Positive Technologies Network Attack Discovery версия 12.2

Руководство оператора

Дата редакции документа: 19.03.2025

Содержание

1. Об этом документе

Руководство оператора содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies Network Attack Discovery (далее также — PT NAD) 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 PT NAD.

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

Комплект документации PT NAD включает в себя следующие документы:

- Этот документ.
- Руководство по проектированию — содержит информацию, необходимую для планирования развертывания продукта в сети организации в соответствии с топологией, имеющимися аппаратными ресурсами и задачами по выявлению угроз информационной безопасности.
- Руководство по установке на один сервер — содержит инструкции по установке PT NAD на один физический сервер или виртуальную машину, а также по обновлению продукта в такой конфигурации.
- Руководство по установке на несколько серверов — содержит инструкции по установке PT NAD на два или три физических сервера, а также по обновлению продукта в таких конфигурациях.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Справочное руководство по REST API — содержит информацию о доступных функциях сервиса REST API в PT NAD.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT NAD (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия

Пример	Описание
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 **OK**	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 PT NAD

Вы можете найти дополнительную информацию о PT NAD на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, 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 22).

2. О PT NAD

PT NAD — система глубокого анализа трафика для выявления аномальной сетевой активности и сложных целенаправленных атак на периметре и внутри сети организации.

Под атакой понимаются сетевое взаимодействие или группа взаимодействий, которые по специальным правилам определяются как целенаправленная угроза информационной безопасности.

PT NAD выполняет следующие функции:

- **Захват и хранение сетевого трафика.** Захват трафика с пропускной способностью 100 Мбит/с — 10 Гбит/с, его индексация и хранение[1] в виде исходной копии в формате PCAP.
- **Разбор захваченного трафика.** Анализ сообщений (см. раздел 2.1.3) сетевых протоколов (в частности, IPv4, IPv6, ICMP, TCP, UDP, HTTP, DNS, NTP, FTP, TFTP) для поиска и расследования инцидентов ИБ.
- **Извлечение и хранение файлов.** Извлечение и хранение[1] объектов, передаваемых по протоколам прикладного уровня (см. приложение В).
- **Визуализация данных.** Отображение статистики сетевых взаимодействий в виде отчетов (см. раздел 16.1) и графиков (см. раздел 11), а также наглядной карты сетевых взаимодействий (см. раздел 12).

PT NAD предоставляет следующие возможности:

- **Обнаружение угроз ИБ.** Использование эвристических и несигнатурных методов, а также поведенческого анализа для выявления сетевых аномалий, скрытого присутствия, активности вредоносного ПО.
- **Самозащита от сканирований, флуда и DDoS-атак.** Использование встроенного несигнатурного метода обнаружения нелегитимных сканирований, флуда и DDoS-атак для защиты PT NAD от переполнения базы данных и для повышения стабильности захвата трафика.
- **Поддержка открытого HTTP API.** Возможность разработки сторонних приложений для работы с проанализированным трафиком.
- **Отправка информации об угрозах ИБ в системы SIEM.** Передача сведений об обнаруженных угрозах ИБ в системы SIEM, в том числе в MaxPatrol 10, для инвентаризации активов и проверки результативности атак. Интеграция с MaxPatrol 10 осуществляется с помощью его API и специального агента, с другими системами SIEM — по протоколу системного журнала (syslog) или с помощью механизма webhook.

1 Хранение исходной копии трафика (см. раздел 7) и файлов не предусмотрено в версии PT NAD Sensor (см. раздел 2.5).

- **Интеграция с внешней аналитической системой.** Передача извлеченных из сетевого трафика файлов на проверку в Positive Technologies MultiScanner (PT MultiScanner) для выполнения антивирусного сканирования и репутационного анализа или в Positive Technologies Sandbox (PT Sandbox) для выполнения антивирусного сканирования, экспертной оценки и поведенческого анализа.
- **Передача экспертизы в продукт.** Использование разработанной в Positive Technologies базы знаний об атаках, нацеленных на удаленную эксплуатацию уязвимостей, и о безопасности IP-адресов, доменных имен, ссылок и файлов.
- **Ретроспективный анализ.** Повторный анализ захваченного трафика с использованием обновленной базы знаний для обнаружения новейших угроз ИБ в сетевой инфраструктуре организации. PT NAD не только регулярно запускает ретроспективный анализ, но и повторно разбирает скопированный трафик (см. раздел 9.10) для поиска инцидентов ИБ.
- **Импорт трафика для анализа.** Возможность анализировать трафик, полученный в виде PCAP-файлов из сторонних систем или программ.
- **Уведомления.** Оповещение операторов о результатах ретроспективного анализа (см. раздел 14.14) и о поступлении или непоступлении в информационную инфраструктуру организации определенного трафика. Уведомления могут быть получены на электронную почту или с помощью системного журнала, а также могут отображаться в интерфейсе PT NAD.
- **Обнаружение DGA-доменов.** Поиск DGA-доменов (см. раздел 2.3) при анализе доменных имен отправителя и получателя, а также при разрешении имен с помощью DNS. Поиск работает в реальном времени для захваченного трафика, а также выполняется в трафике, импортированном в формате PCAP.

В этом разделе

2.1. Алгоритм работы PT NAD

Работа PT NAD с трафиком организации делится на следующие этапы:

1. Захват трафика.
2. Обработка захваченного трафика.
3. Обогащение метаданных трафика.
4. Поиск опасных и потенциально опасных активностей в метаданных трафика.

В этом разделе

2.1.1. Захват трафика

Узлы в компьютерной сети обмениваются информацией. Поток этой информации называется трафиком.

PT NAD захватывает копию трафика при помощи модулей ptdpi подсистемы захвата.

См. также

Параметры фильтрации захвата трафика (см. раздел 20.1.6)

2.1.2. Обработка захваченного трафика. Сохранение исходной копии

Исходную копию захваченного трафика (см. раздел 2.1.1) PT NAD сохраняет в хранилище (см. раздел 7) в формате PCAP.

В дальнейшем сохраненную копию трафика можно использовать для ретроспективного анализа в PT NAD и импорта во внешние программы.

2.1.3. Обработка захваченного трафика. Разбор трафика

Параллельно с сохранением исходной копии трафика (см. раздел 2.1.2) PT NAD выполняет разбор трафика организации. Разбор трафика позволяет получать детальную информацию о сетевых взаимодействиях и обнаруживать атаки в сессиях (см. раздел 9). Каждая сессия соответствует сеансу обмена сетевыми пакетами между двумя узлами (клиентом и сервером) — устройствами в сети TCP/IP, которые отправляют и получают данные и имеют собственные IP-адреса.

В ходе разбора трафика PT NAD анализирует заголовки и содержимое сетевых пакетов (блоков данных, из которых состоит трафик):

1. Распознает в потоке трафика отдельные соединения и реконструирует сессии. В общем случае одна сессия соответствует одному соединению. Если PT NAD выявляет сканирование, флуд или DDoS-атаку, одна сессия содержит информацию обо всех соединениях такой активности.
2. Определяет, какие протоколы были задействованы в сессиях на уровнях модели OSI от канального до прикладного (см. приложение В).
3. Анализирует сообщения протоколов — от запросов на подключение до передаваемых по сети файлов, что позволяет операторам составить максимально полную картину происходящего в сети организации.
4. Обнаруживает атаки (см. раздел 10) в сессиях при помощи правил (см. раздел 2.2).

На этапе разбора трафика PT NAD получает такие данные, как:

— дата и время начала и окончания сессии;

— IP-адреса узлов, инициировавших передачу информации (отправителей);

— IP-адреса узлов, которым передавалась информация (получателей);

— порты отправителей и получателей;

— наименование транспортного протокола;

— наименование протокола прикладного уровня;

— детали взаимодействия узлов на прикладном уровне;

— количество переданных и полученных байтов и пакетов;

— название приложения, которое использовалось при передаче трафика;

— переданные файлы.

Результаты разбора трафика PT NAD сохраняет в виде метаданных в файлы формата JSON. Операторы могут использовать полученные файлы при расследовании инцидентов ИБ, а механизмы поиска и фильтрации обеспечивают навигацию в массивах сохраненных данных.

2.1.4. Обогащение метаданных трафика сессии

PT NAD добавляет к метаданным трафика сессии доменные имена и названия стран отправителей и получателей, а также обнаруженные в трафике сессии индикаторы компрометации.

К индикаторам компрометации относятся объекты или свойства объектов, которые указывают на подозрительную или вредоносную активность в информационной инфраструктуре организации. PT NAD может обнаруживать такую активность при помощи репутационных списков и механизма выявления DGA-доменов (см. раздел 2.3), а также получать информацию

о такой активности от других продуктов Positive Technologies. PT NAD ставит метки индикаторов компрометации на обнаруженные в атрибутах сессии доменные имена, IP-адреса и URL, а также файлы, извлеченные из трафика.

2.1.5. Поиск опасных и потенциально опасных активностей

PT NAD анализирует обогащенные метаданные трафика сессий в том числе для поиска потенциально опасных и опасных активностей (см. раздел 14). Активности выявляются при помощи правил для обнаружения активностей (см. раздел 2.2).

2.2. Правила в PT NAD

В PT NAD для определения атак и опасных и потенциально опасных активностей используются правила.

