Positive Technologies Система Определения и Предотвращения Телекоммуникационных Атак

Версия R2.5

Руководство оператора безопасности

POSITIVE TECHNOLOGIES

Дата редакции документа: 05.11.2020

Содержание

1. Об этом документе ... 5
   - 1.1. Условные обозначения ... 5
   - 1.2. Другие источники информации о СОПТА ... 6
2. О СОПТА ... 7
3. Принцип работы СОПТА ... 8
   - 3.1. Алгоритм обработки трафика в СОПТА ... 8
     - 3.1.1. Этапы обнаружения атак СОПТА ... 8
     - 3.1.2. Этапы фильтрации трафика в СОПТА ... 9
   - 3.2. Об атаках в СОПТА ... 9
4. Вход в СОПТА ... 12
5. Пользовательский интерфейс СОПТА ... 13
   - 5.1. Обзор интерфейса СОПТА ... 13
   - 5.2. Страница Dashboards ... 15
   - 5.3. Страница Attacks ... 16
   - 5.4. Страница Firewall events ... 16
   - 5.5. Временная шкала ... 17
6. Просмотр подробной информации об атаках ... 19
   - 6.1. Просмотр карточки атаки ... 19
   - 6.2. Выгрузка JSON-файла ... 20
7. Просмотр снимков правил Firewall ... 22
8. Использование фильтров ... 23
   - 8.1. Фильтрация данных по времени ... 23
     - 8.1.1. Фильтрация данных с помощью календаря ... 23
     - 8.1.2. Фильтрация данных с помощью временной шкалы ... 24
   - 8.2. Фильтрация данных по атрибуту ... 25
     - 8.2.1. Информация об атрибутах в фильтрах ... 26
     - 8.2.2. Настройка фильтров ... 26
     - 8.2.3. Использование быстрых фильтров ... 27
     - 8.2.4. Сохранение фильтров ... 29
     - 8.2.5. Применение сохраненных фильтров ... 30
     - 8.2.6. Переименование сохраненных фильтров ... 30
     - 8.2.7. Удаление сохраненных фильтров ... 30
9. Настройка параметров отображения атак и событий Firewall ... 31
10. Выгрузка статистического отчета ... 33
11. Работа с правилами отчетов по расписанию ... 34
    - 11.1. Создание правила отчета по расписанию ... 34
    - 11.2. Создание правила отчета по расписанию на основе существующего фильтра ... 37
    - 11.3. Изменение правила отчета по расписанию ... 37
    - 11.4. Удаление правила отчета по расписанию ... 37
12. Работа с правилами уведомления ... 38
    - 12.1. Создание правила уведомления ... 39
    - 12.2. Создание правила уведомления на основе существующего фильтра ... 40
    - 12.3. Изменение правила уведомления ... 41
    - 12.4. Удаление правила уведомления ... 41
13. Управление группами адресов ... 42

13.1. Создание пользовательского справочника ... 42
13.2. Изменение группы адресов ... 43
13.3. Удаление группы адресов ... 43
14. Просмотр операторов ... 45
15. Настройка своей учетной записи ... 47
15.1. Изменение персональных данных ... 47
15.2. Смена пароля ... 47
16. Обращение в службу технической поддержки ... 49
16.1. Техническая поддержка на портале ... 49
16.2. Техническая поддержка по телефону ... 49
16.3. Время работы службы технической поддержки ... 50
16.4. Как служба технической поддержки работает с запросами ... 50
16.4.1. Предоставление информации для технической поддержки ... 50
16.4.2. Типы запросов ... 51
16.4.3. Время реакции и приоритизация запросов ... 52
16.4.4. Выполнение работ по запросу ... 53
Глоссарий ... 54

1. Об этом документе

Руководство оператора безопасности содержит пошаговые инструкции и справочную информацию об использовании продукта "Система Определения и Предотвращения Телекоммуникационных Атак" (далее также — СОПТА) для защиты и управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функций продукта для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию СОПТА.

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о СОПТА (см. раздел 1.2)

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

Пример текста с условным обозначением	Описание
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 16).

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, можно указать параметры сообщений, которые будут заблокированы.

3. Принцип работы СОПТА

В этом разделе содержится информация о принципе работы СОПТА.

В этом разделе

Алгоритм обработки трафика в СОПТА (см. раздел 3.1)

Об атаках в СОПТА (см. раздел 3.2)

3.1. Алгоритм обработки трафика в СОПТА

Трафик в СОПТА обрабатывается одновременно двумя методами, один из которых заключается в обнаружении атак, а второй — в фильтрации трафика.

Обнаружение атак заключается в выявлении потенциально опасных сообщений и их регистрации в виде атак без воздействия на трафик.

Фильтрация трафика — это дополнительная функция СОПТА, которая заключается в блокировании входящих MAP- и CAP-сообщений, соответствующих указанным критериям, для предотвращения их проникновения в сеть оператора.

В этом разделе

Этапы обнаружения атак СОПТА (см. раздел 3.1.1)

Этапы фильтрации трафика в СОПТА (см. раздел 3.1.2)

3.1.1. Этапы обнаружения атак СОПТА

Обнаружение атак в СОПТА состоит из следующих этапов:

1. Сбор сетевого трафика. СОПТА собирает и анализирует сообщения следующих протоколов мобильных сетей: SCTP, M3UA, M2PA, MTP3, SCCP, TCAP, MAP, CAP, Diameter и GTP. Трафик для анализа может быть получен с сетевого интерфейса или в виде PCAP-файлов.
2. Проверка по белому списку. Полученные сообщения проверяются по белым спискам SS7 и Diameter, настроенным администраторами СОПТА. Если номер узла источника или назначения сообщения соответствует GT или хостам, занесенным в белый список, сообщение не рассматривается в качестве атаки и СОПТА не обрабатывает его на следующих этапах.
3. Нормализация. Информация извлекается из трафика и конвертируется в события с заданными наборами полей и их значений.
4. Корреляция. Нормализованные события проверяются по заданным шаблонам (сигнатурам). Если событие соответствует сигнатуре, модуль регистрирует атаку.
5. Отображение. Обнаруженные атаки отображаются в веб-интерфейсе в виде списков, карт и статистических графиков. Вы можете фильтровать (см. раздел 8) эти данные, а также настраивать отображение атак.

3.1.2. Этапы фильтрации трафика в СОПТА

Фильтрация трафика в СОПТА состоит из следующих этапов:

1. Сбор сетевого трафика. СОПТА получает от пограничного STP-узла сигнальный трафик и анализирует сообщения протоколов SCTP, SCCP, TCAP, MAP и CAP, прежде чем они достигнут сети оператора.
2. Проверка по контролю доступа. Модуль СОПТА проверяет полученные сообщения на соответствие правилам Firewall, настроенным администраторами СОПТА. Если сообщение соответствует критериям правила Firewall, применяется одно из действий: сообщение блокируется или разрешается. Если сообщение не соответствует критериям правила, то сообщение разрешается.
3. Доставка сообщений. Если сообщение разрешено, СОПТА отправляет его обратно пограничному STP-узлу. Если сообщение заблокировано, оно не достигает сети оператора.
4. Регистрация событий. Факт срабатывания правила Firewall регистрируется в базе данных в виде события Firewall. Если сообщение не подходит под правило, событие не регистрируется.
5. Отображение. Firewall отображаются в пользовательском интерфейсе на странице **events Firewall**. Вы можете фильтровать их (см. раздел 8) по времени, номеру источника и цели, типу сообщения, действию Firewall (разрешить или заблокировать), а также по наличию атаки, соответствующей такому сообщению.

3.2. Об атаках в СОПТА

В сетях сотовой связи атака — это сообщение или последовательность сообщений, отправленных злоумышленником с целью достижения определенного результата (раскрытия конфиденциальных данных, нелегального использования ресурсов сети, отказа в обслуживании узлов или абонентов).

СОПТА обнаруживает атаки с помощью сигнатур. Сигнатура — это правило, которое определяет признаки атаки в трафике: порядок, в котором получены сообщения, наличие или отсутствие ответа за указанный промежуток времени, типы сообщений и их атрибуты.

Если ваша учетная запись привязана к оператору, вы можете просматривать только те атаки, в которых этот оператор является адресом источника или цели.

Примечание. Время обнаружения атак и событий отображается в часовом поясе UTC+0.

В число атрибутов атаки входят:

— **Severity** — уровень опасности. Возможные значения атрибута:

  - High — успешная атака, представляющая угрозу (узел ответил на запрос злоумышленника);
  - Medium — частично успешная или неуспешная атака (узел ответил ошибкой на запрос злоумышленника);
  - Low — неуспешная атака (узел не ответил на запрос, злоумышленник не получил никакой дополнительной информации).

— **Potential impact** — возможные последствия.

  - Data leakage — перехват данных абонента (местоположения, текстового или голосового трафика) или раскрытие конфигурации сети;
  - Fraud — нелегальное использование ресурсов и сервисов сети, например перевод денег со счета абонента, переадресация вызовов, изменение профиля абонента;
  - Network element DoS — отказ в обслуживании элемента сети;
  - Subscriber DoS — отказ в обслуживании абонента.

  Примечание. Одна атака может иметь несколько возможных последствий. Пример: SendIMSI Aborted имеет три возможных последствия: Data leakage, Fraud, Subscriber DoS. Рекомендуется учитывать это при просмотре статистики на странице **Dashboards** и фильтрации атак по возможным последствиям.

— **Категория**:

  - MAP 1: Prohibited Interconnect Packets;
  - MAP 2.1: Packets from Unauthorized Network requiring an answer;
  - MAP 2.2: Packets from Unauthorized Network not requiring an answer;
  - MAP 3.1: Suspicious Location Packets;
  - MAP 3.2: Suspicious Registration Attempts;
  - MAP 3.3: Abnormal SMS Activity;
  - CAP 2: Abnormal CAP Activity related to inbound roaming;
  - CAP 3: Abnormal CAP Activity related to outbound roaming;
  - Diameter Low-Layer: Fundamental Filtering;
  - Diameter Category 1: Basic Filtering;
  - Diameter Category 2: Robust Filtering;
  - Diameter Category 3: Advanced Filtering;
  - GTP Category 1: Interface-Unauthorised Packet;

  - GTP Category 2: Home-Network Packet;
  - GTP Category 3: Plausible-Network Packet.

— **Source** — источник атаки. Источник атаки может отличаться от адреса источника сообщения. Например, если сообщение является ответом, источником атаки может быть получатель сообщения.

  Примечание. Вы можете использовать порты UDP в фильтрах в качестве атрибута источника или назначения для фильтрации атак GTP, однако указанное значение не отображается на странице **Dashboards** и в столбцах **Source address** и **Destination address** на странице **Attacks**. Вместо этого отображаются IP-адреса отфильтрованных атак.

— **Source operator** — оператор сотовой связи, которому принадлежит узел, являющийся источником атаки.

— **Source country** — страна узла, являющегося источником атаки.

