine получает копию трафика до его получения ключевыми элементами сети, такими как HLR или VLR.

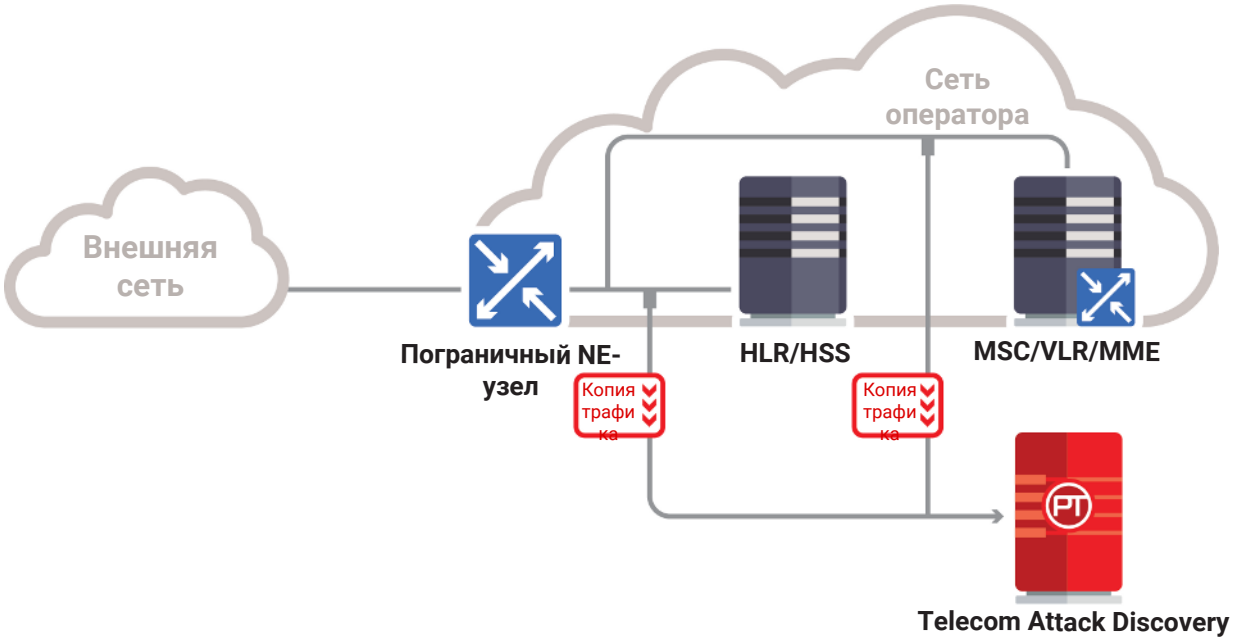


Рисунок 8. Получение трафика перед элементами сети

— Из PCAP-файлов. Модуль Attack Discovery Engine получает копию трафика из PCAP-файлов, предоставленных внешними системами мониторинга через FTP- или NFS-сервер или сетевую папку с настроенным общим доступом.

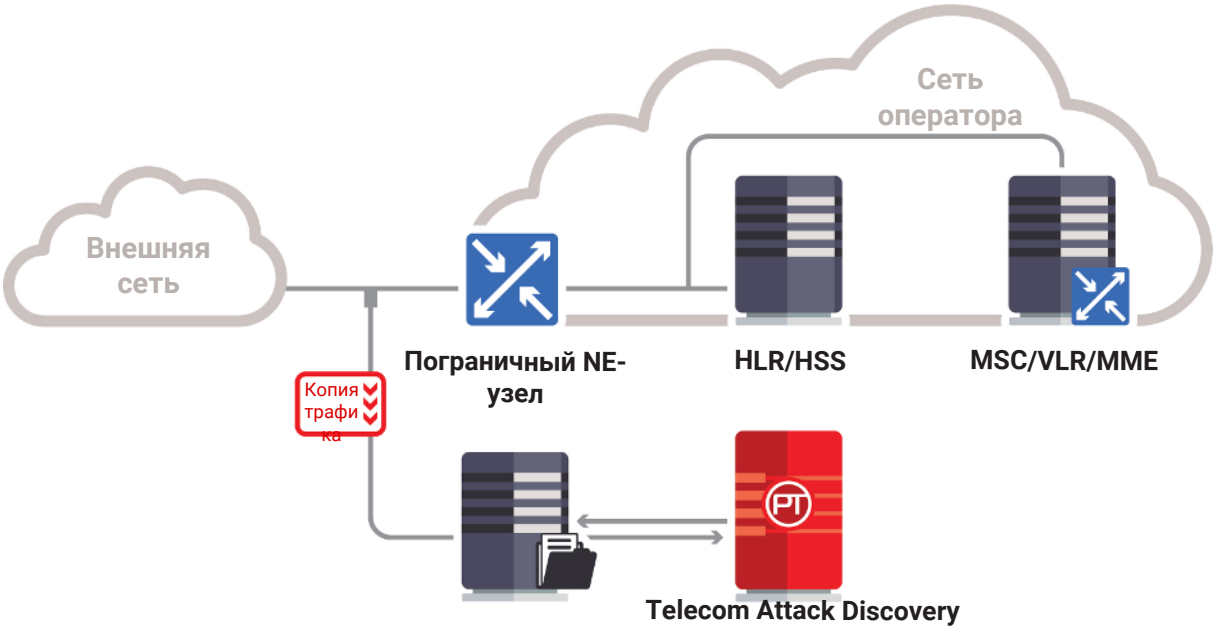


Рисунок 9. Получение трафика из PCAP-файлов

5. О правах доступа

Доступ к ресурсам СОПТА основан на ролях. Роль представляет из себя атрибут учетной записи пользователя, который определяет права доступа к страницам и функциям СОПТА. Пользователь может иметь роль администратора (Administrator) или оператора безопасности (Security officer). Назначать и менять роли других пользователей могут только пользователи с ролью администратора.

Если сотрудники службы безопасности связаны с оператором-партнером, они могут просматривать только атаки и данные на информационных панелях, связанных с этим оператором. Если такой оператор также является владельцем системы (System owner), его пользователи могут также просматривать настройки SMS Home Routing этого оператора.

6. Первоначальная настройка

Для корректной работы СОПТА вы должны выбрать владельца системы и настроить SMS Home Routing.

В этом разделе

6.1. Выбор владельца системы

Владелец системы — это оператор, диапазоны номеров которого считаются СОПТА номерами домашней сети заказчика.

Выбор владельца системы позволяет СОПТА идентифицировать направление сообщений (входящих или исходящих) и определить, принадлежит ли абонент абонентской сети или сети другого оператора. Выбор владельца системы необходим для правильного обнаружения атак GT Spoofing, Spoofing on Home Network, MAP 3.1, Diameter Category 3 и большинства атак MAP 3.2 и MAP 3.3. Если сигнатура зависит от владельца системы, соответствующее предупреждение отображается на странице **Attack types settings**.

Если такие атаки должны обнаруживаться для нескольких операторов, необходимо назначить каждого из них владельцем системы.

Внимание! Для корректного обнаружения атак рекомендуется выключить эти типы атак и их сигнатуры (см. раздел 7.3), если владелец системы не выбран.

Примечание. Префиксы владельца системы не должны совпадать с адресами Global Title из белого списка. Если вы выберете владельца системы, префиксы Global Title которого совпадают с адресами Global Title из белого списка, такие адреса Global Title автоматически удаляются из белого списка.

Примечание. Если вы хотите использовать функцию Firewall, только один оператор может быть выбран в качестве владельца системы.

► Чтобы выбрать владельца системы:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Operators**.
3. Справа от оператора наведите курсор мыши на и нажмите .

   Откроется страница **<Название оператора>**.
4. В левой части страницы нажмите и подтвердите действие.

Оператор выбран в качестве владельца системы и обозначается значком на странице **Operators**.

Вы можете удалить статус владельца системы, щелкнув на странице **Operators** → **<Operator name>**. Это можно использовать, например, для отключения обнаружения атак MAP 3.3. Удаление статуса владельца системы сбрасывает все настройки SMS Home Routing (см. раздел 6.2) оператора.

6.2. Настройка SMS Home Routing

SMS Home Router представляет собой основанное на стандартах (3GPP TR 23.840) решение, обеспечивающее централизацию всего SMS-трафика в общей точке маршрутизации в домашней сети. SMS Home Router вносит следующие изменения в ответы SendRoutingInfoForSM, отправляемые SMS-центру, от которого получены сообщения:

- Заменяет реальный IMSI получателя на Correlation ID. В СОПТА вы можете указать список Correlation ID для проверки их использования вместо реальных IMSI.
- Заменяет реальное местоположение абонента (адрес Global Title обслуживающего MSC) на адрес Global Title SMS Home Router. В СОПТА вы можете указать список адресов Global Title SMS Home Router для проверки их использования вместо реального местоположения абонентов.

Если ответ SendRoutingInfoForSM содержит реальный IMSI абонента (т. е. число, отличное от указанного в списке идентификаторов корреляции) или GT MSC, обслуживающего абонента (т. е. число, отличное от указанного в списке адресов SMS Home Router GT), СОПТА обнаруживает атаку типа SMSHomeRouting Failure.

Если запрос MT-Forward-SM отправляется на адрес Global Title MSC, обслуживающего абонента (т. е. на номер, отличающийся от указанного в списке адресов Global Title SMS Home Router), СОПТА регистрирует атаку типа ForwardSM (обходя SMSHR) Request, Aborted или Completed.

SMS Home Routing можно настроить только для операторов со статусом владельца системы (см. раздел 6.1).

► Чтобы настроить SMS Home Routing, выполните следующие действия:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Operators**.
3. Наведите курсор мыши на (справа от оператора со статусом владельца системы, обозначенного значком) и нажмите .

   Откроется страница **<Название оператора>**.
4. Выберите вкладку **SMS Home Routing**.
5. В таблице **Correlation IDs** введите Correlation ID и нажмите . Ваш Correlation ID должен начинаться с тех же цифр, что и префиксы страны и оператора, префиксы опреатора в диапазоне номеров E.212.

SMS Home Routing настроен.

Корректное обнаружение атак, относящихся к SMS Home Routing, может быть обеспечено, только если указаны все Correlation ID и адреса Global Title SMS Home Router оператора, для которого такие атаки необходимо обнаруживать, и если их список обновляется при появлении новых Correlation ID или адресов Global Title SMS Home Router.

Внимание! Если указаны не все Correlation ID и адреса Global Title SMS Home Router, СОПТА может классифицировать потенциально безопасные сообщения как атаки. Чтобы избежать ложных срабатываний, выключите соответствующие типы атак (см. раздел 7.3) до полного заполнения таблиц СОПТА SMS Home Routing.

7. Управление обнаружением атак

Вы можете гибко управлять алгоритмами обнаружения атак, выполняя следующие действия:

- Исключите узлы SS7 или Diameter из процесса обнаружения атак с использованием белых списков, если вы считаете, что такие узлы являются доверенными, и вам не нужно проверять сообщения, поступающие от них или к ним.
- Выключите типы атак или составляющие их сигнатуры, если вы не хотите регистрировать такие атаки или если отсутствуют соответствующие настройки (см. раздел 6).
- Измените уровень опасности типов атак.
- Настройте конечные точки Diameter и соединения для обнаружения определенных атак Diameter.

В этом разделе

7.1. Настройка белого списка Diameter

Если узел Diameter является доверенным и вы не хотите проверять его входящие или исходящие сообщения, используя сигнатуры, вы можете добавить имя хоста этого узла в белый список Diameter.

Перед проверкой сообщения с использованием сигнатур модуль СОПТА проверяет, совпадает ли AVP Origin-Host или Destination-Host в сообщении с хостом из белого списка. Если это так, модуль СОПТА прекращает обработку сообщения, а если сообщение представляет атаку, атака игнорируется. Если сообщение не соответствует ни одному из хостов, занесенных в белый список, модуль СОПТА проверяет это сообщение, используя сигнатуры.