Правила для атак

Правило для атаки представляет собой элемент сигнатурного анализа сетевого трафика, содержащий совокупность признаков, по которым модуль ptdpi подсистемы захвата обнаруживает атаку или фазу ее проведения. Правило также определяет свойства атаки (название, класс и уровень опасности) и может содержать справочную информацию о ней, например описание эксплуатируемой уязвимости и рекомендации для оператора. Правила пишутся на специализированном языке (см. приложение Ж). Срабатывание правила приводит к созданию записи об атаке.

По способу создания правила для атак в PT NAD делятся на пользовательские правила, которые создаются операторами в интерфейсе продукта, и правила вендоров. Правила вендоров разрабатываются специализированными организациями (вендорами) и экспертами в области информационной безопасности и поставляются в PT NAD в виде пакетов. В работе с правилами вендоров существуют ограничения, например их нельзя удалить.

К правилам вендоров также относятся правила, поставляемые из базы знаний экспертного центра Positive Technologies, и правила Proofpoint ET Open и Proofpoint ET Pro (если их загрузка была настроена администратором PT NAD). Правила Positive Technologies (PTSecurity) и Proofpoint ET не нужно импортировать, так как они загружаются в PT NAD автоматически.

Правила для активностей

Правило для активности представляет собой элемент несигнатурного анализа трафика, содержащий алгоритм выявления опасной или потенциально опасной активности в сети организации по совокупности признаков в цепочке сессий с применением функции самообучения. Правило также определяет название и уровень опасности активности и может содержать такую справочную информацию о ней, как описание и рекомендации для операторов.

Набор правил для обнаружения активностей в PT NAD автоматически обновляется из базы знаний экспертного центра Positive Technologies. Как и в случае с правилами для атак, правила для активностей могут создаваться пользователями.

Пользовательские правила профилирования

Пользовательским правилом профилирования называется пользовательское правило для активности, для которого настроено обучение (см. раздел 20.3.10). Обучение позволяет не задавать статичный порог срабатывания правила, а определять его автоматически, используя технологию машинного обучения.

В процессе обучения PT NAD собирает данные об объекте мониторинга, анализирует значения заданного параметра и определяет порог срабатывания правила. При помощи обученного правила PT NAD отслеживает изменения и уведомляет об аномальных превышениях значений параметра. Объектами мониторинга могут быть узлы, клиенты, серверы, пары «клиент — сервер» либо весь трафик. Параметром для отслеживания может быть, например, объем входящего трафика.

Пользовательское правило профилирования содержит специальный алгоритм для выявления аномальной активности в сети организации, основанный на кластерном анализе данных. Например, если с помощью правила необходимо контролировать объем трафика, поступающий от внешних узлов, то в процессе обучения PT NAD объединяет узлы в кластеры по уровню активности и для каждого кластера определяет норму объема трафика. Порог срабатывания рассчитывается с учетом нормы для кластера и зависит от уровня чувствительности правила (низкий, средний или высокий), изменяя который можно увеличить значение порога в 2, 10 или 100 раз от верхней границы нормы. Обученное правило реагирует на превышение объема трафика по-разному для каждого узла в зависимости от кластера, к которому относится узел. Если узел не участвовал в обучении, он относится к кластеру с низкой активностью.

Автоматически установленный порог срабатывания правила можно обновить, перезапустив обучение. Это может понадобиться, например, если пользовательское правило профилирования сработало на активность, которая не является аномальной для сети организации. После перезапуска правило обучится на актуальных данных и больше не будет срабатывать на подобные активности. Доступен ручной и автоматический перезапуск обучения. По умолчанию включен автоматический перезапуск, при котором повторное обучение выполняется раз в сутки.

См. также

Синтаксис правил для обнаружения атак (см. приложение Ж)

Работа с правилами для обнаружения активностей (см. раздел 20.3)

Работа с правилами для обнаружения атак (см. раздел 20.2)

2.3. Обнаружение DGA-доменов

В PT NAD используется механизм обнаружения DGA-доменов в захваченном трафике среди доменных имен отправителя и получателя, а также при разрешении имен с помощью DNS. Поиск DGA-доменов также выполняется в трафике, импортированном в формате PCAP.

Domain generation algorithms (DGA) — алгоритмы для периодической генерации большого количества доменных имен. Домены, которые были сгенерированы при помощи DGA, называются DGA-доменами.

Один из сценариев использования DGA-доменов можно наблюдать при заражении компьютерной системы вредоносной программой. Вредоносная программа на скомпрометированном узле пытается подключиться к системам под управлением злоумышленника, чтобы получать команды или отправлять обратно собранную информацию.

Злоумышленники используют DGA для вычисления последовательности доменных имен, к которым пытаются подключиться зараженные узлы. Это делается для того, чтобы предотвратить потерю контроля над взломанной инфраструктурой в тех случаях, когда домены или IP-адреса злоумышленника, прописанные прямо в коде, блокируются системами безопасности.

См. также

Просмотр обнаруженных DGA-доменов в таблице сессий (см. раздел 9.8)

Просмотр обнаруженных DGA-доменов в таблице атак (см. раздел 10.7)

Составление списка исключений из DGA-доменов (см. раздел 20.6)

2.4. Единый интерфейс для управления экземплярами PT NAD

Экземпляры PT NAD, которые используются в организации, могут быть объединены в иерархию. В этом случае вы можете использовать центральную консоль в качестве единого интерфейса для работы с данными (см. раздел 8), полученными из подключенных дочерних систем.

Под центральной консолью понимается система, которая не захватывает сетевой трафик самостоятельно. В ней отображаются данные из подключенных дочерних систем.

В центральной консоли отсутствуют возможности, связанные с захватом, разбором, анализом трафика, а также с хранением его исходной копии. Например, в центральной консоли нет правил для атак и правил для активностей, справочников и репутационных списков, поэтому в ее интерфейсе отсутствуют одноименные разделы.

Дочерняя система представляет собой самостоятельный PT NAD, который работает в обычном режиме и подключен к центральной консоли.

2.5. PT NAD Sensor

Для интеграции с MaxPatrol 10 используется или полная, или упрощенная версия PT NAD. Последняя называется PT NAD Sensor. По сравнению с полной версией PT NAD Sensor позволяет снизить требования к аппаратным ресурсам за счет отключения или ограничения функций, не имеющих значения для работы в MaxPatrol 10:

— захваченный трафик не сохраняется на диск (нет хранилища файлов PCAP);

— полученные в ходе обработки трафика (см. раздел 2.1) метаданные трафика хранятся не больше одного дня;

— скорость захвата трафика ограничена 1 Гбит/с.

3. Что нового в версии 12.2

Ниже приводится список новых возможностей и улучшений, которые появились в PT NAD версии 12.2.

Иерархия экземпляров PT NAD

Если в организации используется несколько экземпляров PT NAD, то их можно объединить в иерархию, где один экземпляр будет родительским, а другие — дочерними. Это позволит использовать родительскую систему в качестве единого интерфейса для работы с данными (см. раздел 8) (активностями, сессиями, атаками, узлами), полученными из дочерних систем. Такой подход обеспечивает масштабирование PT NAD и может быть полезен для крупных территориально распределенных организаций.

Родительская система в иерархии называется центральной консолью (PT NAD Central Console). Центральная консоль не захватывает сетевой трафик самостоятельно, а получает данные из подключенных к ней дочерних систем. Каждая дочерняя система является экземпляром PT NAD с уникальной меткой. Связь между системами иерархии обеспечивает сервис единого входа PT MC.

В интерфейсе центральной консоли администраторы могут управлять иерархией — подключать к ней дочерние системы, а также отключать их от нее. Для этого в меню администрирования добавлен раздел **Дочерние системы**.

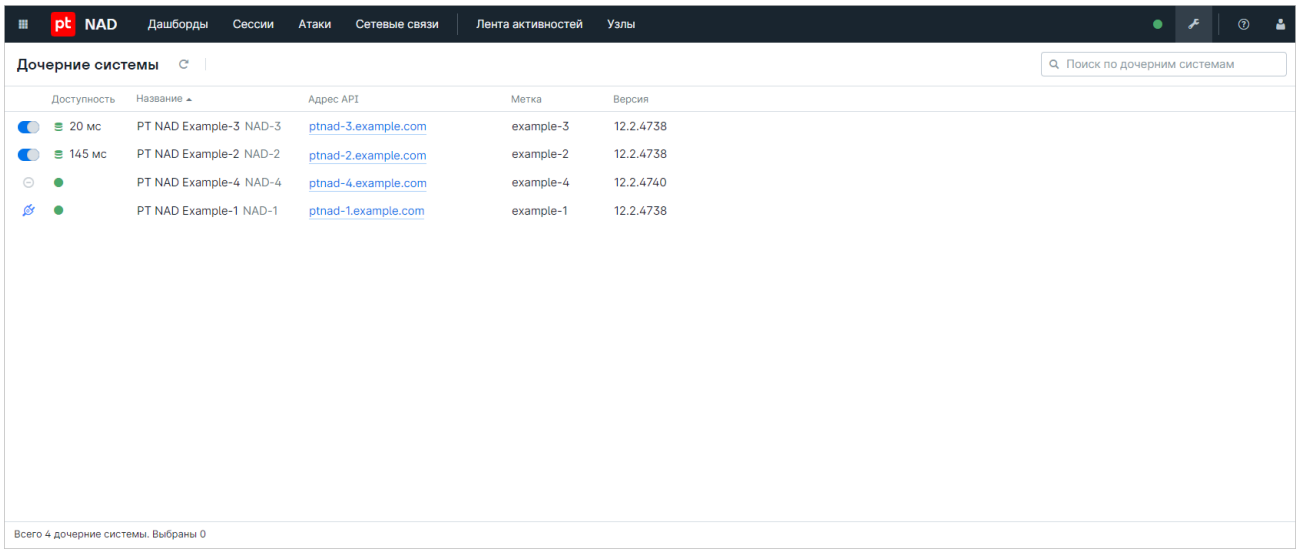


Рисунок 1. Управление иерархией в интерфейсе центральной консоли

На страницах **Дашборды**, **Сессии**, **Атаки**, **Сетевые связи**, **Лента активностей** и **Узлы** интерфейса центральной консоли можно выбрать дочерние системы, данные из которых требуется отображать.