— **Target** — идентификатор атакованного абонента или узла сети (например, MSC, SGSN, HLR или VLR).

— **Target operator** — оператор сотовой связи цели атаки.

— **Target country** — страна цели атаки.

— **Destination** — адрес, используемый для идентификации узла сети, который на момент атаки обслуживает цель. Значение атрибута может совпадать со значением **Target**, если целью атаки является узел сети.

При наличии модуля Traffic Screening (см. раздел 3.1.2) атаку можно предотвратить, если соответствующее входящее сообщение блокируется правилом Firewall, прежде чем оно достигнет вашей сети. Срабатывания правил Firewall регистрируются как события.

На странице **Attacks** заблокированные атаки обозначаются значком , разрешенные атаки обозначаются значком . Отсутствие этих значков означает, что сообщение не подходит под правило Firewall и применяется правило по умолчанию: сообщение разрешается, но событие Firewall не регистрируется.

4. Вход в СОПТА

Для получения адреса веб-интерфейса СОПТА, а также имени и пароля, необходимых для входа, обратитесь к администратору СОПТА.

- Чтобы войти в СОПТА, выполните следующие действия:

  1. В адресной строке браузера введите адрес веб-интерфейса СОПТА.

     Отобразится страница входа **Sign in** СОПТА.

  2. Если ваша учетная запись создана в СОПТА, выберите вкладку **Local**. Если ваша учетная запись создана на LDAP-сервере, выберите вкладку **LDAP**.
  3. Введите логин в поле **Login** и пароль в поле **Password**.
  4. Нажмите кнопку **Sign In**.

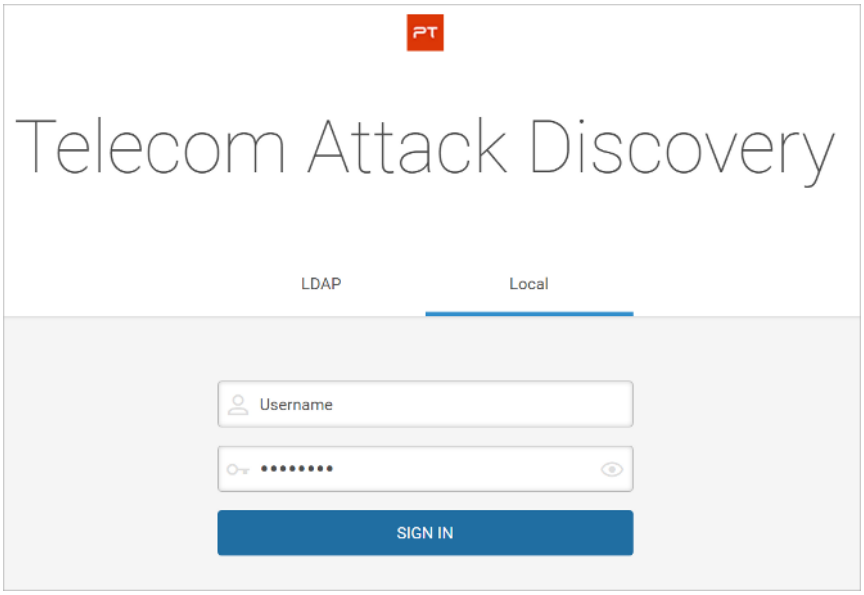


Рисунок 1. Вход в СОПТА

5. Пользовательский интерфейс СОПТА

Вы можете получить доступ ко всем функциям СОПТА с помощью веб-интерфейса СОПТА.

В данном разделе приведено описание пользовательского интерфейса СОПТА.

В этом разделе

Обзор интерфейса СОПТА (см. раздел 5.1)

Страница Dashboards (см. раздел 5.2)

Страница Attacks (см. раздел 5.3)

Страница Firewall events (см. раздел 5.4)

Временная шкала (см. раздел 5.5)

5.1. Обзор интерфейса СОПТА

Результаты анализа трафика отображаются на следующих страницах интерфейса СОПТА:

- **Dashboards**, которая отображает статистику атак в виде карт и графиков, а также позволяет вам создать статистический отчет;
- **Attacks**, которая отображает список атак и позволяет просматривать подробную информацию об атаках.
- **Firewall events**, которая отображает Firewall-события, то есть факты срабатывания правил Firewall.

  Примечание. Время обнаружения атак и событий отображается в часовом поясе UTC+0.

Панель инструментов, панель фильтрации и временная шкала (см. раздел 5.5) являются общими для всех основных страниц интерфейса.

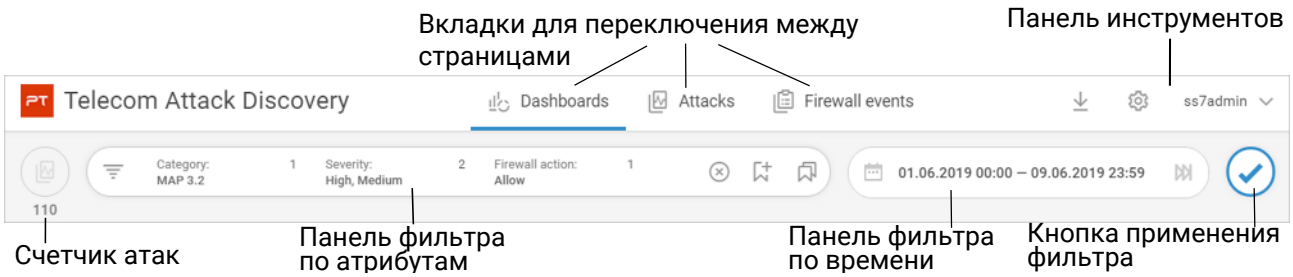


Рисунок 2. Общие элементы интерфейса

Два счетчика показывают количество данных в соответствии с примененным фильтром:

- Счетчик атак на страницах **Dashboards** и **Attacks** отображает количество атак. На странице **Attacks** количество атак на счетчике может отличаться от количества атак в списках атак: счетчик показывает общее количество атак, в то время как на странице **Attacks** может отображаться до 1000 атак (20 страниц по 50 атак).
- Счетчик событий Firewall на странице событий **Firewall events** отображает количество событий Firewall events. Это число может отличаться от количества Firewall events, отображаемого в списках на странице **Firewall events**: счетчик отображает общее количество событий Firewall events, в то время как количество данных на странице **Firewall events** ограничено до 1000 событий (20 страниц по 50 событий).

Панель инструментов содержит следующие элементы управления:

— отображает файлы JSON (см. раздел 6.2) или статистические отчеты (см. раздел 10), доступные для скачивания.

- **<Логин>** — позволяет настраивать правила отчетов и уведомлений, группы адресов, менять настройки профиля и выходить из продукта.

Панель фильтрации отображает выбранный фильтр и содержит следующие элементы управления:

— показывает скрытые критерии фильтра. Панель фильтров отображает до четырех критериев фильтрации. С помощью этой кнопки вы можете просмотреть остальные критерии фильтрации, если их больше трех.

— очистка панели фильтра. Доступно, если выбран хотя бы один критерий фильтра.

— открывает окно **Saved filters**.

Фильтр по времени показывает период, за который отображены атаки, и позволяет фильтровать данные по времени (см. раздел 8.1). Фильтр содержит следующие элементы управления:

— открывает Calendar (см. раздел 8.1.1).

Кнопка временной шкалы используется для того, чтобы развернуть и свернуть временную шкалу (см. раздел 5.5).

Кнопка применения фильтра используется для применения любых изменений, которые вы сделали на панели фильтров, в Calendar или Timeline: выберите фильтр по атрибуту и/или по времени, создайте, измените или удалите фильтр.

После применения фильтра кнопка применения фильтра заменяется кнопкой обновления фильтра . Кнопка обновления фильтра используется для того, чтобы снова применить те же критерии фильтрации и дополнить страницу новыми данными, которые подходят под эти критерии.

Кроме того, страницы **Dashboards** и **Attacks** содержат кнопки и , используемые для быстрого создания отчета по расписанию (см. раздел 11) и правил уведомлений (см. раздел 12).

5.2. Страница Dashboards

Страница **Dashboards** отображается при входе в СОПТА.

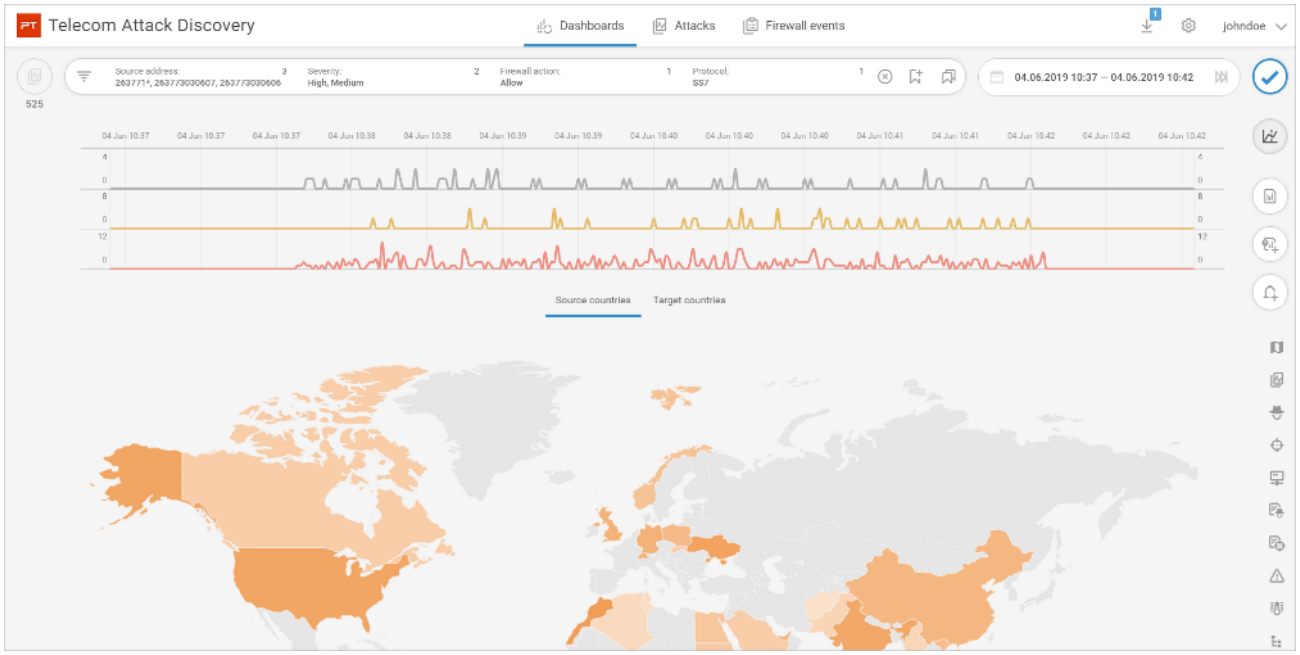


Рисунок 3. Страница **Dashboards**

Страница **Dashboards** отображает статистику атак в следующих формах:

— На географических картах, на которых показано, из каких стран исходят атаки (вкладка **Source countries**) и в каких странах находятся атакованные абоненты и узлы сети (вкладка **Target countries**).