► Чтобы настроить белый список узла Diameter, выполните следующие действия:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите **Diameter White list**.
3. Чтобы включить список, наведите курсор мыши на ✕ в левой части страницы и нажмите ✔.
4. В столбце **Hosts** введите имя хоста и нажмите клавишу ENTER.

Примечание. Если вы хотите внести в белый список одновременно несколько имен хостов, вы можете использовать звездочку в качестве символа подстановки в начале и (или) конце шаблона.

Белый список узла Diameter настроен.

Рисунок 10. Настройка белого списка Diameter

Если у вас уже наблюдались атаки, вы можете использовать их для быстрого добавления исходных или целевых хостов в белый список узла Diameter.

- Чтобы добавить существующий хост в белый список узла Diameter:

  1. Выберите хост одним из следующих способов.
     - На странице **Dashboards** щелкните значение хоста на графике, связанном с адресами источника или назначения.
     - На странице **Attacks** в списке атак или на карточке атаки щелкните значение исходного или целевого хоста.
  2. В открывшемся контекстном меню выберите **Add to Diameter White list**.
  3. Нажмите **Add**.

7.2. Настройка белого списка SS7

Если сетевой узел является доверенным и вы не хотите проверять его входящие и исходящие сообщения MAP и CAP, используя сигнатуры, вы можете добавить GT этого узла в белый список.

Перед проверкой сообщения с использованием сигнатур СОПТА проверяет, соответствует ли номер источника или места назначения в сообщении GT в белом списке. Если это так, модуль СОПТАпрекращает обработку сообщения, а если сообщение представляет атаку, атака игнорируется. Если сообщение не соответствует ни одному из внесенных в белый список GT, СОПТА проверяет это сообщение, используя сигнатуры.

► Чтобы настроить белый список SS7, выполните следующие действия:

1. На панели инструментов нажмите ⚙.
2. Чтобы включить список, наведите курсор мыши на ✕ в левой части страницы и нажмите ✔.

   Примечание. Вы можете использовать звездочку (*) для добавления префикса адреса Global Title (например, 123*).

Белый список настроен.

Рисунок 11. Настройка белого списка SS7

7.3. Включение и выключение сигнатур

Если вы не хотите регистрировать некоторые атаки (например, если вы считаете их ложными срабатываниями), вы можете выключить соответствующие сигнатуры и типы атак.

Типы атак могут включать в себя одну или несколько сигнатур. Если тип атаки включает в себя одну сигнатуру, атаки этого типа обнаруживаются с помощью этой сигнатуры. Если тип атаки включает в себя несколько сигнатур, атаки этого типа могут быть обнаружены с помощью любой из этих сигнатур.

В зависимости от статуса сигнатур тип атаки может иметь один из следующих статусов:

✔ — включен: все сигнатуры этого типа атаки включены.

✕ — выключен: все сигнатуры этого типа атак выключены.

⁘ — частично включен: тип атак включает в себя более одной сигнатуры, некоторые из них выключены.

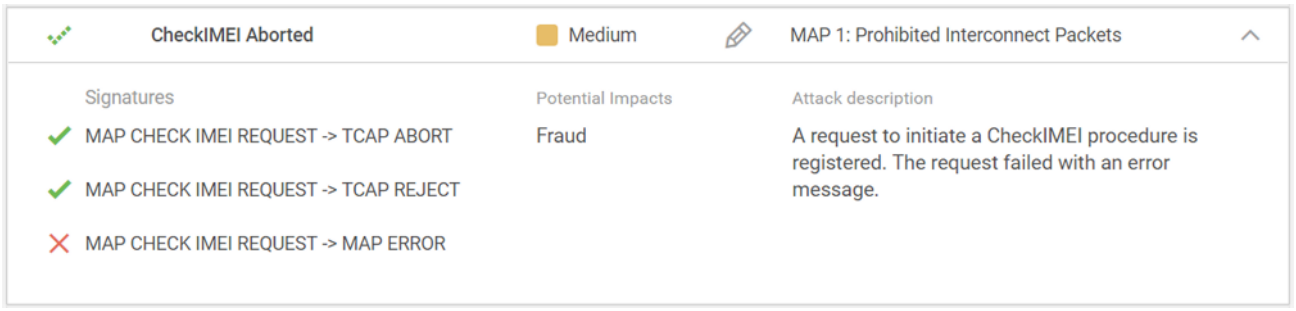


Рисунок 12. Настройки типов атак

Примечание. Все сигнатуры, относящиеся к протоколу GTP, выключены по умолчанию. Прежде чем включать их, убедитесь, что в СОПТА Sensor включен разбор протокола GTP.

► Чтобы включить или выключить сигнатуру, выполните следующие действия:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Attack types settings**.
3. Справа от типа атаки нажмите , чтобы просмотреть все сигнатуры, составляющие этот тип атаки.
4. Выполните одно из следующих действий.

   - Чтобы выключить сигнатуру, наведите курсор мыши на слева от сигнатуры и нажмите .

     Примечание. Если тип атак включает в себя несколько сигнатур, вы можете выключить их все, наведя курсор мыши на слева от типа атак и нажав . Выключение всех сигнатур, составляющих тип атак, выключает весь тип атак.

   - Чтобы включить сигнатуру, наведите курсор мыши на слева от выключенной сигнатуры и нажмите .

     Примечание. Если тип атак включает в себя несколько сигнатур, вы можете включить их все, наведя курсор мыши на (или , если некоторые из них включены) слева от типа атак и нажав .

СОПТА будет использовать все включенные сигнатуры для обнаружения атак и не будет использовать выключенные сигнатуры.

Примечание. Кроме включения, для работы некоторых сигнатур необходимо выбрать владельца системы (см. раздел 6.1) и настроить SMS Home Routing (см. раздел 6.2). Если владелец системы не выбран или не настроен SMS Home Routing, СОПТА не будет использовать или будет некорректно использовать сигнатуры, которые зависят от этих настроек.

7.4. Изменение уровня опасности типов атак

Уровень опасности — это атрибут атаки, который указывает на степень угрозы, основываясь на последствиях и успешности атаки. Уровень опасности зависит от типа атаки: каждая атака имеет заранее установленный уровень опасности (высокий, средний или низкий) в СОПТА .

Если вы считаете, что некоторые типы атак имеют более низкий или более высокий уровень опасности по сравнению с заранее установленными значениями, вы можете изменить их уровень опасности.

Значения уровней опасности, измененные пользователями, обозначаются звездочкой (*). Заранее установленные значения уровней опасности обозначаются как **Recommended**.

► Чтобы изменить уровень опасности типа атак:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Attack types settings**.
3. Наведите курсор мыши на значение уровня опасности типа атак и нажмите .
4. В раскрывающемся списке выберите уровень опасности, который вы хотите присвоить этому типу атак.

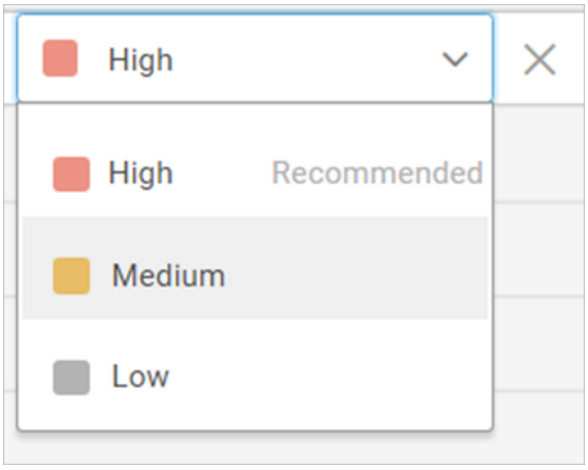


Рисунок 13. Изменение уровня опасности типа атак

Уровень опасности типа атак изменен. Все атаки, обнаруженные СОПТА до и после этого изменения, будут иметь новый уровень опасности.

7.5. Настройка соединений узла Diameter

Для обнаружения атак, связанных с узлом Unsupported Application-Id or Command Code, IP address is not allowed, Spoofing on POI, необходимо настроить следующее:

- Создайте список приложений и их идентификаторы, которые должны поддерживаться в анализируемом трафике.
- Создайте наборы правил, в которых указаны коды команд (Command Code), которые должны быть разрешены для выбранных приложений.
- Создайте конечные точки, которые соответствуют узлам трафика, между которыми вы хотите выполнить анализ, укажите их IP-адреса и назначьте их операторам.
- Создайте соединения между конечными точками и назначьте им созданные наборы правил. Кроме того, для прямых подключений необходимо настроить разрешенные хосты и области.

В этом разделе

Настройка приложений (см. раздел 7.5.1)

Создание наборов правил (см. раздел 7.5.2)

Создание конечных точек (см. раздел 7.5.3)

Создание соединений (см. раздел 7.5.4)

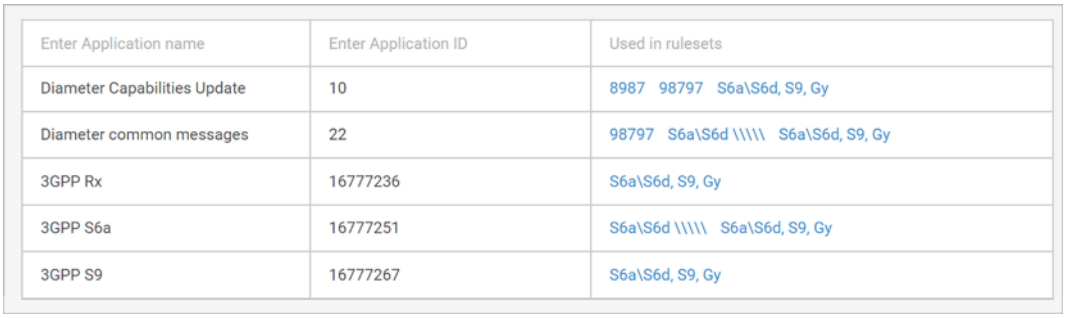
7.5.1. Настройка приложений

Модуль СОПТА позволяет обнаружить неправильное использование интерфейса Diameter путем проверки соответствия между идентификатором приложения (Application ID) и кодом команды (Command Code). Первым шагом является настройка приложений, которые вы ожидаете встретить в анализируемом трафике. По умолчанию список приложений в СОПТА включает общие сообщения (Common Messages) узла Diameter, приложение Diameter Credit Control, обновление Diameter Capabilities Update, 3GPP Rx, 3GPP S6a, 3GPP S13\S13', 3GPP S9, 3GPP S6c, 3GPP SGd.

► Чтобы настроить приложения, выполните следующие действия:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите **Diameter configuration**.
3. Перейдите на вкладку **Applications**.
4. Для каждого приложения введите его имя и идентификатор и нажмите клавишу ENTER.

Приложения настроены.



Enter Application name	Enter Application ID	Used in rulesets
Diameter Capabilities Update	10	8987 98797 S6a\S6d, S9, Gy
Diameter common messages	22	98797 S6a\S6d \\\\\ S6a\S6d, S9, Gy
3GPP Rx	16777236	S6a\S6d, S9, Gy
3GPP S6a	16777251	S6a\S6d \\\\\ S6a\S6d, S9, Gy
3GPP S9	16777267	S6a\S6d, S9, Gy

Рисунок 14. Настройка приложений

Теперь можно создать набор правил (см. раздел 7.5.2), чтобы определить коды команд, которые будут разрешены для каждого приложения.

Если приложение используется в наборах правил, имена таких наборов правил отображаются в столбце **Used in rulesets**.

7.5.2. Создание наборов правил

Набор правил — это набор кодов команд, которые можно использовать с конкретными приложениями (см. раздел 7.5.1). По умолчанию список наборов правил в СОПТА включает наборы правил S6a\S6d и S6a\S6d, S9, Gy.