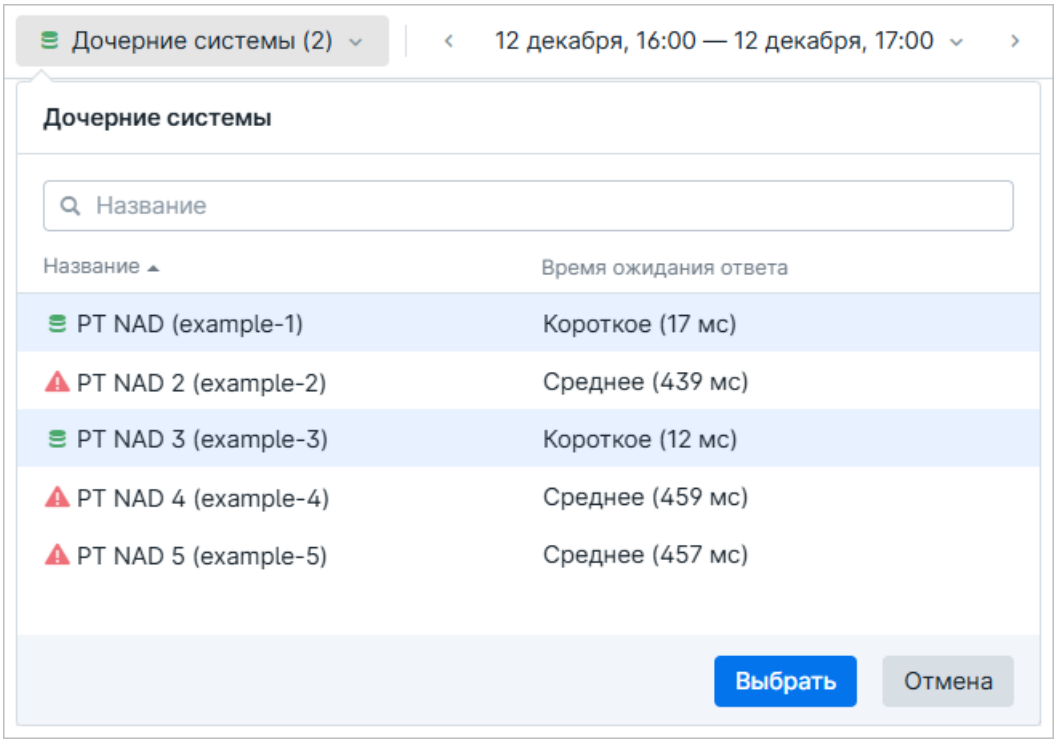


Рисунок 2. Выбор дочерних систем для отображения данных в центральной консоли

В таблицы сессий, атак и узлов центральной консоли добавлен столбец **Дочерняя система** с меткой дочернего PT NAD, а в ленте активностей метка отображается для каждой записи. Это позволяет различать системы, из которых получены данные.

Метка дочерней системы также отображается в названии карточек сессий, атак, узлов и активностей. Из этих карточек можно перейти в интерфейс дочерней системы по кнопке **Перейти в дочерний NAD**.

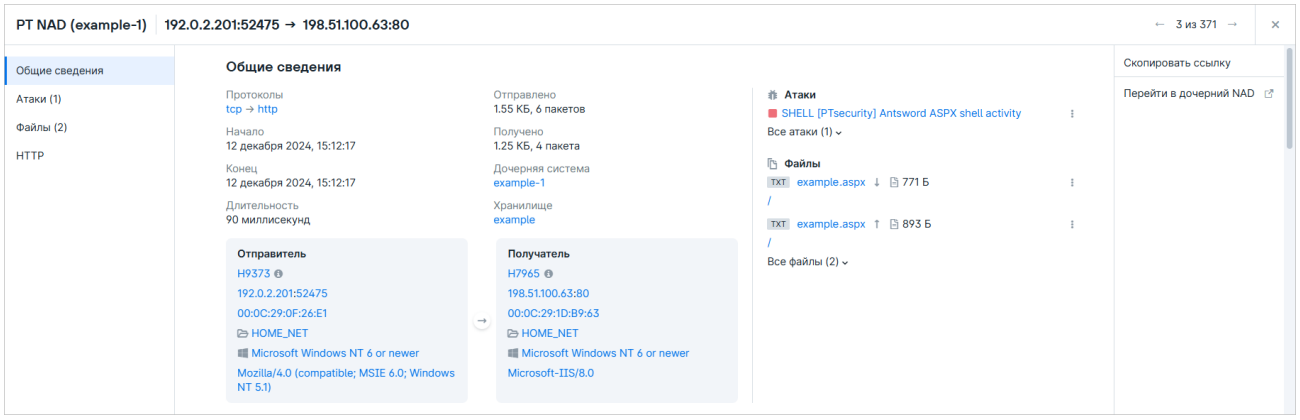


Рисунок 3. Просмотр карточки сессии в центральной консоли

Обнаружение использования WinRM

PT NAD обнаруживает опасные и потенциально опасные активности в информационной инфраструктуре организации. В версии 12.2 добавлено правило для выявления использования WinRM.

WinRM (Windows Remote Management) — это протокол для удаленного управления устройствами, работающими на базе операционной системы Windows. Запись об активности (см. раздел 14) сообщает, что протокол стал использоваться для управления сервером в инфраструктуре организации, с которым ранее не было WinRM-соединений. Это может свидетельствовать о попытках злоумышленников удаленно контролировать устройства в сети, например при помощи инструмента Evil-WinRM.

Обнаружение и разбор HTTP/2

Теперь PT NAD обнаруживает сообщения протокола HTTP/2. Поскольку трафик с использованием этого протокола всегда зашифрован, PT NAD может разбирать его, только если он будет предварительно расшифрован перед подачей в продукт, например пропущен через прокси-сервер TLS.

Ключевые слова в правилах для атак временно не применяются к сообщениям протокола HTTP/2. Это ограничение будет снято в следующей версии PT NAD.

Стороны соединения и репутационные списки

Начиная с версии 12.2 в репутационных списках IP-адресов и доменных имен отображается информация о стороне соединения (клиент, сервер или клиент и сервер), к которой применяется список. Для этого в таблицу репутационных списков (см. раздел 20.5) добавлен столбец **Применим к стороне соединения**.

По умолчанию пользовательские репутационные списки IP-адресов и доменных имен применяются к обеим сторонам соединения. Теперь, чтобы исключить ложные или неинтересные срабатывания, операторы могут выбрать только одну из этих сторон, указав ее в новом поле при создании или изменении списка. Выбранная сторона соединения не влияет на применение списка к транзакциям протоколов, поиск индикаторов компрометации в этом случае будет выполняться во всех транзакциях.