  Принадлежность абонента и узла к стране определяется на основе списка операторов. Более темные оттенки указывают на большее количество обнаруженных атак. Вы можете навести курсор мыши на страну, чтобы отобразить точное количество атак в этой стране или из этой страны.

— В виде гистограмм, показывающих распределение атак по наиболее частым типам атак, источникам, целям и операторам.

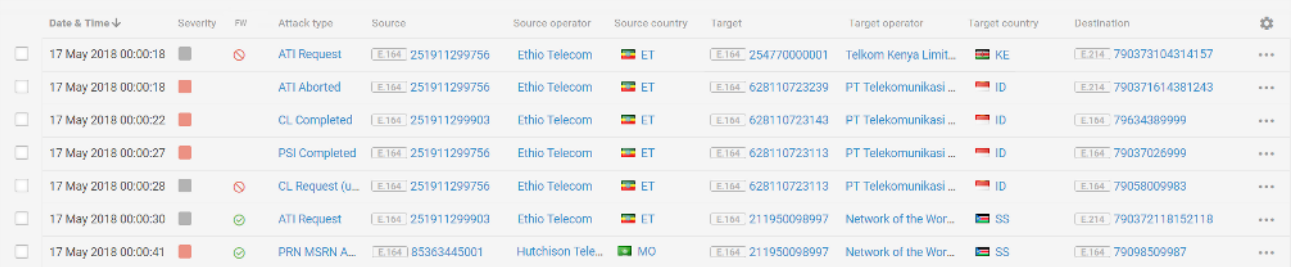
  Вы можете изменить количество данных на гистограмме, нажав кнопку **Show top 10**, **20**, **30**, **40** или **50**.

— В виде кольцевых диаграмм, показывающих распределение атак по возможным последствиям, уровням опасности и категориям.

  Примечание. Общее количество атак на диаграмме **Potential impacts** может отличаться от количества атак, отображаемых счетчиком атак , поскольку одна атака может иметь несколько потенциальных воздействий.

5.3. Страница Attacks

Страница **Attacks** отображает список атак.



Date & Time	Severity	FW	Attack type	Source	Source operator	Source country	Target	Target operator	Target country	Destination
17 May 2018 00:00:18			ATI Request	E.164 251911299756	Ethio Telecom	ET	E.164 254770000001	Telkom Kenya Limit...	KE	E.214 790373104314157
17 May 2018 00:00:18			ATI Aborted	E.164 251911299756	Ethio Telecom	ET	E.164 628110723239	PT Telekomunikasi ...	ID	E.214 790371614381243
17 May 2018 00:00:22			CL Completed	E.164 251911299903	Ethio Telecom	ET	E.164 628110723143	PT Telekomunikasi ...	ID	E.164 79634389999
17 May 2018 00:00:27			PSI Completed	E.164 251911299756	Ethio Telecom	ET	E.164 628110723113	PT Telekomunikasi ...	ID	E.164 79037026999
17 May 2018 00:00:28			CL Request (u...	E.164 251911299756	Ethio Telecom	ET	E.164 628110723113	PT Telekomunikasi ...	ID	E.164 79058009983
17 May 2018 00:00:30			ATI Request	E.164 251911299903	Ethio Telecom	ET	E.164 211950098997	Network of the Wor...	SS	E.214 790372118152118
17 May 2018 00:00:41			PRN MSRN A...	E.164 85363445001	Hutchison Tele...	MO	E.164 211950098997	Network of the Wor...	SS	E.164 79098509987

Рисунок 4. Списки атак

По умолчанию список атак на странице **Attacks** настроен следующим образом:

— Отображаются атаки, обнаруженные за последние 24 часа. Для изменения этого интервала вы можете фильтровать атаки по времени (см. раздел 8.1).

— Атаки сортируются по дате и времени по убыванию, и отображаются следующие атрибуты: **Date & time**, **Severity**, **FW**, **Category**, **Attack type**, **Source**, **Source operator**, **Source country**, **Target**, **Target operator**, **Target country**, **Destination**. Чтобы изменить набор отображаемых атрибутов, вы можете настроить отображение атак.

Для просмотра детальной информации об атаке вы можете развернуть карточку атаки (см. раздел 6.1).

5.4. Страница Firewall events

СОПТА может блокировать или явно разрешать входящие запросы, используя свои модули Firewall:

— SS7 Firewall используется для обработки запросов MAP и CAP.

— Diameter Firewall используется для обработки запросов Diameter.

Администраторы СОПТА настраивают правила Firewall, где они задают параметры запросов, которые должны быть заблокированы или разрешены (условие правила).

Если входящий запрос соответствует условию правила Firewall, запрос блокируется или разрешается. Для каждого срабатывания правила также может быть зарегистрировано событие Firewall. Если запрос не соответствует правилу Firewall, он разрешен по умолчанию.

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

Зарегистрированные события Firewall отображаются на странице **Firewall events**. Список содержит основную информацию о заблокированных или разрешенных запросах (адреса источника и назначения, протокол, тип сообщения) и следующие атрибуты:

- **Action** содержит **Block**, если запрос был заблокирован, или **Allow**, если он был разрешен.
- **Attacks** содержит , если событие связано с атакой (только для событий SS7 Firewall).
- **Firewall rule** содержит описание правила Firewall, которое было применено к запросу (только для событий Diameter Firewall). Вы можете щелкнуть описание правила, чтобы просмотреть параметры правила, включая условие, которое было выполнено в запросе, или просмотреть правила группы Firewall. (см. раздел 7).

Вы можете нажать , чтобы отобразить сведения о событии:

- В случае событий SS7 Firewall будет отображаться информация об атаках, связанных с этим событием. Вы можете открыть карту атаки, нажав .
- Для событий Diameter Firewall здесь будет показана более подробная информация о запросе, который был заблокирован или разрешен.

5.5. Временная шкала

СОПТА позволяет просматривать данные в виде временной шкалы: временной шкалы атак на страницах **Dashboards** и **Attacks** и временной шкалы событий Firewall на странице **events Firewall**.

Временная шкала на страницах **Dashboards** и **Attacks** отображает количество атак в виде трех графиков: серый — атаки низкого уровня опасности, желтый — атаки среднего уровня опасности, красный — атаки высокого уровня опасности. По наведению курсора мыши на график отображается точное количество атак за момент времени.

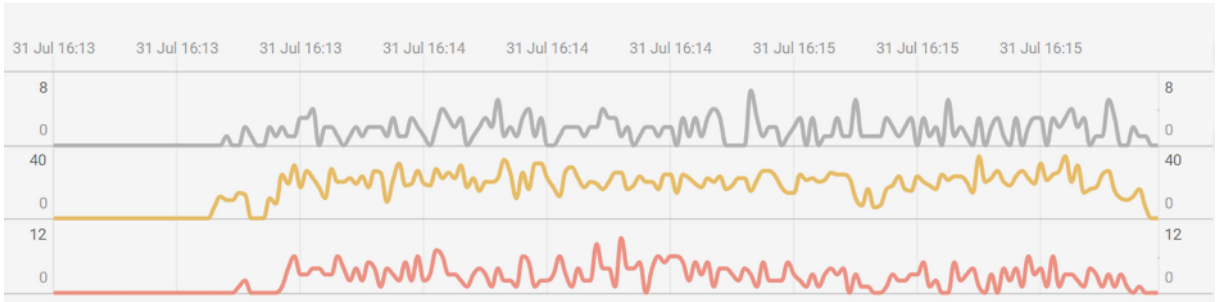


Рисунок 5. Временная шкала на страницах **Dashboards** и **Attacks**

Временная шкала на странице **Firewall events** отображает события Firewall в виде двух графиков: зеленый — события, соответствующие разрешающим правилам (Allow), красный — события, соответствующие запрещающим правилам (Block). По наведению курсора мыши на график отображается точное количество событий Firewall за момент времени.

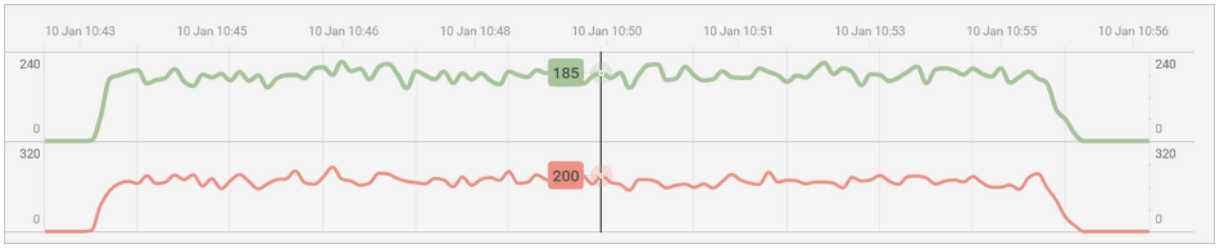


Рисунок 6. Временная шкала **Firewall**

Примечание. Время обнаружения атак и событий отображается в часовом поясе UTC+0.

Чтобы показать или скрыть временную шкалу, можно нажать .

Временная шкала позволяет фильтровать данные по времени (см. раздел 8.1). При фильтрации данных по времени масштаб горизонтальной оси меняется в соответствии с выбранным периодом (чем дольше выбранный период, тем длиннее промежутки времени между делениями), а масштаб вертикальной оси меняется в соответствии с объемом данных за выбранный период.

Секунды не отображаются на временной шкале и в панели фильтрации по времени, но учитываются при фильтрации данных по времени с использованием временной шкалы. Фильтрация атак и событий Firewall основывается на их временной метке (дне, часе, минуте и секунде). Если с помощью календаря (см. раздел 8.1.1) вы выбираете период в одну минуту (например, 10.08.2017 05:37 — 10.08.2017 05:37), то в рамках этой минуты вы не сможете выбрать более короткий период с помощью временной шкалы.

6. Просмотр подробной информации об атаках

Списки атак на странице **Attacks** отображают общую информацию об атаках.

Для просмотра подробной информации об атаке вы можете использовать следующие инструменты:

- открыть карточку атаки в браузере;
- скачать JSON-файл, содержащий набор атрибутов и их значений для одной или нескольких атак.

В этом разделе содержатся инструкции для просмотра подробной информации об атаках.

В этом разделе

Просмотр карточки атаки (см. раздел 6.1)

Выгрузка JSON-файла (см. раздел 6.2)

6.1. Просмотр карточки атаки

Вы можете просматривать все атрибуты атаки в карточке атаки.

► Чтобы открыть карточку атаки, сделайте следующее:

1. Откройте страницу **Attacks**.
2. Нажмите ⌄.

   Откроется карточка атаки. Она содержит все атрибуты атаки и сообщения, которые составили атаку.