► Чтобы создать набор правил, выполните следующие действия:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите **Diameter configuration**.
3. Перейдите на вкладку **Rulesets**.
4. Нажмите +.

   Откроется форма создания набора правил.
5. В поле **Name** введите имя для набора правил.
6. В раскрывающемся списке **Application** выберите приложение.
7. В поле **Command Codes** введите коды команд, которые должны быть разрешены для выбранного приложения.
8. Нажмите ⊕.
9. Нажмите кнопку **Save**.

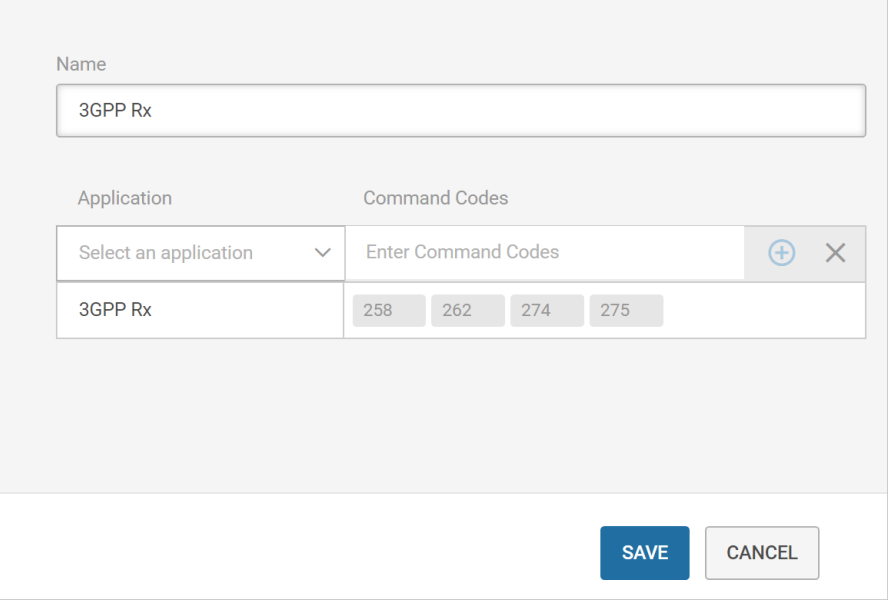


Рисунок 15. Создание набора правил

Теперь набор правил создан.

После этого можно назначить набор правил для соединений (см. раздел 7.5.4).

7.5.3. Создание конечных точек

Конечные точки соответствуют узлам Diameter, трафик между которыми вы хотите проанализировать. Одна конечная точка может иметь один или несколько IP-адресов в зависимости от того, хотите ли вы применить набор правил к трафику между двумя конкретными IP-адресами или между наборами IP-адресов.

Вы должны создать как минимум две конечные точки и связать их (см. раздел 7.5.4) друг с другом.

Если вы хотите проверить трафик между операторами для хостов и областей, разрешенных в их точках межсоединений (Point of Interconnect), вы можете создать конечные точки этих операторов и настроить прямое соединение между ними. Если вы не хотите проверять трафик на наличие разрешенных хостов и областей, вы можете выбрать поставщика IPX и создать косвенное соединение для такой конечной точки.

► Чтобы создать конечную точку, сделайте следующее:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите **Diameter configuration**.
3. Перейдите на вкладку **Endpoints**.
4. Нажмите +.

   Откроется форма создания конечной точки.

5. В раскрывающемся списке **Operator** выберите оператора конечной точки.

   Примечание. После создания конечной точки вы не можете изменить ее оператора.

6. В поле **Endpoint name** введите имя конечной точки.
7. В поле **IP addresses** введите IP-адрес конечной точки и нажмите клавишу ENTER.

   Примечание. Вы также можете добавить несколько IP-адресов к конечной точке.

8. Нажмите кнопку **Save**.

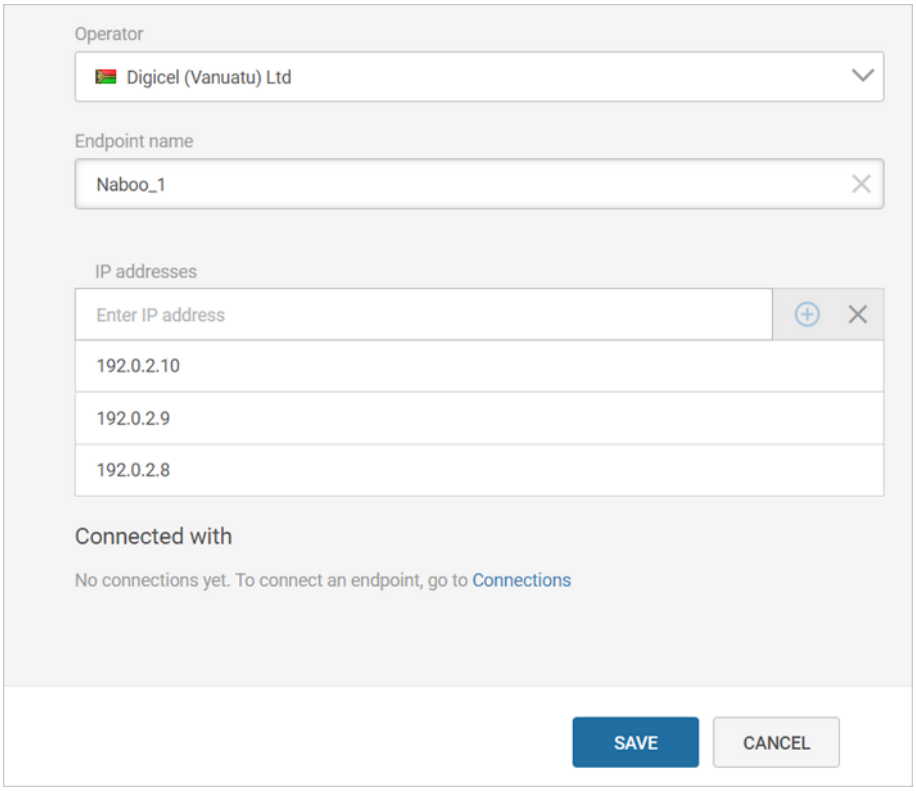


Рисунок 16. Создание конечной точки

Теперь конечная точка создана.

Все созданные конечные точки доступны для каждого оператора на странице **Operators** → **<Operator name>**. Если конечная точка связана с другой конечной точкой, информация о таком соединении отображается в столбце **Connected with**.

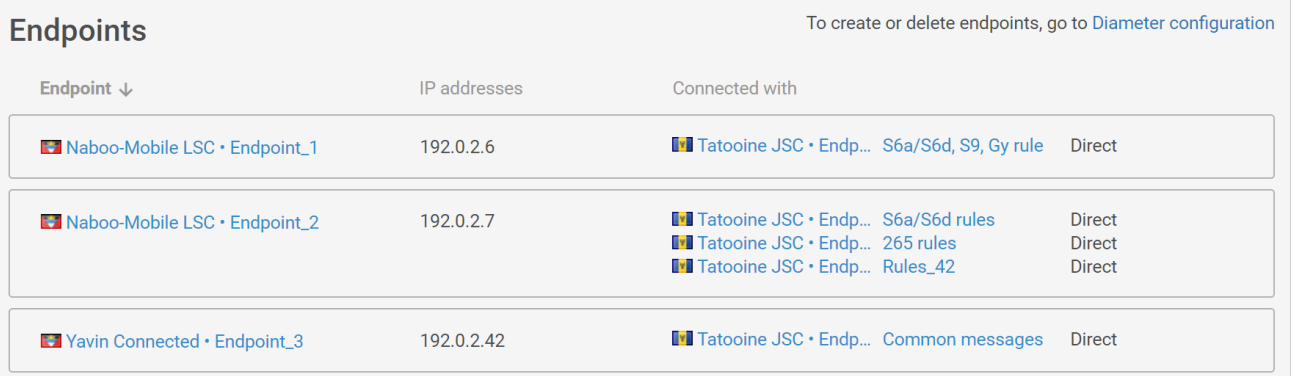


Рисунок 17. Конечные точки оператора

7.5.4. Создание соединений

Необходимо соединить каждую созданную конечную точку хотя бы еще с одной конечной точкой.

Соединения не соответствуют существующим соединениям или ассоциациям, но используются для применения (см. раздел 7.5.2) наборов правил к сообщениям узла Diameter между указанными IP-адресами.

► Чтобы создать соединение, сделайте следующее:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите **Diameter configuration**.
3. Перейдите на вкладку **Connections**.
4. Нажмите +.

   Откроется форма создания соединения.
5. Выберите тип соединения.
   - **Direct** — если вы хотите проверить трафик между конечными точками для разрешенных областей и хостов (обычно используется для соединений между конечными точками разных операторов).
   - **Indirect** — если вы не хотите проверять трафик между конечными точками на предмет разрешенных областей и хостов (обычно используется для соединений с конечными точками поставщика IPX).
6. В раскрывающемся списке **Ruleset** выберите набор правил для применения к соединению.
7. В раскрывающихся списках **Endpoint A** и **Endpoint B** выберите конечные точки, которые вы хотите подключить.

Примечание. При обнаружении атак между конечными точками направление не учитывается: конечные точки A и B могут быть узлами источника или назначения. Вы не можете создать более одного соединения между одинаковыми конечными точками или между конечными точками с одинаковыми IP-адресами.

8. Нажмите кнопку **Save**.

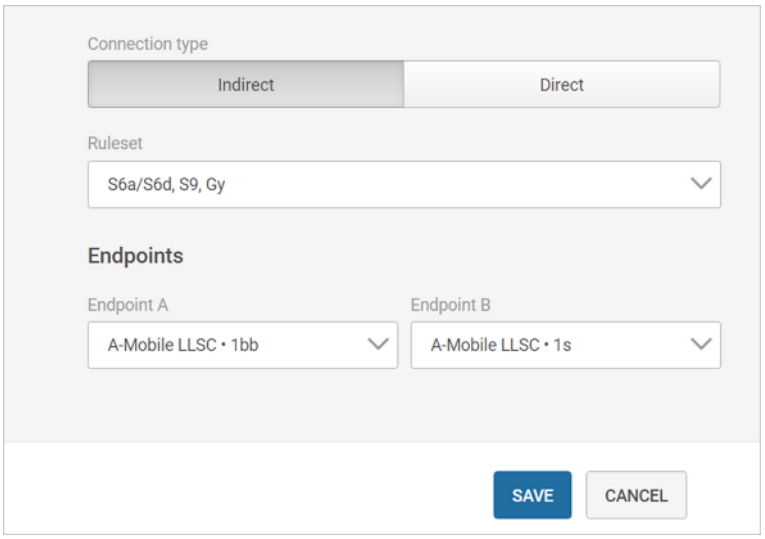


Рисунок 18. Создание соединения

Теперь соединение создано.

Если приложение или код команды в сообщении между подключенными конечными точками не соответствуют приложениям и кодам команд, указанным в наборе правил, назначенном для соединения, обнаруживается атака Unsupported Application-Id or Command Code.

Если IP-адрес источника или назначения не совпадает ни с одним из IP-адресов, указанных в подключенных конечных точках, обнаруживается атака IP address is not allowed.

Если значения Origin-Host, Origin-Realm, Destination-Host или Destination-Realm не соответствуют ни одной из областей и хостов, указанных для прямого соединения, обнаруживается атака Spoofing on POI.

8. Работа с правилами Firewall

СОПТА позволяет блокировать или явно разрешать входящие запросы на основе критериев, указанных в правилах Firewall. СОПТА может содержать два узла Firewall, которые работают отдельно: SS7 Firewall позволяет настраивать правила для блокировки или разрешения запросов MAP и CAP, Diameter Firewall позволяет настраивать правила для блокировки или разрешения запросов Diameter. Создание и редактирование правил доступно только пользователям с ролью Administrator.