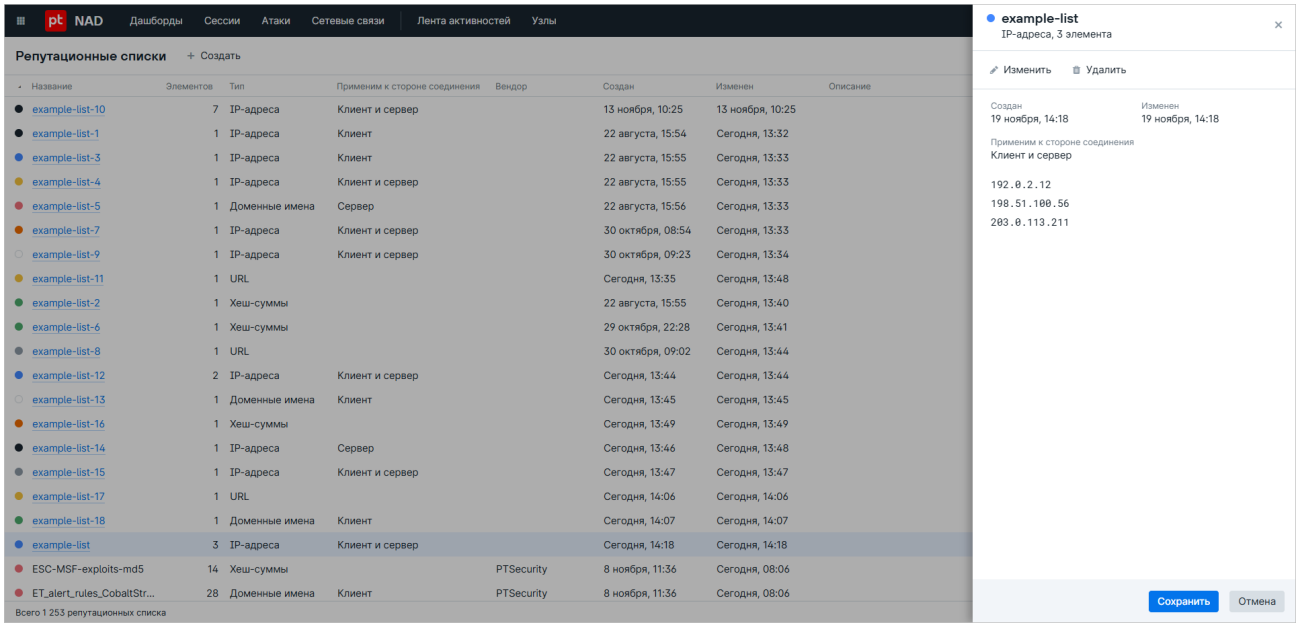


Рисунок 4. Просмотр карточки репутационного списка IP-адресов

Информация о смене прикладного протокола в сессии

Теперь, если в ходе сессии прикладной протокол сменился один или несколько раз, PT NAD отображает всю цепочку задействованных протоколов (см. приложение В). Такое может произойти из-за вкладывания сообщений одного протокола в сообщения другого, в частности из-за проксирования соединения или отправки электронной почты по шифрованному каналу (SMTP через TLS). В предыдущих версиях PT NAD отображался только основной прикладной протокол сессии, что могло затруднять анализ инцидентов ИБ и поиск сессий операторами.

Цепочка прикладных протоколов отображается в карточке сессии в блоке **Общие сведения** и в карточке атаки в блоке **Сессия**.

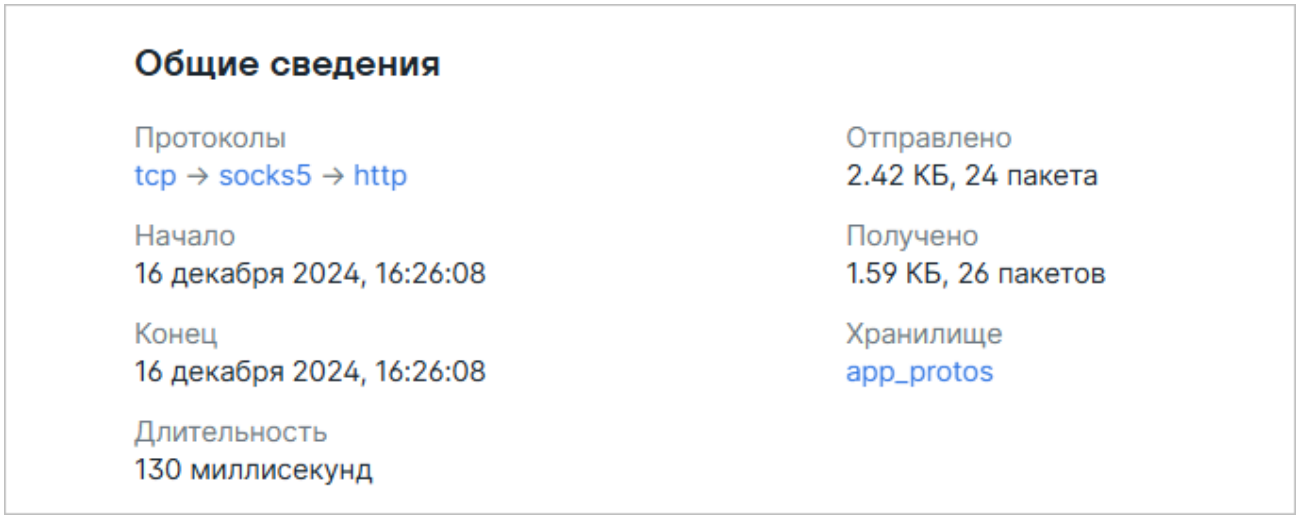


Рисунок 5. Протоколы в карточке сессии

Вы можете также добавить новый столбец **Прикладные протоколы** в таблицу сессий или атак. По умолчанию отображается столбец **Прикладной протокол**, в котором указан основной прикладной протокол сессии.

Для фильтрации сессий по всем прикладным протоколам можно использовать новый параметр `app_protos`, только по основному — `app_proto`, как и в предыдущих версиях PT NAD.

Примечание. Круговая диаграмма на системном виджете **Прикладные протоколы** продолжает строиться на данных `app_proto`.

Ускорение работы правил для атак

Механизм сигнатурного анализа (см. раздел 2.2) стал обрабатывать трафик в три раза быстрее, чем в предыдущих версиях. Это улучшение позволяет проверять больший объем трафика на существующей аппаратуре и снижает требования к аппаратной платформе для будущих реализаций. Ускорение наиболее заметно в инсталляциях, работающих на виртуальных машинах, а также в системах с небольшими аппаратными ресурсами.

Объединение правил для атак и групп узлов и портов

Начиная с версии 12.2 правила для атак (см. раздел 20.2) и группы узлов и портов (см. раздел 20.7) находятся в одном разделе меню администрирования **Правила для атак и группы**. Благодаря этому стало удобнее отслеживать изменения, которые были внесены в правила и группы с момента последней синхронизации.

Кроме того, теперь операторы могут отдельно просматривать группы узлов и портов, содержащие ошибки или неприменённые изменения. Для этого доступны соответствующие фильтры, которые ранее применялись только к правилам для атак.

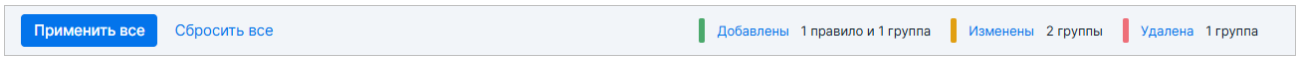


Рисунок 6. Фильтрация правил и групп с изменениями

Более удобная регистрация инцидента в MaxPatrol 10

При настроенной интеграции PT NAD с MaxPatrol 10 можно регистрировать инциденты (см. раздел 19) в MaxPatrol 10 на основе метаданных трафика, захваченного PT NAD. В новой версии PT NAD функция регистрации инцидента была улучшена. Теперь операторы могут заполнить форму с описанием инцидента, не покидая PT NAD.