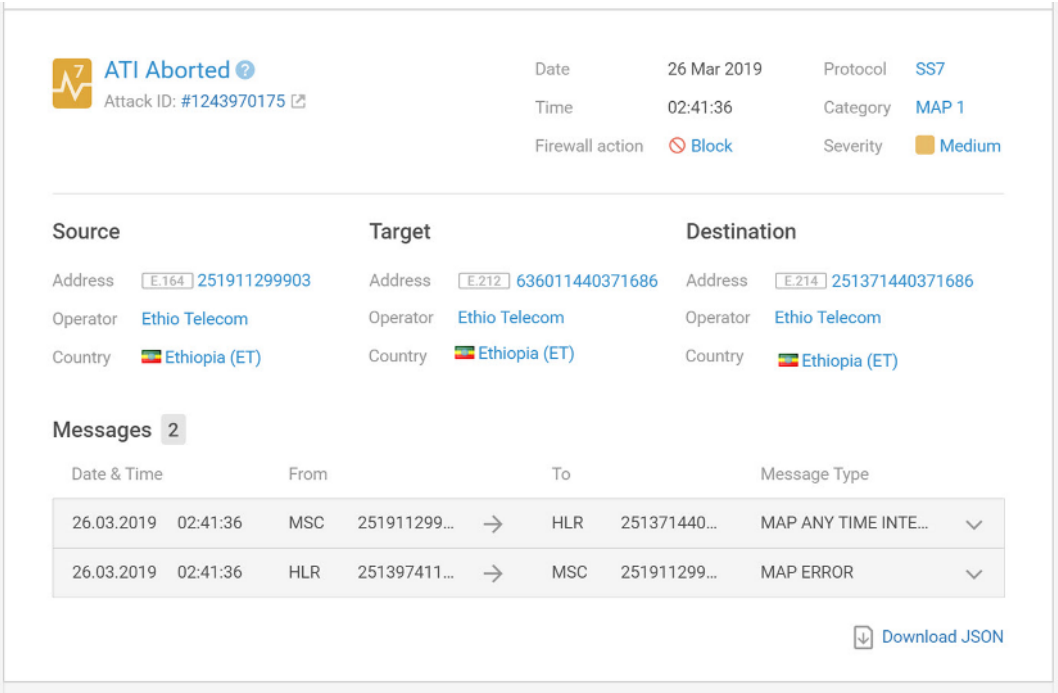


Рисунок 7. Просмотр карточки атаки

Чтобы просмотреть описание типа атаки, можно навести курсор на ? рядом с именем типа атаки.

Примечание. Если вы хотите оставить карточку атаки открытой для просмотра, вы можете открыть ее в отдельной вкладке браузера, нажав на идентификатор атаки в левом верхнем углу карточки атаки.

6.2. Выгрузка JSON-файла

СОПТА позволяет выгружать подробную информацию об одной или нескольких атаках в виде JSON-файла.

► Чтобы скачать JSON-файл:

1. Откройте страницу **Attacks**.
2. Установите флажки слева от атак.

   Начнется создание JSON-файла. Если отчет успешно создан, в верхней части страницы будет отображено сообщение **File generation completed**. В противном случае будет отображено сообщение об ошибке.

3. 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**.

4. Нажмите ссылку с именем созданного файла.

Начнется выгрузка файла.

7. Просмотр снимков правил 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. Каждая группа Firewall имеет свой собственный набор правил Firewall.

Если правило создается, редактируется или удаляется администратором СОПТА, то СОПТА создает моментальный снимок правила и группы Firewall, к которой присоединено правило. При открытии правила из события Firewall параметры правила отображаются в том виде, в котором они были при применении правила. При открытии группы Firewall, к которой присоединено правило из события Firewall, все правила отображаются в том виде, в котором они были при применении правила.

Например, вы можете просмотреть правила Firewall и снимки групп Firewall, чтобы проанализировать причину применения определенного правила: запрос не соответствует условиям других правил или правило имеет более высокий приоритет.

- Чтобы просмотреть снимок правила Firewall, выполните следующие действия:

  1. На странице **Firewall events** найдите событие Firewall с необходимым правилом, а в столбце **Firewall rule** щелкните описание правила.
  2. В появившемся диалоговом окне щелкните **Firewall rule details**.

     Откроется боковая панель, содержащая параметры правила, какими они были при применении правила, включая условие, которое было выполнено в запросе.
  3. Если вы хотите просмотреть соответствующий снимок группы Firewall, нажмите **Go to Firewall group rules**.

     Это отображает группу Firewall, какой она была при применении правила. Текущую версию правил группы Firewall вы можете просмотреть, нажав **Show current version**.

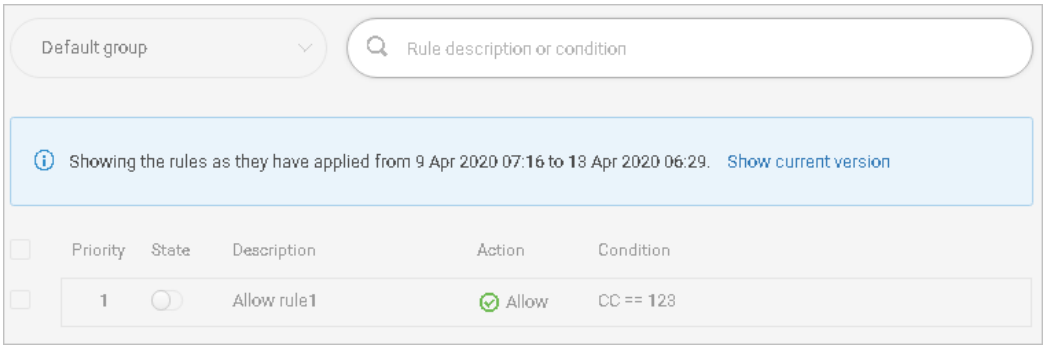


Рисунок 8. Просмотр снимка группы Firewall

8. Использование фильтров

Вы можете отфильтровать следующие данные в пользовательском интерфейсе СОПТА :

— Статистика на странице **Dashboards**

— Атаки на странице **Attacks**

— События Firewall на странице **Firewall events**

По умолчанию данные отображаются за последние 24 часа.

Вы можете фильтровать данные по времени или атрибуту и комбинировать оба типа фильтра.

В этом разделе

Фильтрация данных по времени (см. раздел 8.1)

Фильтрация данных по атрибуту (см. раздел 8.2)

8.1. Фильтрация данных по времени

Вы можете фильтровать данные по времени, используя следующие инструменты:

— Calendar: полезен для фильтрации по дням, неделям и месяцам.

— Timeline: полезен для более точного поиска (по часам и минутам).

В этом разделе приведены инструкции по использованию обоих инструментов.

В этом разделе

Фильтрация данных с помощью календаря (см. раздел 8.1.1)

Фильтрация данных с помощью временной шкалы (см. раздел 8.1.2)

8.1.1. Фильтрация данных с помощью календаря

Используя календарь, можно фильтровать данные по дням, неделям и месяцам.

► Чтобы отфильтровать данные с помощью календаря, выполните следующие действия:

1. Нажмите .

   Откроется окно **Calendar**.

2. Выберите период, за который вы хотите просмотреть данные.

   • Выберите начальную и конечную даты.

   • Нажмите **Last 31 days**, **Last 7 days** или **Last 24 hours**, чтобы быстро выбрать соответствующие временные диапазоны.

- В поле в нижней части окна введите диапазон времени в формате ДД.ММ.ГГГГ ЧЧ:ММ — ДД.ММ.ГГГГ ЧЧ:ММ.

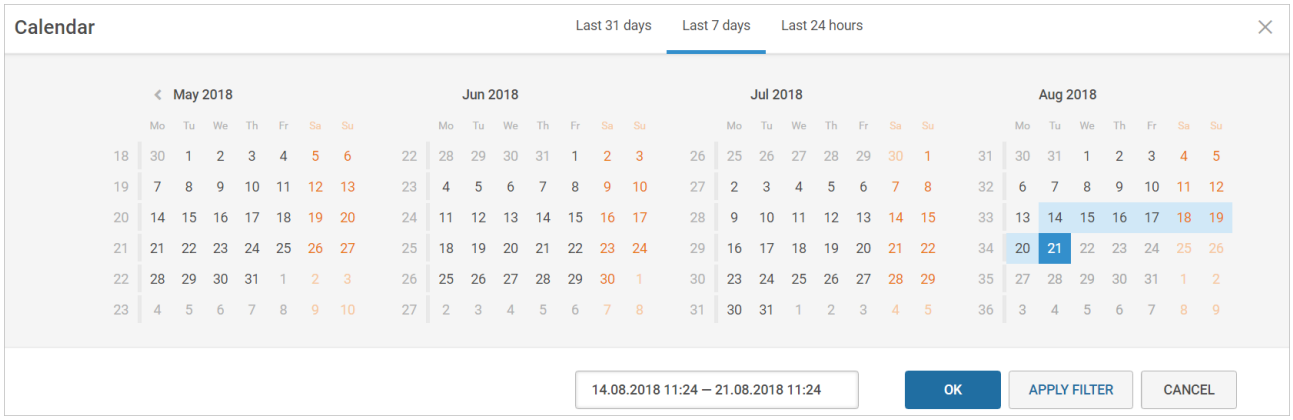


Рисунок 9. Фильтрация данных с помощью календаря

3. Нажмите кнопку **Apply filter**.

Страницы **Dashboards**, **Attacks** и **events Firewall** обновляются в соответствии с выбранным временным диапазоном, а кнопка применения фильтра заменена кнопкой обновления фильтра .

Линейные графики на временной шкале обновляются в соответствии с объемом данных, доступных для выбранного временного диапазона.

Примечание. Если вы также хотите фильтровать данные по атрибуту, вы можете нажать **OK** на последнем шаге и настроить фильтр по атрибуту (см. раздел 8.2).

► Чтобы быстро отфильтровать данные за прошедший час,

нажмите справа от панели временного диапазона.

Примечание. Нажатие применяет как фильтр по времени, так и фильтр по атрибуту. Если перед нажатием вы добавили некоторые атрибуты на панель фильтра, будет также применен фильтр по атрибуту.

8.1.2. Фильтрация данных с помощью временной шкалы

Используя временную шкалу, вы можете фильтровать данные по часам и минутам.

► Чтобы отфильтровать данные с помощью временной шкалы, сделайте следующее:

1. Чтобы расширить график, нажмите .
2. Выделите интервал на временной шкале, удерживая левую клавишу мыши.

   Выбранный временной диапазон отображается на панели временного диапазона.

   Примечание. Вы можете нажать , чтобы отменить выбор.