> **Примечание.** Для включения функции Firewall и доступа к страницам **Firewall rules** и **Firewall events** необходимо активировать соответствующую лицензию.

Если входящий запрос соответствует всем критериям правила Firewall, к нему применяется действие (блокировать или разрешить). Для каждого срабатывания правила также может быть зарегистрировано событие Firewall. Если сообщение не подходит под правило Firewall, оно разрешается (правило по умолчанию).

В этом разделе

8.1. О модулях Firewall

Правила управления узлом Firewall для SS7 Firewall и Diameter Firewall отличаются. Различия представлены в следующей таблице.

Таблица 2. Правила SS7 и Diameter Firewall

Функция	SS7	Diameter
Применение изменений (создание, удаление и редактирование правила, в том числе его включение/отключение и изменение его приоритета)	Изменения применяются после их сохранения.	Изменения сохраняются, но не применяются. Кнопка **Apply** используется для применения всех изменений к набору правил.
Ссылки на правила Firewall из событий Firewall	Нет в наличии.	Доступно.
История версий правил Firewall	Отображается только последняя версия.	Доступно по ссылке на правила Firewall из событий Firewall. Ссылка отображает набор правил, какими они были при записи события.

Функция	SS7	Diameter
Применимость правил	Все правила применяются ко всем экземплярам Firewall.	Вы можете создать несколько наборов правил. Каждый набор привязан к экземпляру Firewall или группе экземпляров Firewall (см. раздел 8.3).
Включение и выключение Firewall	Используя переключатель в пользовательском интерфейсе, вы можете отключить службу Firewall. Это действие закрывает ассоциации SCTP, поэтому Firewall не будет получать запросы на обработку.	Используя переключатель в пользовательском интерфейсе, вы можете остановить применение всех правил Firewall. Служба Firewall будет продолжать работу.
Владельцы системы	Для правильной работы Firewall рекомендуется определить одного владельца системы (System).	Количество владельцев системы не влияет на Firewall.
Приоритет по умолчанию для нового правила	1	Последнее правило приоритета + 1
Содержимое карты событий Firewall	Информация о связанной атаке, которая была заблокирована или разрешена, и ссылка на нее.	Информация о запросе узла Diameter, который был заблокирован или разрешен.

8.2. Управление правилами SS7 Firewall

Данный раздел содержит инструкции по управлению правилами SS7 Firewall.

В этом разделе

8.2.1. Создание правил Firewall

Трафик проверяется по правилам Firewall в порядке их приоритета. Если входящий запрос соответствует условию правила, к нему применяется действие (блокировать или разрешить) и сообщение не проверяется по остальным правилам.

► Чтобы создать правило Firewall, сделайте следующее:

1. На панели инструментов нажмите .
2. В появившемся меню настроек нажмите **Firewall rules**.
3. Откройте вкладку **SS7 rules**.
4. Нажмите .

   Откроется страница создания правила Firewall.

   Примечание. Вы также можете открыть форму создания правила, заполненную данными, отображаемыми в интерфейсе (см. раздел 8.2.2).
5. Включите правило.

   Примечание. Вы также можете включать и отключать правила, используя столбец **State** на странице **Firewall rules**.
6. Если необходимо, в поле **Description** введите описание правила.
7. В раскрывающемся списке **Action** выберите действие, которое необходимо применять к сообщениям, соответствующим условию правила.
   - **Block**: запретить попадание совпадающих сообщений в сеть оператора.
   - **Allow**: разрешить попадание соответствующих сообщений в сеть оператора.
8. Если необходимо, измените значение в поле **Priority**.

   По умолчанию приоритет нового правила Firewall равен 1, то есть правило имеет наивысший приоритет и трафик проверяется по нему в первую очередь.
9. В поле **Condition** введите условие правила Firewall, используя язык правил Firewall (см. раздел 8.4).
10. Если вы хотите, чтобы СОПТА создавал событие Firewall при каждом срабатывании правила, установите флажок **Log rule events**.
11. Нажмите кнопку **Сохранить**.

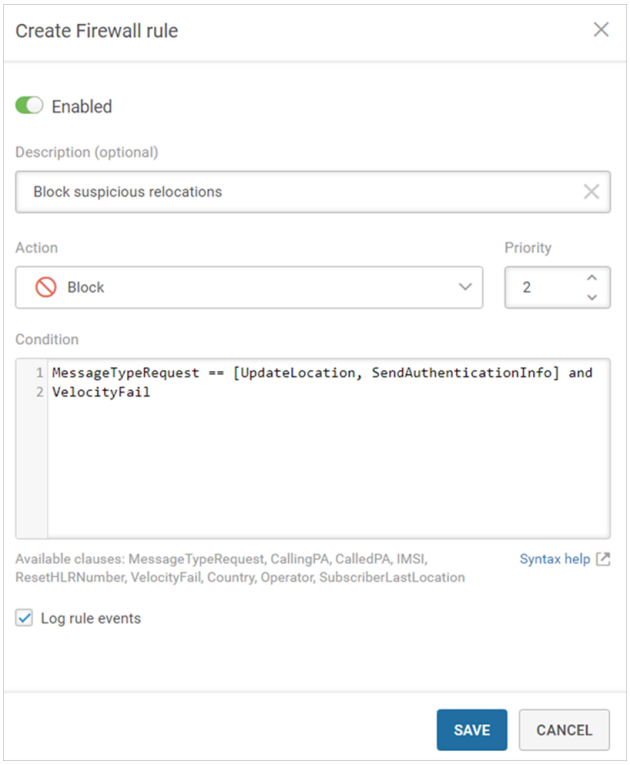


Рисунок 19. Создание правила Firewall

Правило Firewall создано. Для применения правил Firewall необходимо также включить функцию Firewall (см. раздел 8.2.3).

8.2.2. Выбор критерия правила Firewall на основе существующих данных

При наличии атак с определенных номеров или с определенными типами сообщений вы можете открыть форму создания правила Firewall, заполненную имеющимися данными. В таких правилах значение **Source** атаки используется как выражение **CallingPA**, а тип атаки задает выражение **MessageTypeRequest**.

Примечание. Использование существующих атрибутов атаки в правилах Firewall не обязательно предотвращает подобные атаки; функция используется только для быстрого заполнения полей в диалоговом окне создания правил.

- Чтобы использовать номер источника и тип сообщений имеющейся атаки,

  на странице **Attacks** наведите курсор мыши на ••• справа от атаки и нажмите .

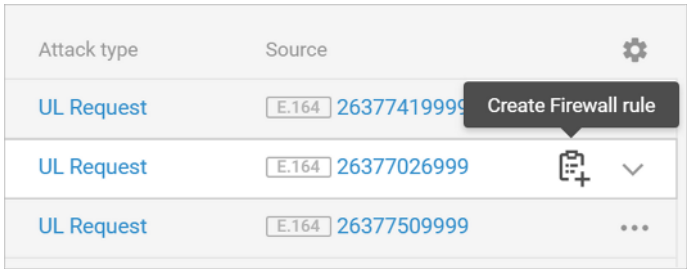


Рисунок 20. Создание правила Firewall из списка атак

- Чтобы использовать номер источника имеющейся атаки,

  в карточке атаки или в списке атак нажмите на значение атрибута источника и в открывшемся меню выберите пункт **Create Firewall rule**.

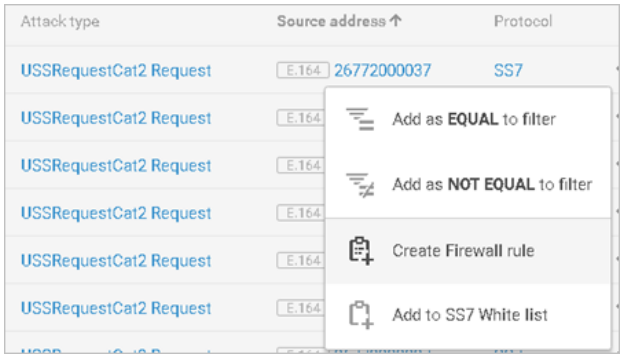


Рисунок 21. Создание правила Firewall из карточки атаки

- Чтобы использовать номер источника из статистических данных,

  на странице **Dashboards** нажмите на номер источника на диаграмме **<Top … sources>** или **<Top … sources by attack types count>** и в открывшемся меню выберите пункт **Create Firewall rule**.

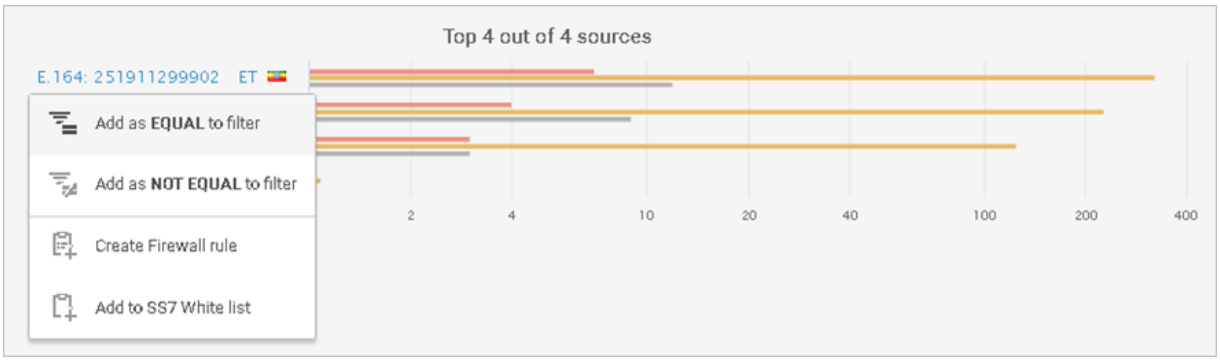


Рисунок 22. Создание правила Firewall на странице **Dashboards**

8.2.3. Включение и отключение службы Firewall

По умолчанию служба Firewall отключена: все входящие сообщения могут входить в сеть оператора.

Чтобы включить СОПТА для блокировки или явного разрешения сообщений на основе правил Firewall, необходимо включить службу Firewall.

- Чтобы включить службу Firewall, сделайте следующее:

  1. На панели инструментов нажмите  .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Откройте вкладку **SS7 rules**.
  4. В левой части страницы наведите курсор на  и нажмите  .
  5. В открывшемся окне подтверждения нажмите кнопку **Enable**.

  Служба Firewall включена. Для применения правил Firewall их также необходимо включить в процессе создания или изменения.

Чтобы включить СОПТА после блокировки или явно разрешить сообщения на основе правил Firewall, необходимо отключить службу Firewall.

> **Примечание.** Отключение службы Firewall закрывает ассоциации SCTP, поэтому Firewall больше не будет получать запросы на обработку. Поэтому необходимо обеспечить правильную маршрутизацию таких сообщений без модуля Firewall.

- Чтобы отключить службу Firewall, сделайте следующее:

  1. На панели инструментов нажмите  .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Откройте вкладку **SS7 rules**.
  4. В левой части страницы наведите указатель мыши на  и нажмите  .
  5. В открывшемся окне подтверждения нажмите кнопку **Disable**.

  Служба Firewall отключена, и правила Firewall не применяются.

8.2.4. Редактирование правил Firewall

- Чтобы изменить правило Firewall, выполните следующие действия:

  1. На панели инструментов нажмите  .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Откройте вкладку **SS7 rules**.

4. Наведите указатель мыши на правило Firewall и нажмите .
5. Измените настройки правила Firewall.

   Примечание. При снижении приоритета правила может быть повышен приоритет правил с более низким приоритетом. При повышении приоритета правила может быть снижен приоритет правил с более высоким приоритетом.
6. Нажмите кнопку **Сохранить**.