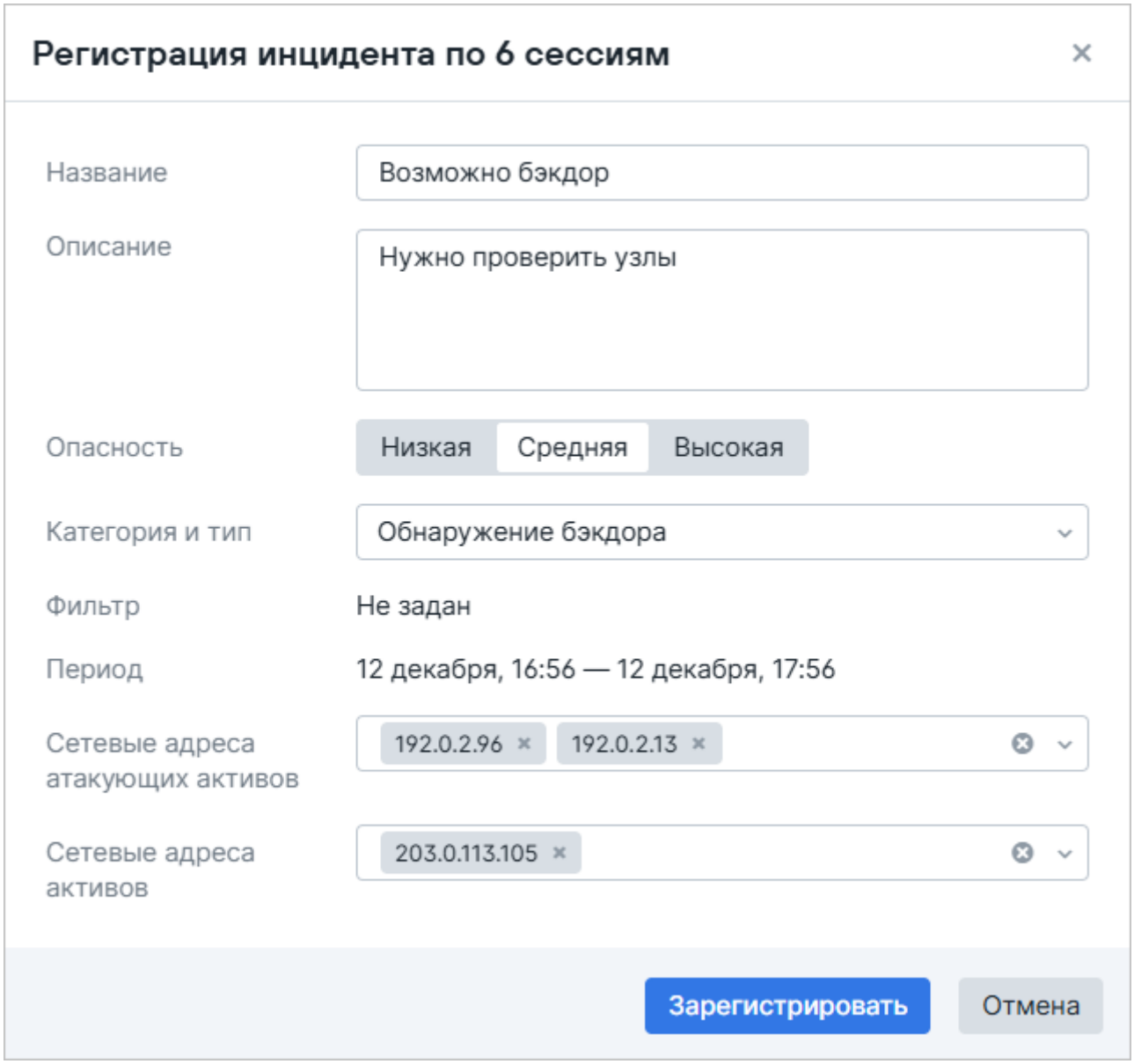


Рисунок 7. Регистрация инцидента

Улучшенный поиск аномального поведения

Для поиска аномального поведения в информационной инфраструктуре организации используется модуль ptdpi-worker@ad подсистемы обогащения. В версии 12.2 переработан как сам модуль, так и внутренняя логика его взаимодействия с другими компонентами PT NAD. Благодаря этому скорость поиска угроз (в частности, атак Kerberoasting) увеличилась в несколько раз. Кроме того, повысилась стабильность работы модуля.

Улучшение навигации по времени

В версии 12.2 навигация по времени при просмотре и фильтрации данных стала более удобной. Для этого на страницы **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** добавлены новые элементы управления (см. раздел 6.4).

Теперь на диаграмме интенсивности трафика (см. раздел 6.3) операторы могут перемещать выбранный период фильтрации и изменять его длину, а также управлять масштабом временной шкалы.

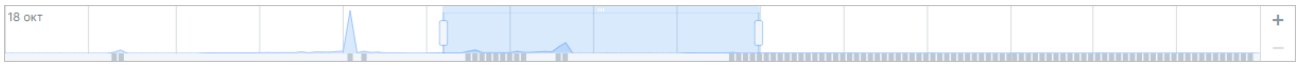


Рисунок 8. Изменение периода фильтрации на диаграмме интенсивности трафика

Для быстрой фильтрации данных появилась возможность смещать период на половину его длины вправо и влево, а также выбирать ранее установленные периоды.

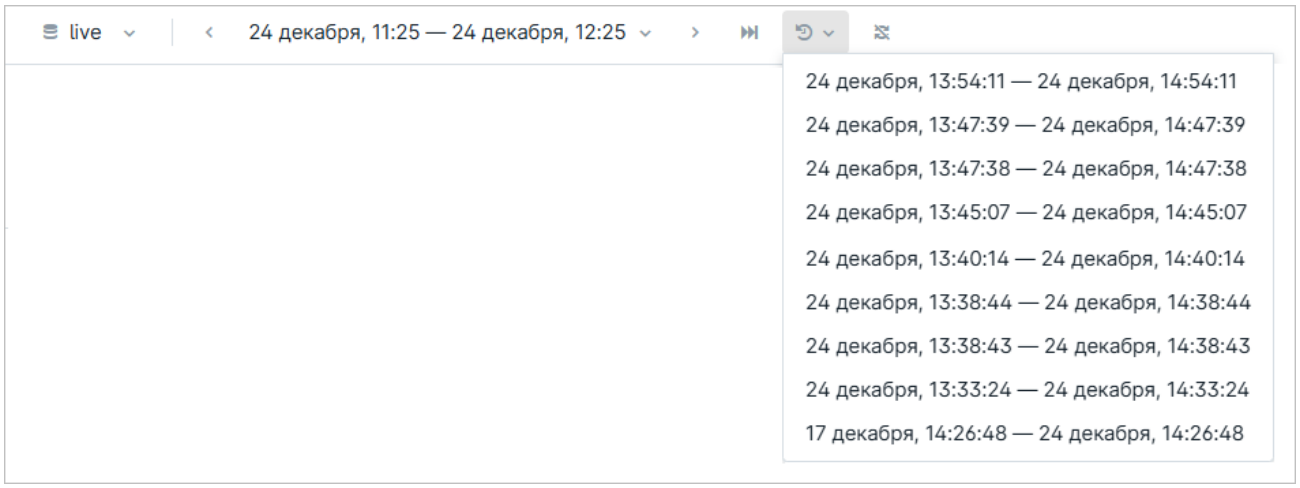


Рисунок 9. Выбор ранее установленных периодов

Отображение типа сработавшего правила в ленте активностей

Начиная с версии 12.2 в ленте (см. раздел 14) напротив активностей, которые были сгенерированы по срабатыванию пользовательских правил по личным или общим фильтрам, добавлены значки и соответственно. Для активностей, сгенерированных по срабатыванию системных правил, значок отсутствует. Улучшение позволяет визуально различать активности в ленте, а также быстрее находить нужные.

Кроме того, теперь операторы могут искать активности по типу сработавших правил. Для этого в панель фильтрации в блок параметров **Тип** добавлена группировка активностей по типу правил (**Личные**, **Общие** и **Системные**).

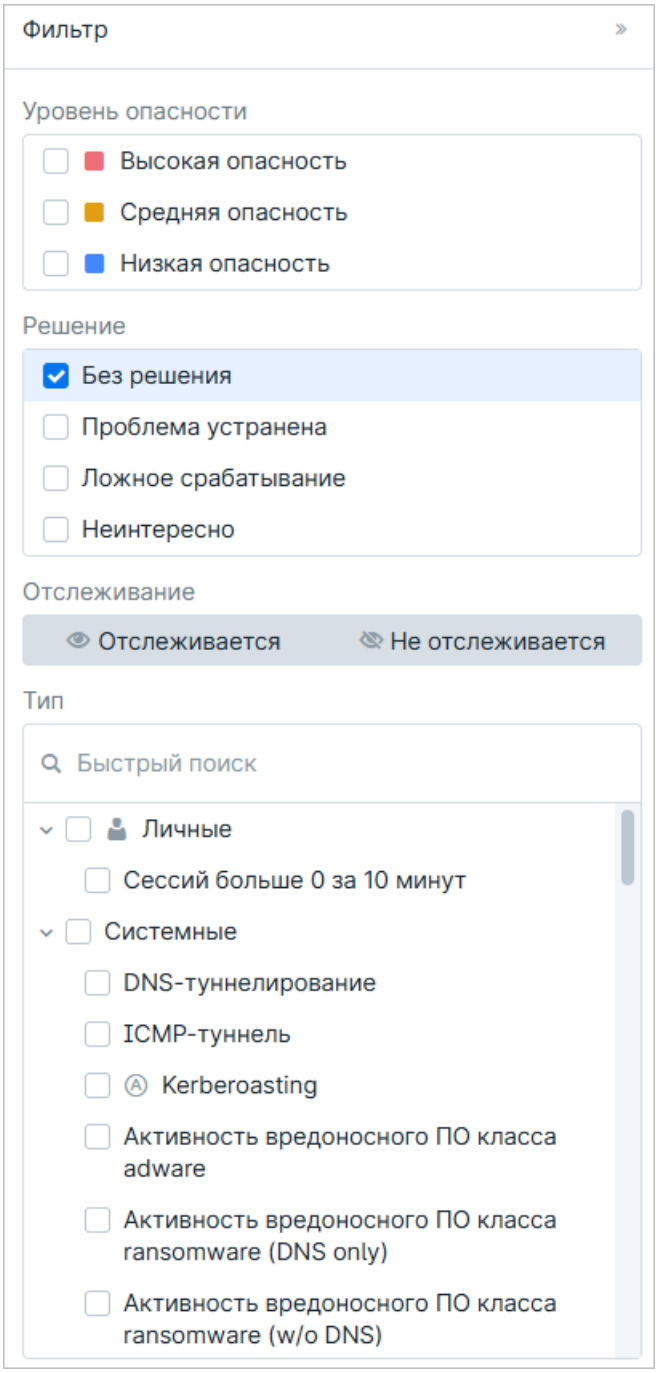


Рисунок 10. Фильтрация активностей

Работа с нормализованным URL

Начиная с версии 12.2 адрес HTTP-запроса отображается в карточке сессии в нормализованном (декодированном) виде. Это было сделано, в частности, для удобства просмотра URL, содержащих кириллицу. Например, закодированный адрес `/content/`

%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%B5%D1%86%20%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%20%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0.pdf теперь отображается как /content/Образец паспорт объекта.pdf.