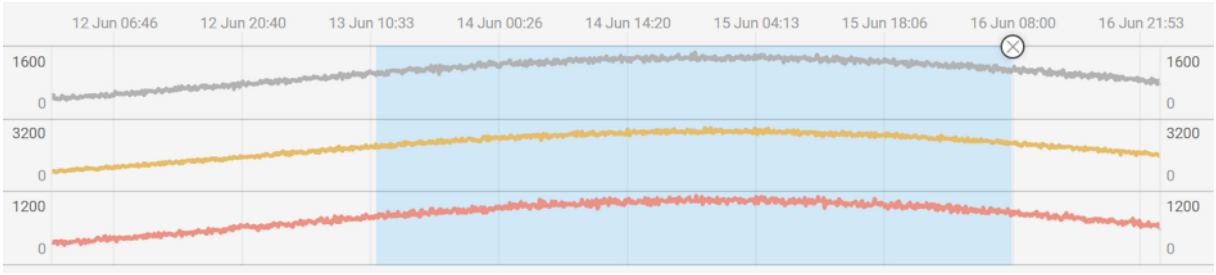


Рисунок 10. Выбор периода на временной шкале

3. Нажмите ✓.

Страницы **Dashboards**, **Attacks** и **events Firewall** обновляются в соответствии с выбранным временным диапазоном, а кнопка применения фильтра ✓ заменена кнопкой обновления фильтра ↻.

Фильтрация данных с использованием временной шкалы не перерисовывает линейные графики временной шкалы. Линейные графики временной шкалы перерисовываются только при использовании календаря (см. раздел 8.1.1) или фильтра по атрибутам.

См. также

Временная шкала (см. раздел 5.5)

8.2. Фильтрация данных по атрибуту

Вы можете фильтровать атаки, статистику на панелях мониторинга и события Firewall, используя атрибуты событий атаки и Firewall.

В этом разделе

Информация об атрибутах в фильтрах (см. раздел 8.2.1)

Настройка фильтров (см. раздел 8.2.2)

Использование быстрых фильтров (см. раздел 8.2.3)

Сохранение фильтров (см. раздел 8.2.4)

Применение сохраненных фильтров (см. раздел 8.2.5)

Переименование сохраненных фильтров (см. раздел 8.2.6)

Удаление сохраненных фильтров (см. раздел 8.2.7)

8.2.1. Информация об атрибутах в фильтрах

Фильтры состоят из атрибутов атаки и событий Firewall. Доступность и применимость некоторых из них имеют следующие особенности:

- Атрибуты, относящиеся к Firewall, доступны в том случае, если ваша лицензия включает функцию Firewall.
- Список атрибутов в окне **Configure filter** одинаков для всех страниц, но атрибуты применяются по-разному.
  - Атрибуты, относящиеся к адресам источника и назначения, а также атрибуты **Protocol** и **Firewall action** применяются ко всем данным (страницы **Dashboards**, **Attacks** и **Firewall events**).
  - Атрибуты, относящиеся к адресам назначения, операторам и странам, а также атрибуты **Protocol**, **Attack type**, **Attack severity**, **Attack category** и **Attack potential impact** применяются к данным только на страницах **Dashboards** и **Attacks**. Применение этих атрибутов на странице **Firewall events** не приведет к отображению данных.
  - Атрибуты **Firewall message type** и **Firewall attack link** применяются только к данным на странице **Firewall events**. Применение этих атрибутов на странице **Dashboards** или **Attacks** не отобразит никаких данных.
- Одна атака может иметь несколько возможных последствий. Когда вы исключаете возможное последствие из критериев фильтра, вы исключаете только атаки, которые имеют только это указанное возможное последствие и не имеют никаких других возможных последствий. Атаки, имеющие несколько последствий (включая добавленное в фильтр), будут отображаться.

См. также

Об атаках в СОПТА (см. раздел 3.2)

8.2.2. Настройка фильтров

Если вы хотите настроить критерии для фильтрации данных на страницах событий **Dashboards**, **Attacks** и **Firewall events**, вы можете настроить фильтр. Если у вас уже есть атаки или события межсетевого экрана с необходимыми значениями атрибутов, вы можете использовать быстрые фильтры (см. раздел 8.2.3) для быстрого добавления критериев фильтрации.

► Чтобы настроить фильтр, сделайте следующее:

1. На панели фильтров нажмите  .
2. В открывшемся окне **Configure filter** выберите атрибуты, которые вы хотите использовать для фильтрации атак, статистики и событий Firewall, и укажите их значения.

Примечание. Если вы хотите добавить несколько адресов одновременно, вы можете выбрать группы адресов (см. раздел 13) в разделах **Source address groups**, **Target address groups** и **Destination address groups**.

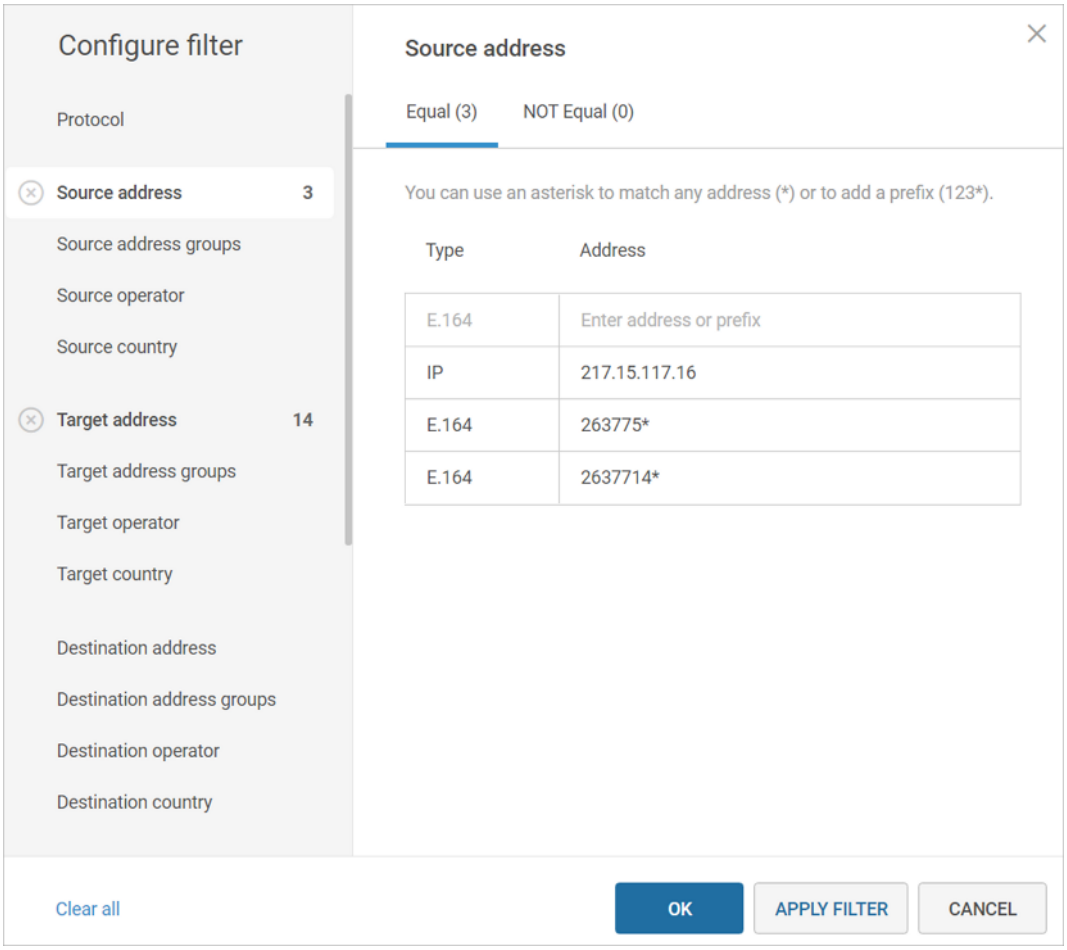


Рисунок 11. Использование адресных групп

3. Завершите настройку фильтра.
   - Если вы хотите применить настроенный фильтр, нажмите **Apply filter**.
   - Если вы также хотите фильтровать данные по времени, нажмите **OK** и выберите диапазон времени (см. раздел 8.1).

8.2.3. Использование быстрых фильтров

Используя быстрые фильтры, можно быстро создавать и изменять фильтры по атрибутам. Если значение атрибута отображается на странице **Dashboards**, **Attacks** или **events Firewall**, вы можете щелкнуть это значение, чтобы добавить его в фильтр или исключить из фильтра.

► Чтобы отфильтровать данные с помощью быстрых фильтров, сделайте следующее:

1. Выберите значение атрибута одним из следующих способов.

   • На странице **Dashboards** выберите страну, являющуюся источником или целью атаки, на карте или выберите значение на диаграмме.

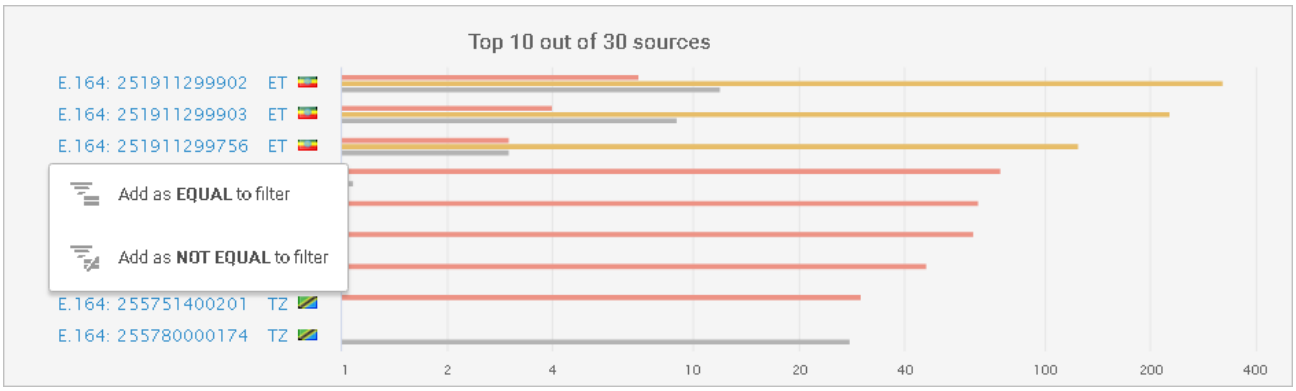


Рисунок 12. Фильтрация по наиболее частым источникам атак

   • На странице **Attacks** выберите значение атрибута атаки.

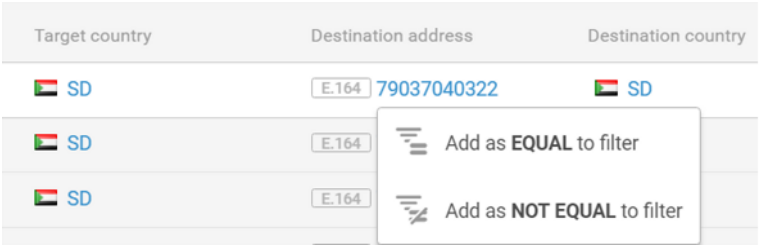


Рисунок 13. Фильтрация атак по месту назначения

   • На странице **events Firewall** щелкните отображаемое значение атрибута события Firewall.

Рисунок 14. Фильтрация событий Firewall по типу сообщений

2. В открывшемся контекстном меню выберите один из следующих вариантов.