8.2.5. Удаление правила Firewall

- Чтобы удалить правило Firewall, выполните следующие действия:

  1. На панели инструментов нажмите .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Наведите указатель мыши на правило Firewall и нажмите .
  4. Нажмите для подтверждения удаления.

  Примечание. Удаление правила повышает приоритет всех правил, расположенных ниже удаленного.

8.3. Управление правилами Diameter Firewall

Данный раздел содержит инструкции по управлению правилами Diameter Firewall.

В Diameter Firewall каждое правило присоединяется к группе Firewall. Группа Firewall — это группа экземпляров Firewall, которые должны принимать один и тот же трафик, например, для защиты определенного оператора в точке межсоединения или обработки трафика от конкретного поставщика IPX. Если вы создаете, редактируете или удаляете правило, вы делаете это только в отношении определенной группы Firewall, поэтому перед внесением каких-либо изменений необходимо выбрать группу Firewall. По умолчанию существует только одна группа — **Default**.

Включение и приостановка Diameter Firewall не относятся к группе Firewall, эти действия применяются ко всем группам Firewall.

Примечание. Diameter Firewall не обрабатывает запросы, где значение Application-ID равно 0 (общие сообщения Diameter). Такие запросы разрешены, даже если они соответствуют правилу Firewall.

В этом разделе

Удаление правила Firewall (см. раздел 8.3.5)

Применение изменений (см. раздел 8.3.6)

8.3.1. Создание правил Firewall

Трафик проверяется по правилам Firewall в порядке их приоритета. Если входящий запрос соответствует условию правила, к нему применяется действие (блокировать или разрешить) и запрос не проверяется по остальным правилам.

► Чтобы создать правило Firewall, сделайте следующее:

1. На панели инструментов нажмите  .
2. В появившемся меню настроек нажмите **Firewall rules**.
3. Перейдите на вкладку **Diameter rules**.
4. Выберите группу Firewall, в которую вы хотите добавить правило.
5. Нажмите  .

   Откроется диалоговое окно **Create Firewall rule**.

   Примечание. Вы также можете открыть диалоговое окно создания правил, предварительно заполненное данными, отображаемыми в пользовательском интерфейсе (см. раздел 8.2.2).
6. Включите правило.

   Примечание. Вы также можете включать и отключать правила, используя столбец **State** на странице **Firewall rules**.
7. В поле **Description** введите описание правила.
8. В списке **Action** выберите действие, которое будет применено к соответствующим запросам.
   - **Block**: предотвратить попадание совпадающих запросов в сеть оператора.
   - **Allow**: разрешить попадание соответствующих запросов в сеть оператора.
9. Если необходимо, измените значение в поле **Priority**.

   Значение приоритета по умолчанию для нового правила Firewall — приоритет самого низкого правила, увеличенный на единицу.
10. В поле **Condition** введите условие правила Firewall, используя язык правил Firewall (см. раздел 8.4).
11. Если вы хотите, чтобы СОПТА создавал событие Firewall при каждом срабатывании правила, установите флажок **Log rule events**.
12. Нажмите кнопку **Сохранить**.

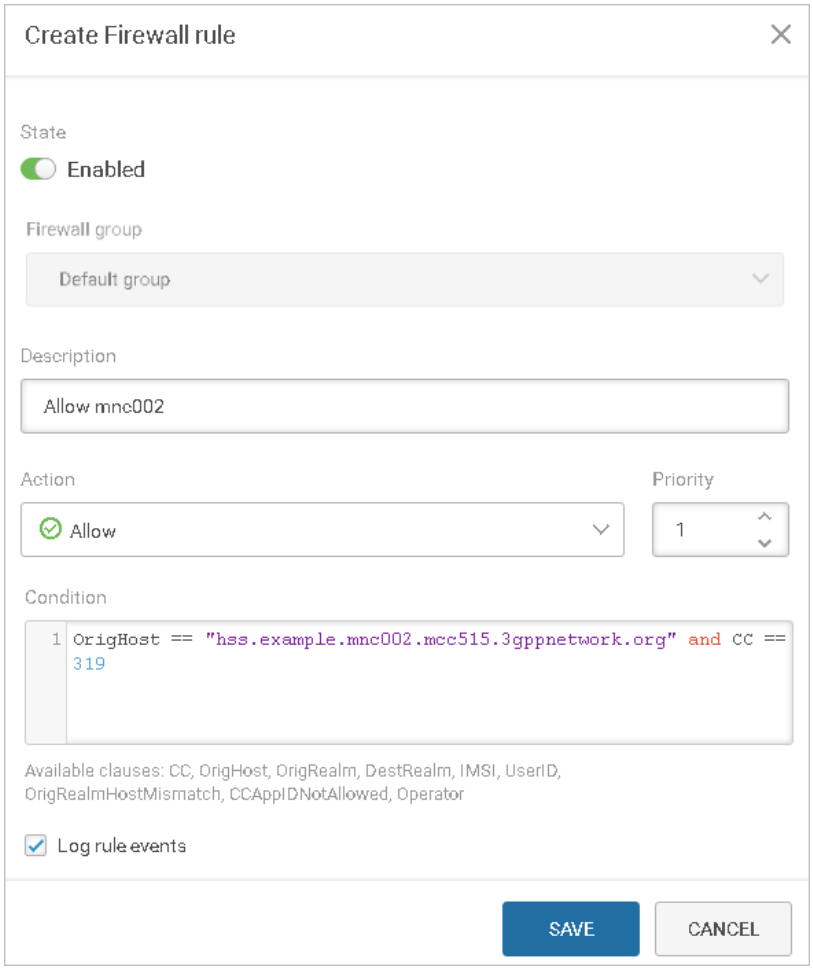


Рисунок 23. Создание правила Diameter Firewall

Правило Firewall создано. Чтобы правило вступило в силу, необходимо применить изменения (см. раздел 8.3.6) и убедиться, что Firewall включен (см. раздел 8.2.3).

8.3.2. Выбор критерия правила Firewall на основе существующих данных

Если у вас уже есть атаки с определенных хостов с определенными кодами команд, вы можете открыть диалоговое окно создания правила Firewall, предварительно заполненное существующими данными. В таких правилах исходное значение хоста используется в качестве выражения OrigHost, а запрос кода команды используется в качестве выражения CC.

Примечание. Использование существующих атрибутов атаки в правилах Firewall не обязательно предотвращает подобные атаки; функция используется только для быстрого заполнения полей в диалоговом окне создания правил.

- Чтобы использовать исходный хост и запросить тип имеющейся атаки,

  на странице **Attacks** наведите курсор мыши на ••• справа от атаки и нажмите .

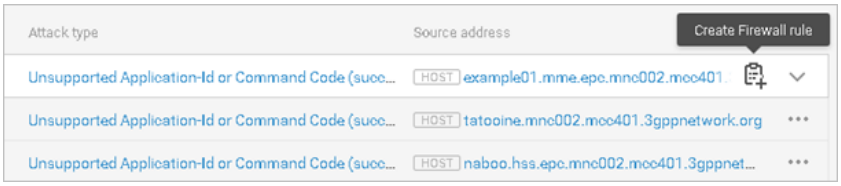


Рисунок 24. Создание правила Firewall из списка атак

- Чтобы использовать исходный хост имеющейся атаки,

  в карточке атаки или в списке атак выберите исходное значение хоста и в появившемся меню выберите **Create Firewall rule**.

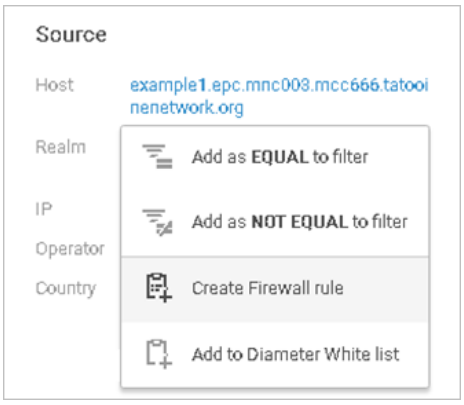


Рисунок 25. Создание правила Firewall из карточки атаки

- Чтобы использовать исходный хост из статистических данных,

  на странице **Dashboards** нажмите на номер источника на диаграмме **<Top … sources>** или **<Top … sources by attack types count>** и в появившемся меню выберите пункт **Create Firewall rule**.

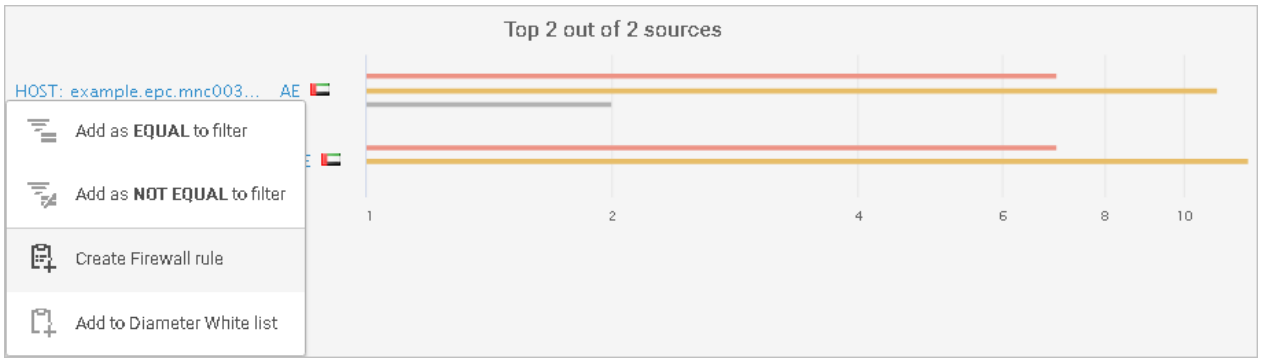


Рисунок 26. Создание правила Firewall на странице **Dashboards**

8.3.3. Включение и приостановка Firewall

По умолчанию Firewall приостановлен: все входящие запросы разрешены для доступа к сети оператора. Чтобы включить СОПТА для блокировки или явного разрешения запросов на основе правил Firewall, необходимо включить службу Firewall.

- Чтобы включить Firewall, сделайте следующее:

  1. На панели инструментов нажмите .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Перейдите на вкладку **Diameter rules**.
  4. В левой части страницы наведите курсор на и нажмите .
  5. В появившемся диалоговом окне подтверждения нажмите кнопку **Enable**.

  Firewall включен. Для применения правил Firewall их также необходимо включить в процессе создания или изменения.

Чтобы включить после блокировки или явно разрешить запросы на основе правил Firewall, необходимо отключить службу Firewall.

- Чтобы приостановить Firewall, сделайте следующее:

  1. На панели инструментов нажмите .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Перейдите на вкладку **Diameter rules**.
  4. В левой части страницы наведите указатель мыши на и нажмите .
  5. В появившемся диалоговом окне подтверждения нажмите кнопку **Disable**.

  Firewall приостановлен, и никакие правила Firewall не применяются.

8.3.4. Редактирование правил Firewall

- Чтобы изменить правило Firewall, выполните следующие действия:

  1. На панели инструментов нажмите .
  2. В появившемся меню настроек нажмите **Firewall rules**.
  3. Перейдите на вкладку **Diameter rules**.
  4. Выберите группу Firewall.
  5. Наведите указатель мыши на правило Firewall и нажмите .
  6. Измените настройки правила Firewall.

Примечание. При снижении приоритета правила может быть повышен приоритет правил с более низким приоритетом. При повышении приоритета правила может быть снижен приоритет правил с более высоким приоритетом.

7. Нажмите кнопку **Сохранить**.

Правило Firewall отредактировано.

Чтобы изменения вступили в силу, их следует применить (см. раздел 8.3.6).