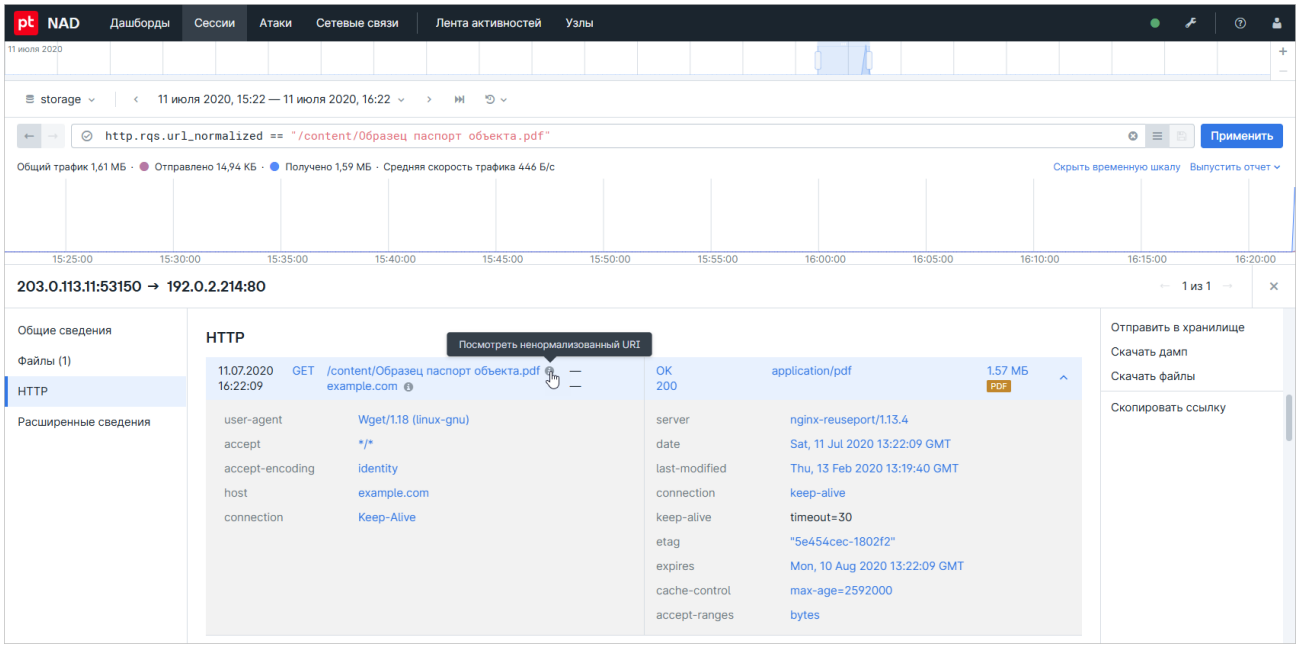


Рисунок 11. Просмотр нормализованного URL в карточке сессии

Для поиска сессий с использованием нормализованного URL операторы могут использовать новый параметр фильтрации `http.rqs.url_normalized`.

Ненормализованный URL можно увидеть, нажав на значок рядом. Поиск сессий по таким URL также сохраняется — например, для расследования инцидентов ИБ, когда злоумышленники манипулируют с URL для эксплуатации уязвимостей. Для поиска операторы могут по-прежнему использовать параметр фильтрации `http.rqs.url`.

Улучшение существующих правил для активностей

В версии 12.2 улучшены правила для выявления следующих активностей:

— Активность сервера OpenVPN внутри организации.

— Соединения с внешними серверами OpenVPN.

— Медленное сканирование.

— Атака NTLM Relay.

Улучшения направлены на то, чтобы уменьшить количество ложных и неинтересных срабатываний правил (см. раздел 14), а также сделать карточки активностей, сгенерированных по срабатыванию правил, более информативными.

4. Принципы безопасной работы

Безопасная работа PT NAD гарантируется, если:

— Перед развертыванием PT NAD установлены все обновления безопасности для среды функционирования системы (операционное обеспечение).

— Система установлена корректно в соответствии с документами «Руководство по установке на один сервер» и «Руководство по установке на несколько серверов».

— Система установлена и администрируется человеком, имеющим достаточную квалификацию и (или) прошедшим курс обучения работе с PT NAD и администрированию этого средства защиты информации.

— Работа с системой выполняется в соответствии с документами «Руководство оператора» и «Руководство администратора».

5. Вход в PT NAD

Пользовательский интерфейс PT NAD доступен в браузере. Предусмотрено два варианта входа в интерфейс продукта:

— Вход напрямую в интерфейс продукта с учетными данными, предварительно настроенными администратором.

— Вход через сервис PT Management and Configuration (далее также — PT MC), обеспечивающий единый вход для всех продуктов Positive Technologies.

  Сервис PT MC доступен только в том случае, если интеграция с ним была настроена.

В этом разделе

Вход в PT NAD без сервиса единого входа (см. раздел 5.1)

Вход в PT NAD через PT MC (см. раздел 5.2)

5.1. Вход в PT NAD без сервиса единого входа

Примечание. Если настроена аутентификация с помощью сервиса единого входа PT MC, то по умолчанию вход в интерфейс продукта выполняется через этот сервис.

Перед входом в интерфейс запросите у администратора PT NAD ссылку для входа, а также логин и пароль вашей учетной записи пользователя.

► Чтобы войти в PT NAD:

1. В адресной строке браузера введите ссылку, предоставленную вам администратором PT NAD.

   Откроется страница входа в PT NAD.

2. Введите логин и пароль учетной записи.
3. Нажмите **Войти**.

5.2. Вход в PT NAD через PT MC

Примечание. Если настроена аутентификация с помощью сервиса единого входа PT MC, то по умолчанию вход в интерфейс продукта выполняется через этот сервис.

Перед входом в PT NAD через сервис PT MC запросите у администратора этого сервиса ссылку для входа в интерфейс продукта, а также логин и пароль вашей учетной записи.

Перед выполнением инструкции нужно убедиться, что в браузере разрешены всплывающие окна.

► Чтобы войти в PT NAD:

1. В адресной строке браузера введите ссылку для входа в интерфейс PT NAD.

   Откроется страница входа в PT MC.

2. Введите логин и пароль учетной записи.

   Примечание. Стандартная сессия пользователя в PT NAD длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

3. Нажмите **Войти**.

6. Интерфейс PT NAD

Все действия в PT NAD вы можете выполнять с помощью графического пользовательского интерфейса. В этом разделе приводится описание основных элементов интерфейса PT NAD, доступных после входа в PT NAD.

Для работы в интерфейсе PT NAD рекомендуется использовать браузер Google Chrome или Mozilla Firefox.

В этом разделе

См. также

6.1. Главное меню

В верхней части любой страницы интерфейса PT NAD расположено главное меню.

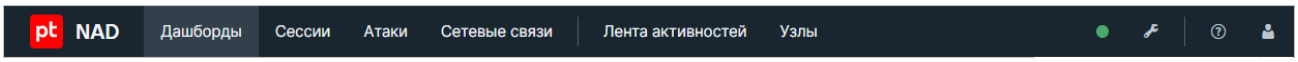


Рисунок 12. Главное меню PT NAD

Главное меню обеспечивает доступ к основным функциям PT NAD.

Переход к другим приложениям

При настроенной интеграции с MaxPatrol 10 версии 21 или выше в левой части главного меню отображается кнопка меню для перехода в другие приложения Positive Technologies, зарегистрированные в сервисе управления пользователями и доступом PT Management and Configuration (PT MC).

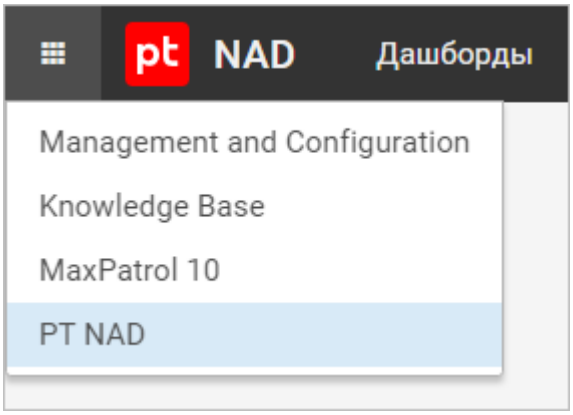


Рисунок 13. Меню перехода в другие приложения Positive Technologies

Переход к страницам продукта

Главное меню содержит разделы для перехода к страницам продукта (см. раздел 6.2):

- **Дашборды** — страница со статистическими данными о трафике в сети в наглядном представлении (например, на карте, графике, в таблице).
- **Сессии** — страница со списком сессий и информацией о них.
- **Атаки** — страница со списком срабатываний правил (см. раздел 20.2) и информацией о них.
- **Сетевые связи** — страница с топологией сети, показывающая связи между узлами.
- **Лента активностей** — страница со списком обнаруженных подозрительных активностей в информационной инфраструктуре.

  При наличии непросмотренных вами активностей рядом с названием раздела отображается счетчик новых и обновленных активностей.
- **Узлы** — страница с перечнем обнаруженных узлов.

Прочие элементы управления

Среди прочего в главном меню также находится индикатор состояния продукта (см. раздел 6.6), а справа от него — следующие элементы управления:

раскрывает меню для перехода к страницам, предназначенным для настройки работы и администрирования PT NAD.

раскрывает меню с номером установленной версии PT NAD и ссылками на пользовательскую документацию.

позволяет просмотреть и изменить личные данные пользователя, настроить интерфейс, уведомления и рассылку отчетов по расписанию, а также завершить работу в PT NAD с текущей учетной записью. По наведению курсора на значок отображаются имя и фамилия пользователя, который вошел в PT NAD.