   • **Add as EQUAL to filter**. Доступен, если значение не было добавлено в фильтр в качестве критерия **EQUAL**. Выберите, если вы хотите отобразить все данные, которые имеют выбранное значение.

- **Add as NOT EQUAL to filter**. Доступен, если значение не было добавлено в фильтр в качестве критерия **NOT EQUAL**. Выберите, если вы хотите отобразить все данные, которые не имеют выбранного значения.
- **Remove as EQUAL from filter**. Доступен, если выбранное значение добавлено в фильтр в качестве критерия **EQUAL**. Используется, чтобы убрать критерий из фильтра.
- **Remove as NOT EQUAL from filter**. Доступно, если выбранное значение добавлено в фильтр в качестве критерия **NOT EQUAL**. Используется, чтобы убрать критерий из фильтра.

3. Чтобы применить фильтр, нажмите .

Страницы **Dashboards**, **Attacks**, и **events Firewall** обновляются в соответствии с выбранным временным диапазоном, а кнопка применения фильтра заменена кнопкой обновления фильтра .

Примечание. Если вы хотите регулярно фильтровать данные, используя выбранные атрибуты и их значения, вы можете сохранить их (см. раздел 8.2.4).

8.2.4. Сохранение фильтров

Если вы хотите регулярно использовать набор атрибутов и их значений для фильтрации данных, их можно сохранить.

► Чтобы сохранить текущий фильтр в виде нового сохраненного фильтра, сделайте следующее:

1. Настройте фильтр (см. раздел 8.2.2) или используйте быстрые фильтры (см. раздел 8.2.3), чтобы добавить значения атрибутов на панель фильтров.
2. На панели фильтров нажмите .
3. В открывшемся окне **Saved filters** введите имя нового фильтра и нажмите клавишу ENTER.

Вы также можете заменить существующий сохраненный фильтр текущим фильтром.

► Чтобы заменить существующий сохраненный фильтр, сделайте следующее:

1. Настройте фильтр или используйте быстрые фильтры, чтобы добавить значения атрибутов на панель фильтров.
2. На панели фильтров нажмите .
3. В открывшемся окне **Saved filters** наведите курсор на фильтр, который вы хотите заменить, и нажмите (**Save and replace filter**).

8.2.5. Применение сохраненных фильтров

Для фильтрации данных с использованием предварительно настроенного набора атрибутов и их значений вы можете применить сохраненный фильтр.

- Чтобы применить сохраненный фильтр, сделайте следующее:

  1. На панели фильтров нажмите .
  2. В открывшемся окне **Saved filters** выберите сохраненный фильтр.

     Выбранный фильтр отображается на панели фильтров.
  3. Нажмите .

8.2.6. Переименование сохраненных фильтров

- Чтобы переименовать сохраненный фильтр, сделайте следующее:

  1. На панели фильтров нажмите .
  2. В открывшемся окне **Saved filters** наведите указатель мыши на сохраненный фильтр и нажмите .
  3. Введите новое имя для фильтра и нажмите клавишу ENTER.

8.2.7. Удаление сохраненных фильтров

- Чтобы удалить сохраненный фильтр, сделайте следующее:

  1. На панели фильтров нажмите .
  2. В открывшемся окне **Saved filters** наведите указатель мыши на сохраненный фильтр и нажмите .
  3. Нажмите для подтверждения удаления.

9. Настройка параметров отображения атак и событий Firewall

По умолчанию атаки на странице **Attacks** отсортированы по дате и времени по убыванию; отображаются следующие атрибуты атак: **Date & Time**, **Severity**, **FW**, **Category**, **Attack type**, **Source address**, **Source operator**, **Source country**, **Target address**, **Target operator**, **Target country**, **Destination**.

По умолчанию события Firewall на странице **Firewall events** отсортированы в порядке убывания по дате и времени; отображаются следующие атрибуты событий: **Date & Time**, **Action**, **Attacks**, **Source address**, **Message type**, **Protocol**, **Firewall rule**.

Вы можете изменить набор и порядок отображаемых атрибутов, сортировку и ширину столбца.

► Чтобы изменить набор и порядок отображаемых атрибутов, сделайте следующее:

1. Справа на странице **Attacks** или **Firewall events** нажмите ⚙.
2. В открывшемся окне **Display settings**:
   - Если вы хотите показать или скрыть атрибуты, установите или снимите флажки.
   - Если вы хотите изменить порядок, в котором отображаются атрибуты, перетащите их вверх или вниз.

     Примечание. Вы можете сбросить настройки дисплея до их состояния по умолчанию, нажав **Reset to default**.
3. Нажмите кнопку **Применить**.

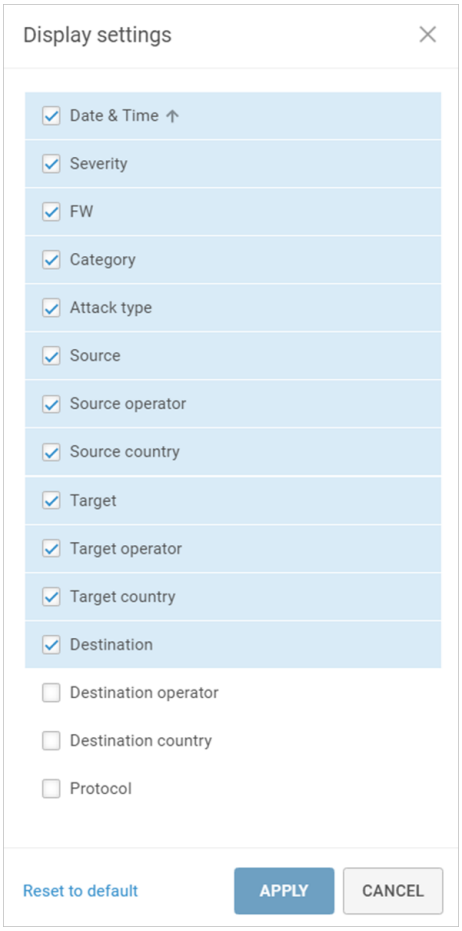


Рисунок 15. Настройка отображения атак

- Чтобы изменить сортировку атак или событий Firewall,

  щелкните заголовок столбца в списке атак или событий Firewall.

  Атрибут, используемый для сортировки, отмечен стрелкой в списке и в окне **Display settings**.

- Чтобы изменить ширину столбца,

  перетащите границу заголовка столбца.

См. также

Страница Attacks (см. раздел 5.3)

Страница Firewall events (см. раздел 5.4)

10. Выгрузка статистического отчета

Вы можете создавать и выгружать статистические отчеты в формате ODS.

Статистический отчет содержит данные со страницы **Dashboards**: статистику атак по уровням опасности, категориям, возможным последствиям, источникам, целям, операторам и странам. Отчет может содержать до 10 000 строк на листе.

► Чтобы выгрузить статистический отчет:

1. Откройте страницу **Dashboards**.
2. Если необходимо, отфильтруйте атаки (см. раздел 8), чтобы включить в отчет только нужные данные.
3. В правой части страницы нажмите .

   Начнется создание отчета. Если файл журнала успешно создан, в верхней части страницы появится сообщение **File generation completed**. В противном случае появится сообщение об ошибке.
4. 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**.
5. Нажмите ссылку с именем созданного файла.

   Начнется выгрузка отчета.

11. Работа с правилами отчетов по расписанию

В дополнение к выгрузке статистических отчетов (см. раздел 10) из веб-интерфейса СОПТА вы можете также настроить отправку таких отчетов СОПТА по расписанию, указанному в правиле отчета по расписанию. Отчет по расписанию может содержать до 10 000 строк на лист. Вы можете включать в отчет только определенные атаки (например, атаки указанного типа или из указанной страны) с помощью фильтра по атрибуту, созданного в правиле отчета по расписанию.

Количество отчетов, созданных с момента последнего изменения правила, отображается в столбце **Count**. Если СОПТА не удается отправить отчет (например, из-за недоступности почтового сервера), количество отправленных отчетов может быть меньше количества созданных отчетов.

В качестве часового пояса для расписания отчетов и времени их отправки используется UTC+0.

Сообщения с отчетами по расписанию имеют следующую тему:

```
[TAD][<Начальное время> — <Конечное время>][<Название правила отчета по расписанию>] Attacks report
```

В этом разделе

Создание правила отчета по расписанию (см. раздел 11.1)

Создание правила отчета по расписанию на основе существующего фильтра (см. раздел 11.2)

Изменение правила отчета по расписанию (см. раздел 11.3)

Удаление правила отчета по расписанию (см. раздел 11.4)

11.1. Создание правила отчета по расписанию

- Чтобы создать правило отчета по расписанию, выполните следующие действия:

  1. В панели инструментов выберите **<Ваш логин>** → **Report and notification rules**.
  2. Нажмите  .

     Откроется страница создания правила.

     Примечание. Вы также можете создать правило отчета по расписанию на основе существующего фильтра (см. раздел 11.2).
  3. Включите правило.

     Примечание. Вы также можете включить и выключить правило в столбце **State** на странице **Report and notification rules**.
  4. В поле **Имя** введите имя правила.

5. В блоке параметров **Generate reports** укажите частоту отправки отчетов. Частота отправки отчетов определяет период, за который данные включаются в отчеты.
6. Если вы хотите включать в отчеты только определенные атаки, нажмите кнопку **Set filter** и в открывшемся окне **Edit filter** укажите атрибуты атак и их значения.

   Примечание. Фильтры, созданные в рамках правил отчета по расписанию, не сохраняются в списке **Saved filters**.
7. В блоке параметров **Send reports to** укажите получателей отчетов. При установке флажка **Other emails** вы можете добавить до 10 адресов электронной почты внешних получателей.
8. Нажмите кнопку **Сохранить**.