8.3.5. Удаление правила Firewall

- Чтобы удалить правило Firewall, выполните следующие действия:

1. На панели инструментов нажмите .
2. В появившемся меню настроек нажмите **Firewall rules**.
3. Перейдите на вкладку **Diameter rules**.
4. Выберите группу Firewall.
5. Наведите указатель мыши на правило Firewall и нажмите .
6. Нажмите для подтверждения удаления.

Примечание. Удаление правила повышает приоритет всех правил, расположенных ниже удаленного.

Чтобы правило прекратило обработку трафика, необходимо применить изменения (см. раздел 8.3.6).

8.3.6. Применение изменений

При внесении изменений в группу Firewall (создание, редактирование или удаление правила) они не будут автоматически применяться к Firewall. Вместо этого на вкладке **Diameter rules** появится сообщение о том, что изменения сохранены, но не применены (**Changes saved but not applied to Firewall**). Вы можете применить или отменить изменения.

- Чтобы применить изменения, сделайте следующее:

1. На панели инструментов нажмите .
2. В появившемся меню настроек нажмите **Firewall rules**.
3. Перейдите на вкладку **Diameter rules**.
4. Выберите группу Firewall.
5. Нажмите кнопку **Apply**.

Все изменения в выбранной группе Firewall будут применены.

8.4. Язык правил Firewall

Чтобы правило Firewall могло применяться к сообщению, оно должно соответствовать условию правила. Условия задаются с помощью языка правил Firewall.

Условия правил Firewall состоят из выражений, определяющих трафик, к которому необходимо применять эти правила. Предложение может быть параметром сообщения и его значением или специальным выражением.

Поскольку структуры сообщений MAP, CAP и Diameter отличаются, пункты правил межсетевого экрана для SS7 и Diameter также различаются. Синтаксические требования (касающиеся операторов равенства и неравенства, комментариев, нечувствительности к регистру) одинаковы для обоих межсетевых экранов.

В этом разделе

Синтаксис правил (см. раздел 8.4.1)

Выражения правил SS7 (см. раздел 8.4.2)

Выражения правил Diameter (см. раздел 8.4.3)

8.4.1. Синтаксис правил

Операторы равенства и неравенства

Если для применения правила параметр должен быть равен указанному значению, используйте оператор равенства `==`.

```
IMSI == 648040280727544
CC == 322
```

Если для применения правила параметр должен быть не равен указанному значению, используйте оператор неравенства `!=`.

```
CalledPA != 26328960439
OrigHost! = Diascanner.example.epc.mnc012.mcc244.3gppnetwork.org
```

Значения IMSI и GT

В правилах Firewall SS7 значения IMSI и GT можно указывать одним из следующих способов:

— Полный номер
  `IMSI == 648010280727545`

— Префикс со звездочкой
  `IMSI == 64804*`

— Специальные переменные:

- `MyIMSI` — все IMSI, которые начинаются с MCC + MNC владельца системы.

```
IMSI == MyIMSI
```

- `MyGT` — все адреса Global Title, которые начинаются с CC + NDC владельца системы. `CalledPA == MyGT`

Примечание. Правила Diameter Firewall не позволяют использовать префиксы. Вы можете указать только точные значения в выражениях `CC` и `OrigHost`.

Перечисления

Для указания нескольких значений параметра необходимо заключить значения в квадратные скобки и разделить запятыми.

```
CalledPA == [26328960431, 26328960432]
IMSI == [64801*, 64803*, 64804*]
CC != [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]
```

Комментарии

Для объяснения значения выражений вы можете использовать комментарии. Для однострочных комментариев используется символ `//`, для многострочных комментариев используются символы `/*...*/`. Текст после символа `//` до конца строки или с символами `/*...*/` в начале и в конце считается комментарием и не считается частью выражений.

```
CalledPA == 26328960431 // однострочный комментарий
MessageTypeRequest == CancelLocation
/*многострочный комментарий*/
```

8.4.2. Выражения правил SS7

Условие правила Firewall должно включать в себя хотя бы одно выражение. Регистр символов в выражениях не учитывается. Чтобы проверить запросы, используя несколько пунктов, их можно объединить с помощью операции `and`. Правило будет применяться к запросу, если оно соответствует всем выражениям условия правила.

Например:

```
IMSI == 12345* and
CallingPA != 26328960438
```

Правило применяется к сообщениям, в которых IMSI начинается с 12345 и Calling Party Address не равен 26328960438.

MessageTypeRequest

Название (см. приложение А) службы MAP или CAP-операции (без пробелов и дефисов)

Пример:

```
MessageTypeRequest == [CancelLocation, UpdateLocation]
```

Правило применяется к запросам CancelLocation и UpdateLocation.

```
MessageTypeRequest != SendRoutingInfo
```

Правило применяется ко всем запросам, кроме SendRoutingInfo.

```
MessageTypeRequest == MAPUnused
```

Правило применяется к запросам с неиспользуемыми кодами операций MAP (0, 1, 16, 27, 78–82, 90–255).

```
MessageTypeRequest == CAPUnused
```

Правило применяется к запросам с неиспользуемыми кодами операций CAP (1–15, 21, 25, 26, 28–30, 37–40, 42, 43, 50–52, 54, 57–59, 68, 69, 84, 85, 87, 89, 91, 92, 94, 98–255).

IMSI

International Mobile Subscriber Identity

Пример:

```
IMSI == 12345*
```

Правило применяется к сообщениям, в которых IMSI начинается с 12345.

> **Примечание.** Для запросов MAP Reset СОПТА проверяет только первый IMSI из HLR-List (см. раздел 8.4.2).

CallingPA

Источник сообщения (Calling Party Address)

Пример:

```
CallingPA == [26328960438, 26328960439]
```

Правило применяется к сообщениям, в которых Calling Party Address равен 26328960438 или 26328960439.

CalledPA

Адресат сообщения (Called Party Address)

Пример:

```
CalledPA != MyGT
```

Правило применяется к сообщениям, в которых адреса Global Title Called Party Address не принадлежат владельцу системы.

HLR-Number в запросах MAP Reset

Чтобы применить правило к запросам MAP Reset, в которых оператор, определяемый по HLR-Number, совпадает с оператором Called Party Address, вы можете использовать выражение `ResetHLRNumber` и указать одинаковый адрес Global Title (или его префикс) в `ResetHLRNumber` и `CalledPA`.

```
MessageTypeRequest == Reset и CalledPA == <GT оператора A> и ResetHLRNumber == <GT оператора A>
```

Пример:

```
MessageTypeRequest == Reset and CalledPA == MyGT and ResetHLRNumber == MyGT
```

Правило применяется к запросам MAP Reset, в которых Called Party Address и HLR-Number принадлежат владельцу системы.

> **Примечание.** Указывать `MessageTypeRequest == Reset` не обязательно. Если указан тип сообщений, отличный от Reset, условие становится некорректным и правило не применяется.

HLR-List в запросах MAP Reset

Если вы используете выражение `IMSI` с типом сообщений Reset, СОПТА проверяет первый IMSI из HLR-List в запросах MAP Reset. Вы можете использовать это для применения правила к запросам MAP Reset, в которых оператор, определяемый по HLR-List, совпадает с оператором Called Party Address.

> **Примечание.** Если первый IMSI из HLR-List не соответствует IMSI, указанному в правиле, остальные IMSI из HLR-List не проверяются и правило не применяется.

```
MessageTypeRequest == Reset и CalledPA == <GT оператора A> и IMSI == <IMSI оператора A>
```

Пример:

```
MessageTypeRequest == Reset and CalledPA == MyGT and IMSI == MyIMSI
```

Правило применяется к запросам MAP Reset, в которых Called Party Address и первый IMSI из HLR-List принадлежат владельцу системы.

Проверка скорости изменения местоположения

С помощью номера VLR из запросов UpdateLocation или SendAuthenticationInfo СОПТА определяет страну текущего местоположения абонента и сравнивает ее с предыдущей страной (получаемой из предыдущего сообщения UpdateLocation). Информация о предыдущей стране хранится только для абонентов владельца системы.

С помощью выражения `VeloctityFail` вы можете применять правило Firewall к запросам UpdateLocation и SendAuthenticationInfo, если время изменения местоположения абонента меньше указанного приемлемого значения. Если СОПТА не удается определить страну, правило не применяется.

Пример:

```
MessageTypeRequest == SendAuthenticationInfo and
VeloctityFail
```

Примечание. Если `MessageTypeRequest` не указан, правило применяется к запросам UpdateLocation и SendAuthenticationInfo. Вы можете указывать только эти типы сообщений в выражении `VeloctityFail`. Если указаны другие типы сообщений, условие становится некорректным и правило не применяется.

Проверка последнего местоположения абонента

Выражения `Country()` и `Operator()` позволяют сравнивать страны и операторов из параметров сообщений: `CallingPA`, `CalledPA`, `IMSI`, `ResetHLRNumber`.

```
Country(CallingPA) == Country(IMSI) // проверка, соответствует ли страна в адресе источника стране IMSI
```

С помощью функции `SubscriberLastLocation` вы можете сравнивать один из этих параметров с последним известным местоположением абонента (получаемым из последнего сообщения UpdateLocation). Например, это позволяет блокировать сообщения категорий MAP 3.1 и CAP 3, если текущее местоположение абонента (страна или оператор номера источника) не соответствует последнему известному местоположению.

Информация о последнем известном местоположении хранится только для абонентов владельца системы, поэтому Firewall применяет правило к запросам, которые содержат IMSI из диапазона IMSI владельца системы. По умолчанию информация о местоположении хранится 24 часа. Если для абонента не поступал запрос UpdateLocation или запрос, который необходимо проверить, получен спустя 24 часа после запроса UpdateLocation, правило не применяется.

Примечание. Вы можете сравнивать `Country()` только с `Country()` и `Operator()` только с `Operator()`.

Пример:

```
MessageTypeRequest == RegisterSS and
Country(CallingPA) != Country(SubscriberLastLocation)
```

Правило применяется к запросам RegisterSS, если текущая страна абонента отличается от последней известной страны.

```
MessageTypeRequest == RegisterSS and
Operator(CallingPA) != Operator(SubscriberLastLocation)
```

Правило применяется к запросам RegisterSS, если оператор, обслуживающий абонента в данный момент, отличается от последнего известного оператора.

См. также

Рекомендуемые правила Firewall SS7 (см. приложение Б)

8.4.3. Выражения правил Diameter

Условие правила Firewall должно включать в себя хотя бы одно выражение. Регистр символов в выражениях не учитывается. Чтобы проверить запросы, используя несколько пунктов, их можно объединить с помощью операции `and`. Правило будет применяться к запросу, если оно соответствует всем выражениям условия правила.

CC

Command Code. Значение является целым числом от 0 до 16 777 215 включительно.

Например:

```
CC != 322
CC == [123, 456, 789]
```

OrigHost

Параметр проверяет AVP Origin-Host, который идентифицирует конечную точку, из которой исходил запрос Diameter. Значение является именем хоста, заключенным в кавычки. Вы можете использовать обратный слеш для выделения кавычек (`\"`) и обратные слеши (`\\`), если вы хотите, чтобы Firewall рассматривал их как часть имени хоста.

Например:

```
OrigHost == "diascanner.example.epc.mnc012.mcc244.3gppnetwork.org"
```

Operator

Функция проверяет, совпадает ли оператор одного AVP с оператором другого AVP. Функция принимает `OrigRealm`, `IMSI` или `UserID` в качестве аргумента и идентифицирует оператора на основе MCC и MNC из этих AVP. Если оператор не идентифицирован, результат функции будет равен `Unknown` и правило не будет применяться.

Например:

```
Operator(OrigRealm) != Operator(UserId)
```

Применяет правило к запросам, когда оператор Origin-Realm не совпадает с оператором UserId.