6.2. Страницы интерфейса и рабочая область

Главное меню содержит разделы для перехода к страницам продукта. Страницы по назначению делятся:

— на страницы для мониторинга трафика: **Дашборды** (открывается по умолчанию при входе в интерфейс) и **Лента активностей**;

— страницы для анализа метаданных трафика: **Сессии**, **Атаки**, **Сетевые связи** и **Узлы**;

— страницы для администрирования продукта (кнопка в главном меню);

— страницы для управления учетной записью (кнопка в главном меню).

Рабочая область

Содержимое и вид рабочей области зависят от выбранной страницы, и может отображаться в виде:

— таблицы;

— виджета;

— карточки;

— ленты активностей;

— карты сетевых взаимодействий.

Содержимое рабочей области также зависит от выделенного участка на диаграмме интенсивности трафика (см. раздел 6.3) и фильтров, примененных в панели фильтрации (см. раздел 6.5).

6.3. Диаграмма интенсивности трафика

На страницах с информацией о захваченном трафике (**Дашборды**, **Сессии**, **Атаки** и **Сетевые связи**) под главным меню находится диаграмма, которая показывает интенсивность трафика — среднюю скорость передачи данных в определенный момент. С помощью этой диаграммы вы можете фиксировать всплески сетевой активности в сети организации.

Рисунок 14. Диаграмма интенсивности трафика

При наведении курсора на диаграмму отображаются дата, время и объем трафика, который был передан в это время в среднем за секунду.

Серым цветом на диаграмме обозначаются временные промежутки, за которые в трафике было зарегистрировано наибольшее количество атак.

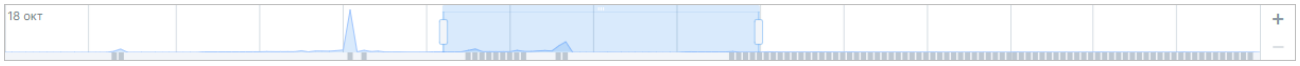


Рисунок 15. Отображение всплесков количества атак на диаграмме интенсивности трафика

Для изменения масштаба временной шкалы на диаграмме используются элементы управления + и −.

При выделении участка на диаграмме данные будут отфильтрованы в соответствии с выбранным периодом. С помощью курсора мыши можно перемещать период, а также изменять его длину.

6.4. Элементы управления для контроля отображения данных

Под диаграммой интенсивности трафика (см. раздел 6.3) находятся элементы управления, с помощью которых вы можете контролировать отображение данных о захваченном трафике:

выводит список хранилищ (см. раздел 7.1), позволяет выбрать хранилища для отображения их содержимого в интерфейсе, а также дает возможность импортировать в хранилища дампы трафика в формате PCAP (см. раздел 7.3). В интерфейсе центральной консоли вместо списка хранилищ выводит список дочерних систем, позволяет выбрать дочерние системы (см. раздел 8) для работы с данными.

Цвет элемента сигнализирует о состоянии подключения дочерних систем:

- все выбранные дочерние системы доступны;
- все выбранные дочерние системы недоступны;
- среди выбранных дочерних систем есть недоступные или отвечающие с ошибками;
- все выбранные дочерние системы отвечают с ошибками.

сбрасывает фильтры по периоду к значению по умолчанию (все события ИБ за последний час). Текущий период фильтрации данных (см. раздел 9.5) отображается слева от элемента.

выводит список ранее выбранных периодов для фильтрации данных.

Примечание. Элементы управления для контроля отображения данных о трафике доступны только на страницах с такими данными (**Дашборды**, **Сессии**, **Атаки** и **Сетевые связи**).

6.5. Панель фильтрации

Аналогично диаграмме интенсивности трафика (см. раздел 6.3), панель фильтрации позволяет настроить отображение не всех данных, а только их части. Фильтрация данных осуществляется с помощью условий (см. приложение Б), введенных в панели фильтрации.

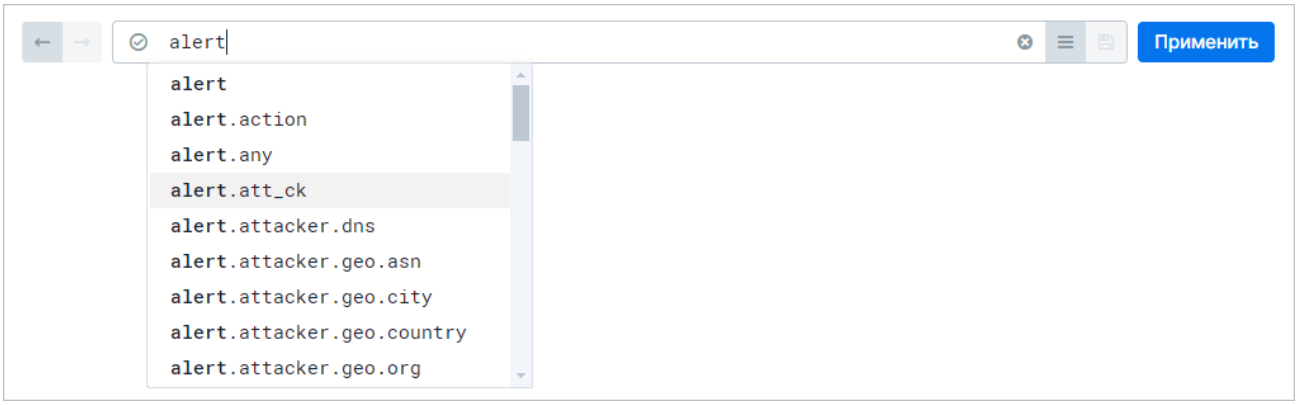


Рисунок 16. Панель фильтрации

Фильтр, примененный в строке фильтрации, определяет содержимое рабочей области (см. раздел 6.2) страниц с обработанным трафиком.

См. также

Управление фильтрами (см. раздел 13)

6.6. Индикатор состояния продукта

Справа от элементов управления для контроля отображения данных о трафике находится индикатор состояния продукта:

- сигнализирует о проблемах или ошибках в работе продукта;
- предупреждает о приближении наблюдаемых параметров (например, загрузки ЦП) к пороговым значениям;
- сообщает о том, что PT NAD работает без ошибок;
- уведомляет о том, что функция мониторинга не была настроена администратором продукта, отключена или не запущена.

По нажатию на индикатор открывается всплывающее окно с информацией о текущем состоянии продукта.

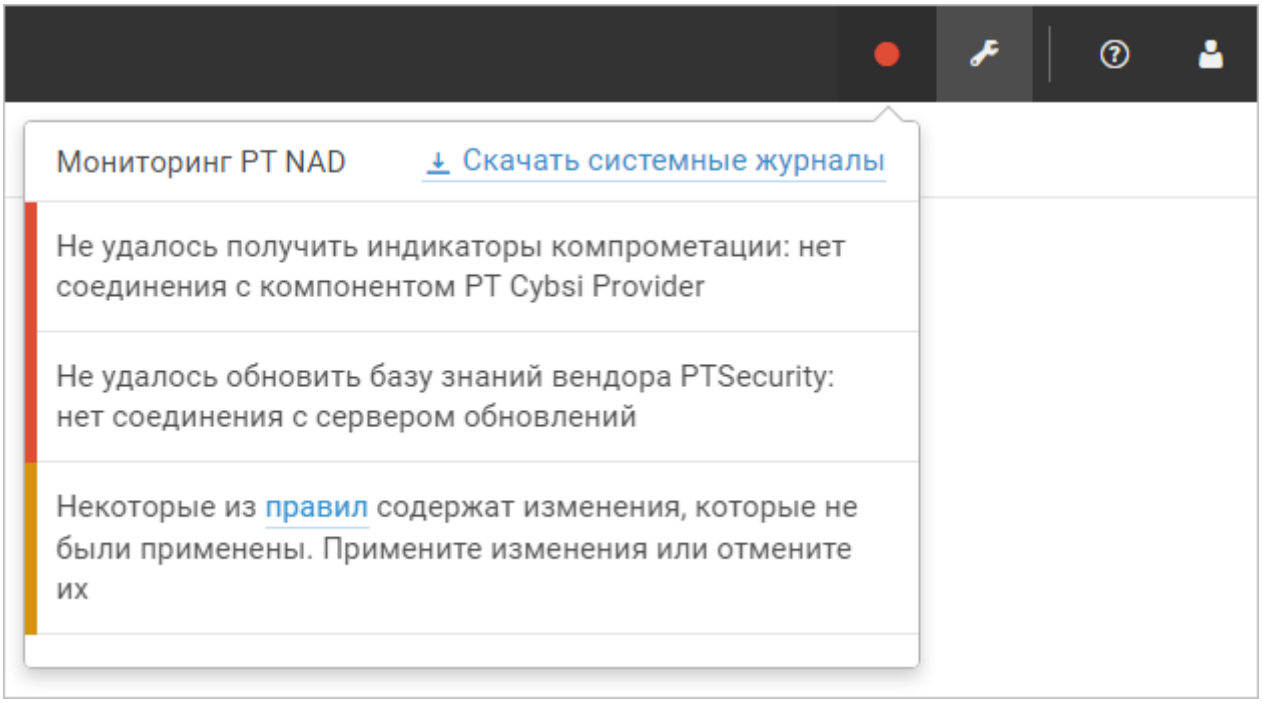


Рисунок 17. Состояние продукта

По нажатию на ссылку **Мониторинг PT NAD** выполняется переход к внешней системе мониторинга (эта возможность может быть не настроена администратором продукта).