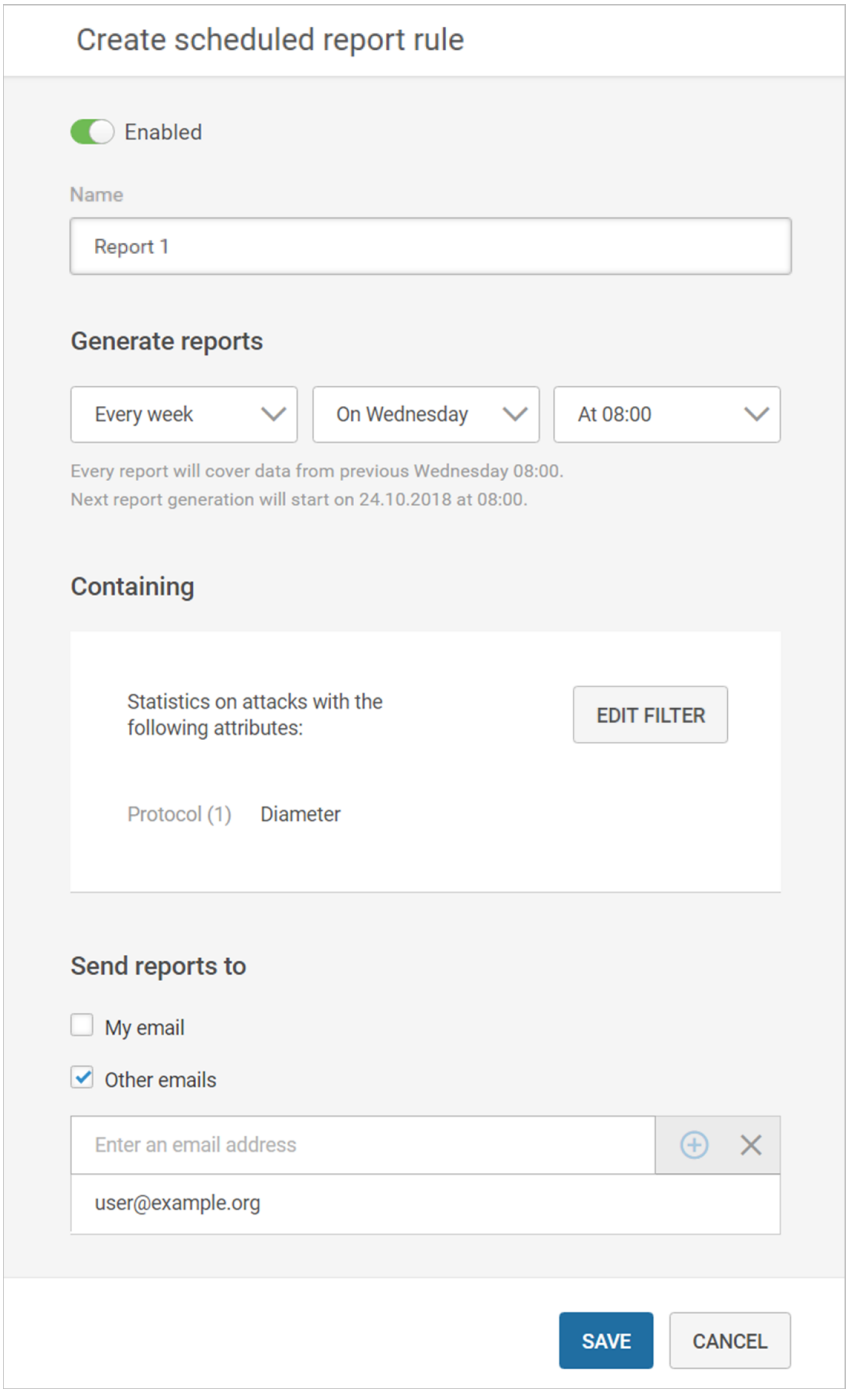


Рисунок 16. Создание правила отчета по расписанию

Правило отчета по расписанию создано.

Примечание. Если ваша учетная запись отключена, правила отчетов и правила уведомления, созданные вами, также автоматически отключаются.

11.2. Создание правила отчета по расписанию на основе существующего фильтра

Если у вас уже есть сохраненный фильтр, вы можете настроить отчеты по расписанию так, чтобы они содержали данные, соответствующие атрибутам, указанным в этом фильтре. Для этого необходимо создать правило отчета по расписанию на основе этого фильтра.

- Чтобы создать правило отчета по расписанию на основе существующего фильтра, сделайте следующее:

  1. Выберите фильтр и примените его.
  2. На странице **Dashboards** или **Attacks** нажмите  .

     Откроется форма создания правила. Блок фильтрации будет заполнен атрибутами атак из примененного фильтра.
  3. Завершите процедуру создания правила (см. раздел 11.1).

     Примечание. Изменения в фильтре правил не влияют на фильтр, используемый для создания правила.

11.3. Изменение правила отчета по расписанию

Вы можете изменить настройки правила отчета по расписанию. Любые изменения, вносимые в правило (кроме включения и отключения), сбрасывают счетчик **Report count since modification**.

- Чтобы изменить правило отчета по расписанию:

  1. Справа от правила наведите курсор на ••• и нажмите  .
  2. Измените настройки правила.
  3. Нажмите кнопку **Save**.

11.4. Удаление правила отчета по расписанию

- Чтобы удалить правило отчета по расписанию:

  1. В панели инструментов выберите **<Ваш логин>** → **Report and notification rules**.
  2. Наведите указатель мыши на правило и нажмите  .
  3. Нажмите  для подтверждения удаления.

12. Работа с правилами уведомления

СОПТА позволяет отправлять уведомления на ваш адрес электронной почты или на сервер syslog, когда количество зарегистрированных атак достигает указанного порога. Вы должны установить период (от 10 минут до 24 часов), в течение которого должны быть обнаружены такие атаки. Вы также можете создавать фильтры по атрибуту в правилах уведомления для отправки уведомлений только об определенных атаках (например, указанного типа или из указанной страны).

СОПТА проверяет количество зарегистрированных атак каждые 10 минут, и, если порог достигнут, СОПТА создает и отправляет уведомление. Количество уведомлений, созданных с момента последнего изменения правила, отображается в столбце **Count**. Если СОПТА не удается отправить уведомление (например, из-за недоступности почтового сервера), количество отправленных уведомлений может быть меньше количества созданных уведомлений.

В качестве часового пояса для времени отправки уведомлений используется UTC+0.

Уведомления по электронной почте

Если порог достигается несколько раз в течение 10 минут, уведомление по электронной почте будет включать данные по каждому периоду, в течение которого эти атаки были зарегистрированы.

Например, в 10:00 вы настраиваете отправку уведомлений при регистрации хотя бы пяти атак в течение часа. Если в 10:02 регистрируются 5 атак и еще 5 атак регистрируются в 10:10, вы получите одно уведомление по электронной почте с данными по периодам 10:00–10:02 и 10:02–10:10. Если в 10:02 регистрируются 5 атак и еще 5 атак регистрируются в 10:20, вы получите два уведомления по электронной почте по каждому периоду. Если в 10:02 регистрируются 4 атаки и еще 4 атаки регистрируются в 11:03, уведомления не будут отправлены.

Сообщения с уведомлениями имеют следующую тему:

```
[TAD][<Начальное время> — <Конечное время>][<Название правила уведомления>]
Notification
```

Уведомления в syslog

В отличие от уведомлений по электронной почте уведомления в syslog не группируются и отправляются каждый раз при достижении порога, не чаще одного раза в минуту.

Уведомления в syslog имеют следующий формат (часть `MSG`):

```
<Количество атак> attacks per <Период> using '<Название правила уведомления>'
from <Начальное время> till <Конечное время>
```

В этом разделе

Создание правила уведомления (см. раздел 12.1)

Создание правила уведомления на основе существующего фильтра (см. раздел 12.2)

Изменение правила уведомления (см. раздел 12.3)

Удаление правила уведомления (см. раздел 12.4)

12.1. Создание правила уведомления

► Чтобы создать правило уведомления, сделайте следующее:

1. В панели инструментов выберите **<Ваш логин>** → **Report and notification rules**.
2. Нажмите  .

   Откроется страница создания правила.

   Примечание. Вы также можете создать правило уведомления на основе существующего фильтра (см. раздел 12.2).
3. Включите правило.

   Примечание. Вы также можете включить и выключить правило в столбце **State** на странице **Report and notification rules**.
4. В поле **Имя** введите имя правила.
5. В блоке параметров **Issue a notification if** укажите условие уведомления: минимальное количество атак и период, в течение которого эти атаки должны быть зарегистрированы (от 10 минут до 24 часов).

   СОПТА проверяет выполнение этого условия каждые 10 минут. Если СОПТА регистрирует указанное количество атак в течение указанного периода, отправляется уведомление.

   Если в качестве условия уведомления указана 1 атака, выбор периода становится недоступным и уведомление отправляется каждый раз, когда СОПТА регистрирует атаку, не больше одного уведомления в 10 минут.
6. Если вы хотите получать уведомления только об определенных атаках, нажмите кнопку **Set filter** и в открывшемся окне **Edit filter** укажите атрибуты атак и их значения.

   Примечание. Фильтры, созданные в рамках правил уведомления, не сохраняются в списке **Saved filters**.
7. В блоке параметров **Notification delivery methods** укажите способ отправки уведомлений о зарегистрированных атаках.
8. Нажмите кнопку **Сохранить**.

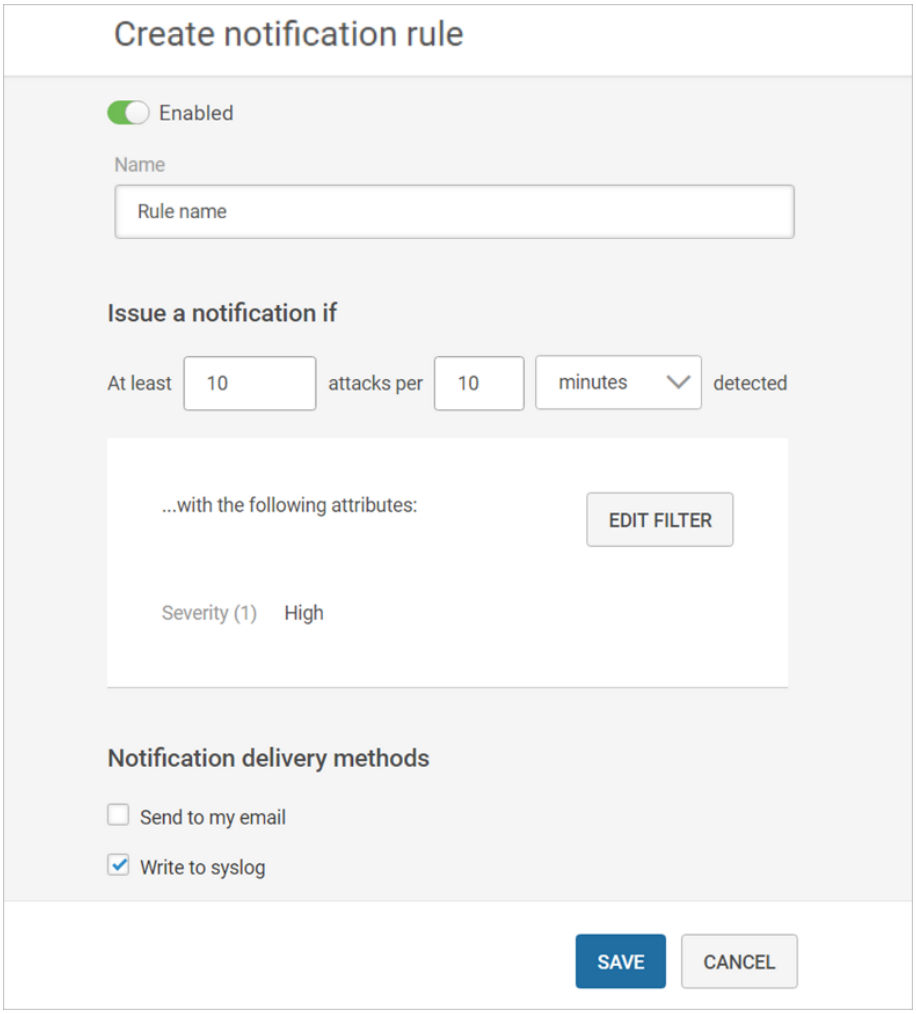


Рисунок 17. Создание правила уведомления

Правило уведомления создано.