CCAppIDNotAllowed

Функция проверяет, соответствуют ли параметры Command Code и Application-ID параметрам одной из указанных пар Command Code и Application-ID. Формат пары `(<Command Code>, <Application-ID>)`. Пары разделены запятой. Список пар заключен в квадратные скобки. Если запрос не соответствует ни одной из пар в списке, действие не применяется.

Примечание. Diameter Firewall не обрабатывает запросы, где значение Application-ID равно 0 (общие сообщения Diameter). Такие запросы разрешены, даже если они соответствуют правилу Firewall.

Например:

```
CCAppIDNotAllowed([(316,16777251),(317,16777251),(318,16777251),(319,16777251),
(320,16777251),(321,16777251),(322,16777251),(323,16777251)])
```

OrigRealmHostMismatch

Функция проверяет, содержит ли AVP Origin-Host область из AVP Origin-Realm. Если это не так, действие применяется.

OrigRealm и DestRealm

Параметры проверяют, равен ли AVP Origin-Realm значению AVP Destination-Realm. Они могут использоваться только в следующих выражениях:

```
OrigRealm == DestRealm
```

```
OrigRealm != DestRealm
```

Запись выражения в обратном порядке, например `DestRealm == OrigRealm`, допустима, но имеет то же значение, что и `OrigRealm == DestRealm`.

9. Работа с учетными записями пользователей

В СОПТА существуют два типа пользователей:

— Собственные пользователи, которые могут просматривать любые атаки, зарегистрированные СОПТА.

— Партнерские пользователи, которые связаны с оператором и могут просматривать только атаки, относящиеся к этому оператору. Отчеты и JSON-файлы, созданные такими пользователями, также включают в себя только атаки, относящиеся к этому оператору. Партнерский пользователь может иметь только роль оператора безопасности.

В СОПТА существуют два типа учетных записей пользователей:

— Локальные учетные записи, которые создают администраторы СОПТА . Администраторы СОПТА могут изменять все параметры локальных учетных записей.

— Учетные записи LDAP, которые автоматически создаются при первом входе пользователей Active Directory в СОПТА. Параметры таких учетных записей загружаются с соответствующего сервера Active Directory (см. раздел 11). Они обновляются в СОПТА при каждом входе пользователя LDAP в СОПТА. Единственным параметром учетной записи LDAP, который можно изменить, является **Role**.

Учетные записи LDAP доступны только для собственных пользователей.

В этом разделе

9.1. Создание локальной учетной записи

Чтобы предоставить локальному пользователю доступ в СОПТА , необходимо создать учетную запись и передать пользователю логин и пароль для входа в СОПТА.

Примечание. Чтобы предоставить пользователю LDAP доступ в СОПТА, необходимо настроить интеграцию с LDAP-сервером (см. раздел 11) и активировать учетную запись, которая автоматически создается при первом входе пользователя LDAP в СОПТА.

► Чтобы создать локальную учетную запись, сделайте следующее:

1. На панели инструментов нажмите  .
2. В открывшемся меню настроек выберите пункт **Users**.

   Откроется страница **Пользователи**.

3. Нажмите  .

   Откроется страница создания учетной записи.

4. Выберите тип пользователя: **Own user** — пользователь может просматривать любые атаки, или **Partner user** — пользователь может просматривать только атаки определенного оператора. После создания учетной записи тип пользователя не может быть изменен.

5. Для партнерского пользователя в раскрывающемся списке **Partner operator** выберите оператора, к которому относится пользователь. После создания учетной записи оператор не может быть изменен.

6. Для собственного пользователя в раскрывающемся списке **Role** выберите роль (см. раздел 5).

   Примечание. Партнерский пользователь может иметь только роль оператора безопасности.

7. В поле **Login** введите уникальный логин.

8. В поле **Email** введите адрес электронной почты пользователя.

9. Установите пароль пользователя. Для этого введите пароль в поле **Password** или нажмите кнопку **Generate password**.

10. Если вы хотите, чтобы пользователь изменил указанный пароль на собственный, установите флажок **Require the user to change password at the next sign in**. При следующем входе в СОПТА пользователю будет предложено создать новый пароль.

11. Нажмите кнопку **Сохранить**.

Локальная учетная запись создана и появится в списке учетных записей.

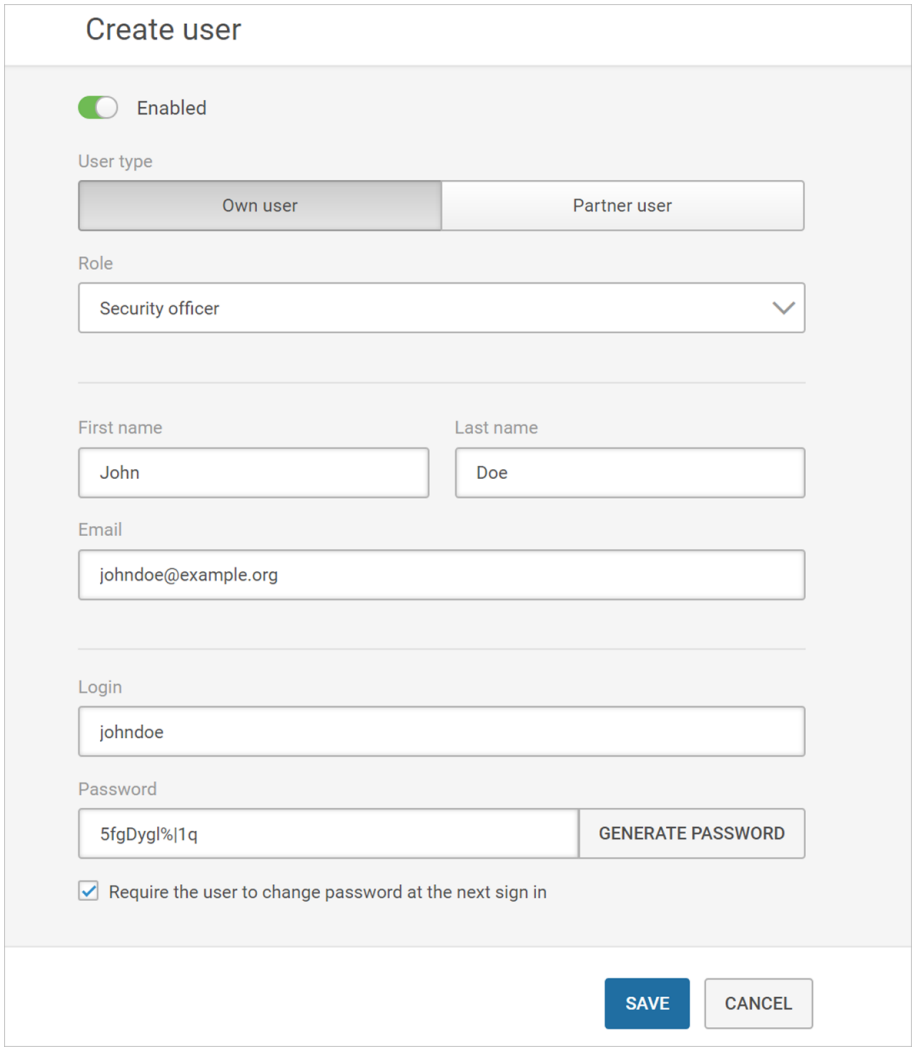


Рисунок 27. Создание локальной учетной записи

9.2. Изменение учетной записи

► Чтобы изменить учетную запись, выполните следующее действие:

1. На панели инструментов нажмите ⚙.
2. В открывшемся меню настроек выберите пункт **Users**.

   Откроется страница **Users**.
3. Справа от учетной записи пользователя наведите курсор на ••• и нажмите ✎.

   Откроется страница **Edit user**.
4. Измените параметры учетной записи.

Примечание. Для учетных записей LDAP вы можете только изменить роль пользователя и включить или отключить учетную запись. Другие параметры учетной записи извлекаются с сервера LDAP и обновляются каждый раз, когда пользователь LDAP входит в СОПТА .

5. Нажмите кнопку **Сохранить**.

Учетная запись изменена.

9.3. Удаление учетной записи

- Чтобы удалить учетную запись пользователя:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Users**.

   Откроется страница **Users**.
3. Справа от учетной записи наведите курсор мыши на и нажмите .
4. Нажмите для подтверждения удаления.

   Примечание. Чтобы удалить сразу несколько учетных записей, вы можете выбрать их с помощью флажков слева от списка учетных записей, нажать и подтвердить удаление, нажав .

Учетная запись удалена.

9.4. Блокирование учетной записи

Вы можете блокировать учетные записи для ограничения доступа пользователей в СОПТА .

- Чтобы заблокировать учетную запись, сделайте следующее:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **Users**.

   Откроется страница **Пользователи**.
3. В столбце **State** выключите переключатель рядом с учетной записью пользователя.

Учетная запись заблокирована. Пользователь не сможет войти в СОПТА.

9.5. Активация учетной записи

Если учетная запись заблокирована, пользователь не имеет доступа в СОПТА .

При первом входе пользователей LDAP в СОПТА их учетные записи автоматически создаются в СОПТА. По умолчанию учетные записи LDAP заблокированы. Чтобы предоставить пользователю LDAP доступ в СОПТА, необходимо активировать учетную запись.

- Чтобы активировать учетную запись, сделайте следующее:

  1. На панели инструментов нажмите  .
  2. В открывшемся меню настроек выберите пункт **Users**.

     Откроется страница **Пользователи**.
  3. В столбце **State** включите переключатель рядом с учетной записью пользователя.

  Учетная запись активирована. Пользователь сможет войти в СОПТА.

10. Скачивание журнала действий пользователей

Журналы действий пользователей позволяют отслеживать историю действий, совершенных пользователями СОПТА в веб-интерфейсе. Вы можете скачивать журналы действий пользователей в формате CSV. СОПТА сохраняет информацию о следующих HTTP-запросах к веб-серверу в качестве журналов действий пользователей. Запросы GET на выход из продукта и любые запросы POST, PUT и DELETE. Журналы также содержат информацию о неудавшихся попытках войти в продукт.

► Чтобы выгрузить историю действий пользователя:

1. На панели инструментов нажмите .
2. В открывшемся меню настроек выберите пункт **User logs**.
3. В поле **For period** введите период, за который вы хотите скачать журнал действий пользователей.

   Вы также можете нажать , чтобы выбрать период с помощью календаря.
4. Выберите пользователей, действия которых вы хотите включить в журнал.
   - Если вы хотите скачать журнал действий всех пользователей, выберите **All users**. Журнал будет также содержать информацию обо всех неудавшихся попытках войти в СОПТА.
   - Если вы хотите скачать журнал действий определенных пользователей, выберите **Selected users** и выберите необходимые учетные записи. Журнал будет также содержать информацию о неудавшихся попытках войти в СОПТА с помощью выбранных учетных записей.
5. Нажмите кнопку **Download**.

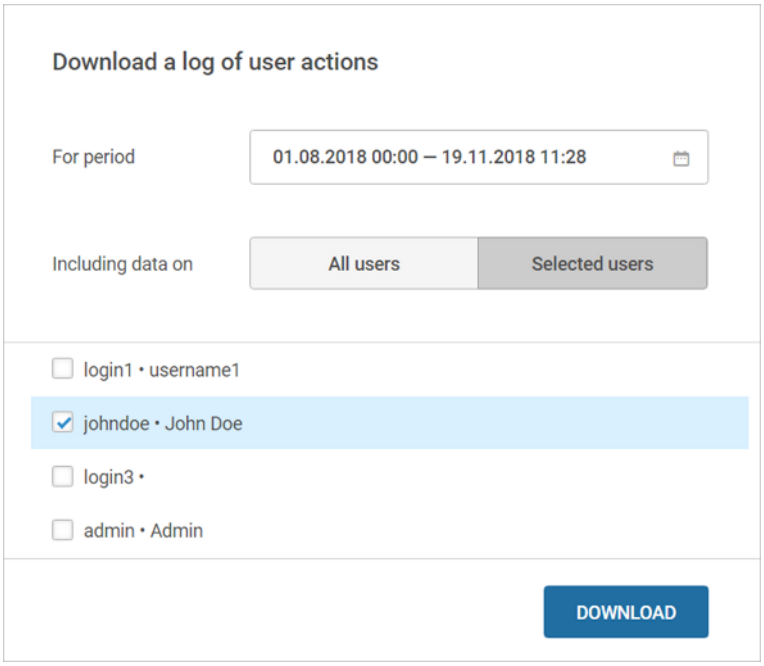


Рисунок 28. Скачивание журнала действий пользователей

Начнется создание файла журнала. Если файл журнала успешно создан, в верхней части страницы появится сообщение **File generation completed**. В противном случае появится сообщение об ошибке.

6. На панели инструментов нажмите .

   Откроется меню загрузок: успешно сгенерированные файлы помечены , неудачные попытки помечены . Если генерация файла не удалась, вы можете навести курсор на уведомление о неудачной попытке, чтобы просмотреть сообщение об ошибке, и нажать , чтобы повторить попытку.

   Примечание. Созданные файлы доступны для скачивания в течение 24 часов. Файлы, созданные более 24 часов назад, периодически удаляются и недоступны для скачивания в меню **Downloads**.

7. Нажмите ссылку с именем созданного файла журнала.

Начнется скачивание журнала действий пользователей.

11. Настройка интеграции с LDAP-сервером

СОПТА позволяет настроить интеграцию с LDAP-сервером Active Directory. Это позволит пользователям LDAP, например сотрудникам вашей организации, входить в СОПТА с помощью логинов и паролей доменных учетных записей.

- Чтобы настроить интеграцию СОПТА с LDAP-сервером, выполните следующие действия:

  1. Откройте следующий файл: `/opt/ptsecurity/etc/backend_config.ini`.
  2. В секции `[ldap]` для атрибута `host` введите доменное имя LDAP-сервера, например `host = mycompany.example`.

  Пользователи вашего домена могут войти в СОПТА, используя учетные данные своего домена.

  Примечание. При первом входе пользователей LDAP в СОПТА их учетные записи автоматически создаются в СОПТА. По умолчанию учетные записи LDAP заблокированы. Чтобы предоставить пользователю LDAP доступ в СОПТА, необходимо активировать учетную запись (см. раздел 9.5).

12. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

12.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

12.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

12.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

12.4. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

Предоставление информации для технической поддержки (см. раздел 12.4.1)

Типы запросов (см. раздел 12.4.2)

Время реакции и приоритизация запросов (см. раздел 12.4.3)

Выполнение работ по запросу (см. раздел 12.4.4)

12.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

12.4.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

12.4.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 3).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 3. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

12.4.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Типы сообщений, поддерживаемые SS7 Firewall СОПТА

В таблице ниже представлен список MAP- и CAP-сообщений, доступных для выбора в СОПТА Firewall в качестве выражения `MessageTypeRequest`.

Таблица 4. Типы сообщений

Протокол	Код операции	Имя в MessageTypeRequest
MAP	2	UpdateLocation
	3	CancelLocation
	4	ProvideRoamingNumber
	5	NoteSubscriberDataModified
	6	ResumeCallHandling
	7	InsertSubscriberData
	8	DeleteSubscriberData
	9	SendParameters
	10	RegisterSS
	11	EraseSS
	12	ActivateSS
	13	DeactivateSS
	14	InterrogateSS
	15	AuthenticationFailureReport
	17	RegisterPassword
	18	GetPassword
	19	ProcessUnstructuredSSData
	20	ReleaseResources
	21	MTForwardSMVGCS
	22	SendRoutingInfo
	23	UpdateGPRSLocation
	24	SendRoutingInfoForGPRS
	25	FailureReport
	26	NoteMSPresentForGPRS
	28	PerformHandover
	29	SendEndSignal

Протокол	Код операции	Имя в MessageTypeRequest
	30	PerformSubsequentHandover
	31	ProvideSIWFSNumber
	32	SIWFSSignallingModify
	33	ProcessAccessSignalling
	34	ForwardAccessSignalling
	35	NoteInternalHandover
	36	CancelVCSGLocation
	37	Reset
	38	ForwardCheckSSIndication
	39	PrepareGroupCall
	40	SendGroupCallEndSignal
	41	ProcessGroupCallSignalling
	42	ForwardGroupCallSignalling
	43	CheckIMEI
	44	MTForwardSM
	45	SendRoutingInfoForSM
	46	MOForwardSM
	47	ReportSMDeliveryStatus
	48	NoteSubscriberPresent
	49	AlertServiceCentreWithoutResult
	50	ActivateTraceMode
	51	DeactivateTraceMode
	52	TraceSubscriberActivity
	53	UpdateVCSGLocation
	54	BeginSubscriberActivity
	55	SendIdentification
	56	SendAuthenticationInfo
	57	RestoreData
	58	SendIMSI
	59	ProcessUnstructuredSSRequest
	60	UnstructuredSSRequest
	61	UnstructuredSSNotify

Протокол	Код операции	Имя в MessageTypeRequest
	62	AnyTimeSubscriptionInterrogation
	63	InformServiceCentre
	64	AlertServiceCentre
	65	AnyTimeModification
	66	ReadyForSM
	67	PurgeMS
	68	PrepareHandover
	69	PrepareSubsequentHandover
	70	ProvideSubscriberInfo
	71	AnyTimeInterrogation
	72	SSInvocationNotification
	73	SetReportingState
	74	StatusReport
	75	RemoteUserFree
	76	RegisterCCEntry
	77	EraseCCEntry
	83	ProvideSubscriberLocation
	85	SendRoutingInfoForLCS
	86	SubscriberLocationReport
	87	IstAlert
	88	IstCommand
	89	NoteMMEvent
	0, 1, 16, 27, 78–82, 90–255	MAPUnused
CAP	0	InitialDP
	60	InitialDPSMS
	78	InitialDPGPRS
	1–15, 21, 25, 26, 28–30, 37–40, 42, 43, 50–52, 54, 57–59, 68, 69, 84, 85, 87, 89, 91, 92, 94, 98–255	CAPUnused

Приложение Б. Рекомендуемые правила Firewall SS7

Этот раздел содержит правила Firewall, рекомендуемые к использованию на основе рекомендаций по настройке межсетевых экранов в FS.11.

Category 1

Блокировать все запросы категории MAP 1 и запросы с неиспользуемыми кодами операций MAP и CAP:

```
MessageTypeRequest == [NoteSubscriberDataModified, ResumeCallHandling,
ReleaseResources, SendRoutingInfo, SendRoutingInfoForGprs, FailureReport,
NoteMsPresentForGprs, ProvideSiwfsNumber, SiwfsSignallingModify,
NoteInternalHandover, CheckIMEI, TraceSubscriberActivity, SendIdentification,
SendIMSI, AnyTimeSubscriptionInterrogation, AnytimeModification,
AnyTimeInterrogation, SendRoutingInfoForLCS, SubscriberLocationReport, MAPUnused,
CAPUnused]
```

MAP Category 2

Блокировать запросы категории MAP 2, где IMSI относится к одному из IMSI владельца системы:

```
MessageTypeRequest == [ProvideRoamingNumber, ProvideSubscriberInfo,
ProvideSubscriberLocation, CancelLocation, InsertSubscriberData,
DeleteSubscriberData, UnstructuredSSRequest, UnstructuredSSNotify] and IMSI == MyIMSI
```

Блокировать запросы сброса MAP, если первый IMSI из списка HLR принадлежит владельцу системы:

```
MessageTypeRequest == Reset and IMSI == MyIMSI
```

Блокировать запросы MAP Reset, в которых Called Party Address и HLR-Number принадлежат владельцу системы:

```
MessageTypeRequest == Reset and ResetHLRNumber == MyGT
```

MAP Category 3

Блокировать запросы категории MAP 3.1, если страна Calling Party Address не соответствует стране последнего местоположения абонента:

```
MessageTypeRequest == [RegisterSS, EraseSS, ActivateSS, DeactivateSS, InterrogateSS,
AuthenticationFailureReport, RegisterPassword, ProcessUnstructuredSsData,
ReportSMDeliveryStatus, NoteSubscriberPresent, BeginSubscriberActivity, RestoreData,
ProcessUnstructuredSSRequest, ReadyForSM, PurgeMS, SSInvocationNotification,
StatusReport, IstAlert, NoteMMEvent] and

Country(CallingPA) != Country(SubscriberLastLocation)
```

Блокировать запросы UpdateLocation и SendAuthenticationInfo, если время изменения местоположения абонента меньше приемлемого значения:

```
MessageTypeRequest == [UpdateLocation, SendAuthenticationInfo] and VelocityFail
```

CAP Category 3

Блокировать запросы категории CAP 3, если страна Calling Party Address не соответствует стране последнего местоположения абонента:

```
MessageTypeRequest == [InitialDP, InitialDPSMS, InitialDPGPRS] and
Country(CallingPA) != Country(SubscriberLastLocation)
```

Глоссарий

Attack type

Свойство атаки, которое определяется сигнатурами, использованными для обнаружения атаки. Тип атаки может определяться одной или несколькими сигнатурами.

Destination

Адрес, который используется для определения сетевого элемента, обслуживающего цель в текущий момент. Может иметь такое же значение, как атрибут Target, если цель атаки является сетевым элементом.

Firewall

Компонент, используемый для блокировки или разрешения входящих запросов до того, как они достигнут защищенного сетевого интерфейса.

Potential impact

Возможные последствия атаки для оператора: Data leakage, Fraud, Network element DoS, Subscriber DoS. Одна атака может иметь несколько возможных последствий.

Severity

Атрибут атаки, который указывает на степень угрозы, основываясь на последствиях и успешности атаки. Опасность зависит от типа атаки: каждый тип атаки имеет предопределенную опасность (высокую, среднюю или низкую).

Signature

Правило, которое определяет характеристики атаки в полученном трафике: порядок, в котором получены сообщения, наличие указанного запроса или ответа, отсутствие запроса или ответа в течение указанного времени, типы и атрибуты сообщений. Если сообщение или последовательность из сообщений соответствует сигнатуре, регистрируется атака.

Source

Элемент сети, откуда происходит атака.

System owner

Оператор, номерная емкость которого рассматривается в качестве домашней сети клиента. Выбор System owner позволяет продукту определить направление сообщения (входящее или исходящее) и принадлежность абонента, что необходимо для корректной работы некоторых сигнатур.

Target

Идентификатор атакованного абонента или сетевого элемента (например, MSC, SGSN, HLR или VLR).

Атака

Сообщение или последовательность сообщений, отправленных злоумышленником с целью достижения определенного результата (раскрытия конфиденциальных данных, нелегального использования ресурсов сети, отказа в обслуживании узлов или абонентов).

Группа Firewall

Группа Firewall — это группа экземпляров Firewall, которые должны принимать один и тот же трафик, например, для защиты определенного оператора в точке межсоединения или обработки трафика от конкретного поставщика IPX. Каждая группа Firewall имеет свой собственный набор правил Firewall.

Группа адресов

Наборы адресов (E.164-, E.212-, E.214-номера, номера IMEI, IP-адреса, узлы, области, UDP-порты), создаваемые пользователями. Группы адресов могут использоваться для быстрого добавления набора адресов в фильтры в качестве атрибутов Source, Target или Destination.

Правило Firewall

Инструкция, которая определяет действие (блокировать или разрешить) и трафик, к которому это действие необходимо применять (условие). Условия правил задаются с помощью специального языка правил Firewall.

Событие Firewall

Возникновение сработавшего правила Firewall. Событие записывается, если запрос соответствует всем критериям правила Firewall. Если запрос не соответствует правилу Firewall, сообщение разрешается, но событие Firewall не записывается.

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com