Примечание. Если ваша учетная запись отключена, правила отчетов и правила уведомления, созданные вами, также автоматически отключаются.

12.2. Создание правила уведомления на основе существующего фильтра

Если у вас уже есть сохраненный фильтр, вы можете настроить уведомления так, чтобы они содержали данные, соответствующие атрибутам, указанным в этом фильтре. Для этого необходимо создать правило уведомления на основе этого фильтра.

- Чтобы создать правило уведомления на основе существующего фильтра, выполните следующие действия:

  1. Выберите фильтр и примените его.
  2. На странице **Dashboards** или **Attacks** нажмите .

     Откроется форма создания правила. Блок фильтрации будет заполнен атрибутами атак из примененного фильтра.
  3. Завершите процедуру создания правила (см. раздел 12.1).

     Примечание. Изменения в фильтре правил не влияют на фильтр, используемый для создания правила.

12.3. Изменение правила уведомления

Вы можете изменить настройки правила уведомления. Любые изменения, вносимые в правило (кроме включения и отключения), сбрасывают счетчик **Notification count since modification**.

- Чтобы изменить правило уведомления:

  1. Справа от правила наведите курсор на ••• и нажмите .
  2. Измените настройки правила.
  3. Нажмите кнопку **Save**.

12.4. Удаление правила уведомления

- Чтобы удалить правило уведомления:

  1. В панели инструментов выберите **<Ваш логин>** → **Report and notification rules**.
  2. Наведите указатель мыши на правило и нажмите .
  3. Нажмите для подтверждения удаления.

13. Управление группами адресов

Группы адресов — это создаваемые пользователями списки адресов. Вы можете использовать группы адресов для быстрого добавления нескольких адресов или масок в фильтр.

В этом разделе содержится информация о создании, изменении и удалении групп адресов.

В этом разделе

Создание пользовательского справочника (см. раздел 13.1)

Изменение группы адресов (см. раздел 13.2)

Удаление группы адресов (см. раздел 13.3)

13.1. Создание пользовательского справочника

- Чтобы создать группу адресов:

  1. На панели инструментов выберите **<ваш логин>** → **Address groups**.
  2. Нажмите .

     Откроется страница создания address group.
  3. В поле **Group name** введите уникальное название для идентификации группы адресов.
  4. Введите адреса, которые вы хотите добавить в группу.

     Примечание. Вы также можете выбрать **Unknown** в качестве типа адреса, чтобы добавить пустые адреса в качестве атрибутов Source, Target или Destination.
  5. Нажмите кнопку **Сохранить**.

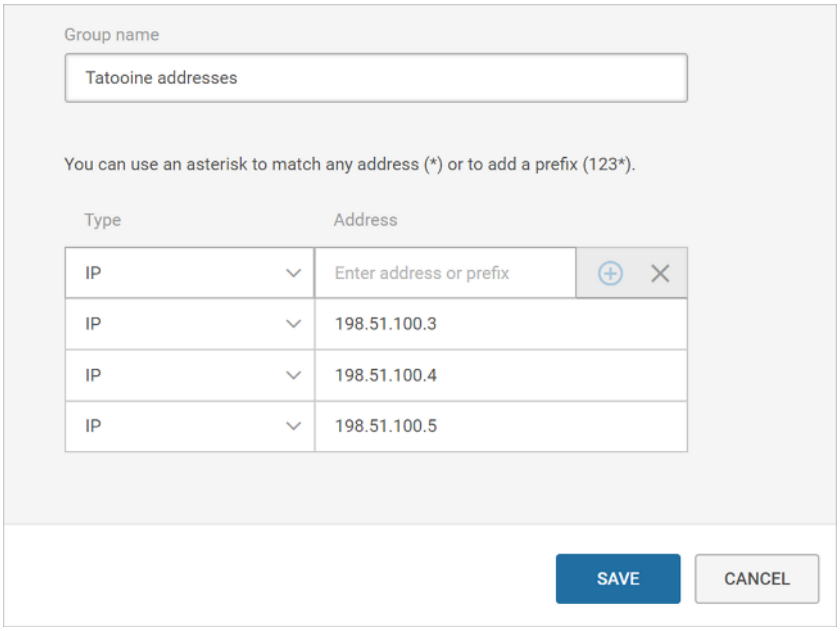


Рисунок 18. Создание группы адресов

13.2. Изменение группы адресов

- Чтобы изменить группу адресов:

  1. На панели инструментов выберите **<ваш логин>** → **Address groups**.
  2. Справа от группы адресов наведите курсор на ••• и нажмите ✎.

     Откроется страница **<Имя address group>**.
  3. Измените группу адресов
     - Если вы хотите изменить адрес, выберите его, введите новое значение и нажмите клавишу ENTER.
  4. Нажмите кнопку **Сохранить**.

13.3. Удаление группы адресов

- Чтобы удалить группу адресов:

  1. На панели инструментов выберите **<ваш логин>** → **Address groups**.
  2. Справа от группы адресов, которую вы хотите удалить, наведите курсор на ••• и нажмите 🗑.
  3. Нажмите 🗑 для подтверждения удаления.

Примечание. Если удаленная группа адресов являлась единственным критерием в фильтре, такой фильтр будет отображать все атаки. Это также влияет на правила отчетов по расписанию и правила уведомления, использующие этот фильтр.

14. Просмотр операторов

СОПТА определяет страны и операторы источников и целей атак на основе списка операторов. Список операторов доступен на странице **Operators**. Список операторов содержит следующую информацию:

- Список операторов сотовой связи и стран, к которым они относятся.
- Коды мобильных стран (MCC) и коды мобильных сетей (MNC) для идентификации стран и операторов по префиксам E.212 (для SS7) или по Real-Realm и Destination-Realm (для Diameter).
- Коды стран (CC) и национальные коды назначения (NDC) для идентификации стран и операторов по префиксам E.164 (для SS7).
- диапазоны IP-адресов для определения операторов GTP-атак.

Владельцы системы обозначены  . Если вы являетесь партнерским пользователем, а ваш оператор является владельцем системы, вы можете просматривать параметры SMS Home Routing этого оператора. Если вы являетесь собственным пользователем, вы можете просматривать параметры SMS Home Routing всех владельцев системы.

► Чтобы найти оператора, которому принадлежит префикс, выполните следующие действия:

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

   Откроется страница **Operators**.
3. В появившемся поле поиска введите префикс. Для поиска по нескольким префиксам используйте звездочку (*). Например, введите 722*, чтобы найти все префиксы, начинающиеся с 722.
4. Нажмите кнопку **Применить**.

Будут показаны все операторы, имеющие указанные префиксы.

Рисунок 19. Поиск операторов с помощью префикса E.212

Атрибут, используемый в настоящее время для поиска операторов, обозначен . На рисунке выше префикс E.212 используется для поиска операторов.

- Чтобы просмотреть список всех операторов, сделайте следующее:

  1. Нажмите на заголовок колонки, используемой для поиска.

     Откроется поле изменения атрибута.

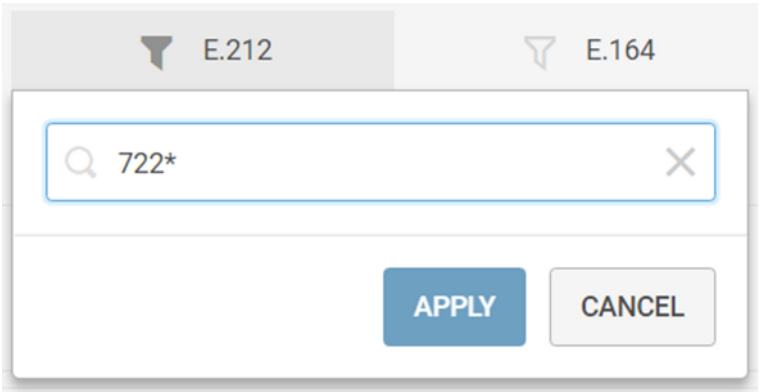


Рисунок 20. Изменение критериев поиска

  2. В текстовом поле удалите указанный префикс или нажмите .
  3. Нажмите кнопку **Применить**.

  Фильтр очищен, и отображен список всех операторов.

15. Настройка своей учетной записи

Страница **My profile** позволяет вам настраивать свою учетную запись.

Возможность изменить параметры учетной записи зависит от ее типа:

- Если вы вошли в СОПТА с помощью локальной учетной записи, созданной в СОПТА, вы можете изменить данные в полях **First name**, **Last name** и **Email**, а также **Password**. Значение **Role** может быть изменено администраторами продукта СОПТА только для собственных локальных пользователей.
- Если вы вошли в СОПТА с помощью учетной записи LDAP, ваш LDAP-сервер передает СОПТА ваши учетные данные при каждом входе в продукт. Учетные записи LDAP доступны только для собственных пользователей.

Партнерские пользователи связаны с оператором и могут иметь только роль оператора безопасности и только локальные учетные записи. Собственные пользователи не связаны с оператором и могут иметь роль оператора безопасности или администратора и локальные учетные записи или учетные записи LDAP.

В этом разделе

Изменение персональных данных (см. раздел 15.1)

Смена пароля (см. раздел 15.2)

15.1. Изменение персональных данных

Примечание. Вы можете изменять персональные данные (**First name**, **Last name** и **Email**), только если вы вошли в СОПТА с помощью локальной учетной записи, созданной в СОПТА.

► Чтобы изменить персональные данные, сделайте следующее:

1. В правом верхнем углу страницы **My profile** нажмите  .
2. Измените значения в следующих полях: **First name**, **Last name**, **Email**.
3. Нажмите кнопку **Сохранить**.

Персональные данные изменены.

15.2. Смена пароля

Примечание. Вы можете изменять свой пароль, только если вы вошли в СОПТА с помощью локальной учетной записи, созданной в СОПТА.

► Чтобы изменить пароль:

1. Нажмите кнопку **Change password**.

Откроется страница **Change password**.

2. В поле **Current password** введите текущий пароль.
3. В полях **New password** и **Confirm new password** введите новый пароль.
4. Нажмите кнопку **Change password**.

Ваш пароль изменен, и вы будете перенаправлены на страницу **My profile**.

16. 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

Техническая поддержка на портале (см. раздел 16.1)

Техническая поддержка по телефону (см. раздел 16.2)

Время работы службы технической поддержки (см. раздел 16.3)

Как служба технической поддержки работает с запросами (см. раздел 16.4)

16.1. 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.

16.2. 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.

16.3. 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.

16.4. 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 16.4.1)

Типы запросов (см. раздел 16.4.2)

Время реакции и приоритизация запросов (см. раздел 16.4.3)

Выполнение работ по запросу (см. раздел 16.4.4)

16.4.1. 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.

16.4.2. 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.

16.4.3. 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 2).

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 2. 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).

16.4.4. 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.

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