По нажатию на ссылку **Скачать системные журналы** на ваш компьютер скачивается архив с журналами продукта. Эта ссылка доступна только тем пользователям, у которых есть право доступа к центру управления.

Примечание. Индикатор состояния продукта может быть скрыт администратором PT NAD.

7. Работа с хранилищами

PT NAD захватывает трафик и выполняет его разбор (см. раздел 2.1.3). Исходная копия захваченного трафика и результаты разбора хранятся в хранилищах.

В интерфейсе продукта вы выбираете те хранилища, с данными из которых вам нужно работать. Например, вы можете просматривать детали сессий, данные о которых записаны в определенное хранилище. Хранилища бывают потоковыми и выделенными.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

Потоковые хранилища

В потоковые хранилища поступает поток трафика из подсистемы захвата. Каждый модуль ptdpi подсистемы захвата в режиме реального времени записывает данные в свое потоковое хранилище. Таким образом, при выборе потокового хранилища вы работаете с информацией о только что или недавно захваченном трафике организации. Кроме того, такие хранилища нужны для настройки уведомлений и регулярных отчетов о поступающем трафике, для экспорта его исходной копии и метаданных, формирования ленты активностей (см. раздел 14) и составления списка узлов (см. раздел 15).

Чтобы избежать переполнения дискового пространства, PT NAD удаляет старые данные из потоковых хранилищ. Новые PCAP-файлы с исходной копией трафика записываются поверх старых в зависимости от занятого ими места на диске, а метаданные трафика удаляются по достижении предельного срока хранения.

> **Примечание.** Вы можете уточнить актуальные значения параметров автоматического удаления данных из потоковых хранилищ у администратора PT NAD.

Выделенные хранилища

Для работы с определенным трафиком вы можете выделить под него отдельное хранилище. Например, для анализа трафика, связанного с инцидентом ИБ, можно выделить хранилище и скопировать в него трафик из потокового хранилища или импортировать PCAP-файл из сторонней программы. Вы можете быстро переключаться между выделенными хранилищами для поиска нужного трафика без необходимости вручную фильтровать потоковый трафик по метаданным и по времени. Кроме того, PT NAD не удаляет содержимое выделенных хранилищ автоматически, поэтому их можно использовать для сохранения данных для истории.

Вы можете создавать любое количество выделенных хранилищ. Неиспользуемые выделенные хранилища можно удалять.

В этом разделе

Импорт трафика в выделенное хранилище (см. раздел 7.3)

Удаление выделенных хранилищ (см. раздел 7.4)

См. также

Копирование трафика сессий в формате PCAP в хранилище (см. раздел 9.10)

Копирование трафика сессий с атаками в формате PCAP в хранилище (см. раздел 10.9)

7.1. Список хранилищ

Вы можете просматривать информацию о хранилищах на странице **Хранилища**, доступной в разделе главного меню.

В списке потоковые хранилища отображаются первыми, независимо от сортировки данных в таблице. Кроме того, в таблице у потоковых хранилищ, в отличие от выделенных, отсутствует информация о трафике и его импорте, о создателе и пути хранения на сервере.

Для удобства работы с хранилищами вы можете к каждому из них добавлять текстовые комментарии по ссылке **Добавить описание** в столбце **Описание**. Ваши комментарии видны всем пользователям, у которых есть доступ к этой странице. Вы можете изменить свой или чужой комментарий, нажав на ссылку с текстом этого комментария.

Вы можете найти хранилище в списке, указав в поле поиска его название, описание или имя пользователя, создавшего хранилище.

7.2. Выбор хранилищ для работы с данными

По умолчанию на страницах **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** отображаются данные только из потоковых хранилищ. При необходимости на этих страницах вы можете также просматривать данные из выделенных хранилищ и работать с представленной информацией. Для этого нужно выбрать хранилища.

- Чтобы выбрать хранилища для работы с данными:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. Нажмите .
  3. Выберите хранилища.

     Примечание. При выборе потокового хранилища нужно убедиться, что модуль ptdpi, который записывает в него данные, включен (см. раздел 20.1.2). Иначе хранилище будет пустым или содержать устаревшие данные.
  4. Нажмите **Выбрать**.

7.3. Импорт трафика в выделенное хранилище

На страницах **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** вы можете работать с выделенными хранилищами. Для наполнения выделенного хранилища вы можете импортировать в него трафик в формате PCAP (дамп).

- Чтобы импортировать трафик в выделенное хранилище:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. Нажмите .
  3. Нажмите **Импортировать трафик**.
  4. Выберите хранилище или добавьте новое.
  5. Перетащите файлы в окно или добавьте их по ссылке **выберите**.
  6. Нажмите **Импортировать**.

     Начнутся загрузка трафика из файла в выделенное хранилище и разбор этого трафика (см. раздел 2.1.3). Поиск активностей, флуда и сканирования, а также сбор информации об узлах на этом этапе не выполняются.

  Вы можете просмотреть последние загруженные данные в рабочей области страниц **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** по кнопке **Показать результат**.

  Примечание. Вы также можете импортировать дампы в выделенные хранилища по кнопке **Импорт трафика** на странице со списком хранилищ (см. раздел 7.1).

См. также

Копирование трафика сессий в формате PCAP в хранилище (см. раздел 9.10)

Копирование трафика сессий с атаками в формате PCAP в хранилище (см. раздел 10.9)

7.4. Удаление выделенных хранилищ

Общий объем хранилищ ограничен дисковым пространством, выделенным для них при развертывании PT NAD. Чтобы освободить дисковое пространство, вы можете удалить ненужные выделенные хранилища.

- Чтобы удалить выделенные хранилища:

  1. В главном меню выберите → **Хранилища**.
  2. Выберите хранилища.

Примечание. Вы можете выбрать несколько хранилищ, удерживая клавишу Ctrl или Shift. Для выбора всех хранилищ нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A. Если среди выбранных хранилищ будет потоковое хранилище, PT NAD не удалит его.

3. Нажмите **Удалить** и подтвердите удаление.

8. Работа с дочерними системами

В этом разделе приводится описание работы с дочерними системами в интерфейсе центральной консоли (см. раздел 2.4) для экземпляров PT NAD, объединенных в иерархию.

Центральная консоль не захватывает сетевой трафик самостоятельно. В интерфейсе этой системы отображаются данные о трафике из подключенных дочерних систем. На страницах **Дашборды**, **Сессии**, **Атаки**, **Сетевые связи**, **Лента активностей** и **Узлы** центральной консоли вы можете выбрать те дочерние системы, с данными из которых вам нужно работать.

В этом разделе

8.1. Просмотр данных из дочерних систем

- Чтобы просмотреть данные из дочерних систем,

  в главном меню выберите **Дашборды**, **Сессии**, **Атаки**, **Сетевые связи**, **Лента активностей** или **Узлы**.

  Примечание. Чтобы у пользователя был доступ к данным из дочерних систем, в каждой системе ему должна быть присвоена стандартная роль оператора или администратора. Для этого нужно обратиться к администратору сервиса PT MC, в котором зарегистрированы дочерние системы.

В интерфейсе центральной консоли вы можете:

- просматривать статистические данные о трафике на виджетах (см. раздел 11);
- просматривать список сессий (см. раздел 9.1), зарегистрированных дочерними системами, а также информацию о каждой отдельной сессии в ее карточке (см. раздел 9.2);
- экспортировать метаданные трафика сессий (см. раздел 9.11);
- просматривать список атак (см. раздел 10.1), обнаруженных дочерними системами, а также информацию о каждой отдельной атаке в ее карточке (см. раздел 10.2);
- экспортировать метаданные трафика с атаками (см. раздел 10.10);
- просматривать сетевые связи узлов (см. раздел 12);
- просматривать список активностей (см. раздел 14.1), обнаруженных дочерними системами, а также карточку (см. раздел 14.2) каждой отдельной активности и связанный с активностью трафик (см. раздел 14.3);
- просматривать список узлов (см. раздел 15.1).

8.2. Выбор дочерних систем для работы с данными

По умолчанию в интерфейсе центральной консоли отображаются данные из доступных дочерних систем. При необходимости вы можете выбрать только те системы, которые вас интересуют.

- Чтобы выбрать дочерние системы для работы с данными:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки**, **Сетевые связи**, **Лента активностей** или **Узлы**.
  2. Нажмите  .

     Примечание. Цвет значка зависит от состояния подключения (см. раздел 6.4) дочерних систем.
  3. Выберите дочерние системы, удерживая клавишу Ctrl или Shift.
  4. Нажмите **Выбрать**.

9. Работа с сессиями

PT NAD анализирует поток трафика и может распознавать отдельные сессии — сеансы передачи информации между двумя узлами (клиентом и сервером). Информация об участниках и параметрах сессии сохраняется в базе данных и используется для автоматического поиска угроз ИБ. Операторы также могут самостоятельно изучать сессии в интерфейсе продукта для расследования инцидентов ИБ.

Список зарегистрированных сессий отображается на странице **Сессии**, доступной из одноименного раздела главного меню.

В этом разделе

9.1. Просмотр списка сессий

- Чтобы просмотреть список сессий,

  в главном меню выберите **Сессии**.

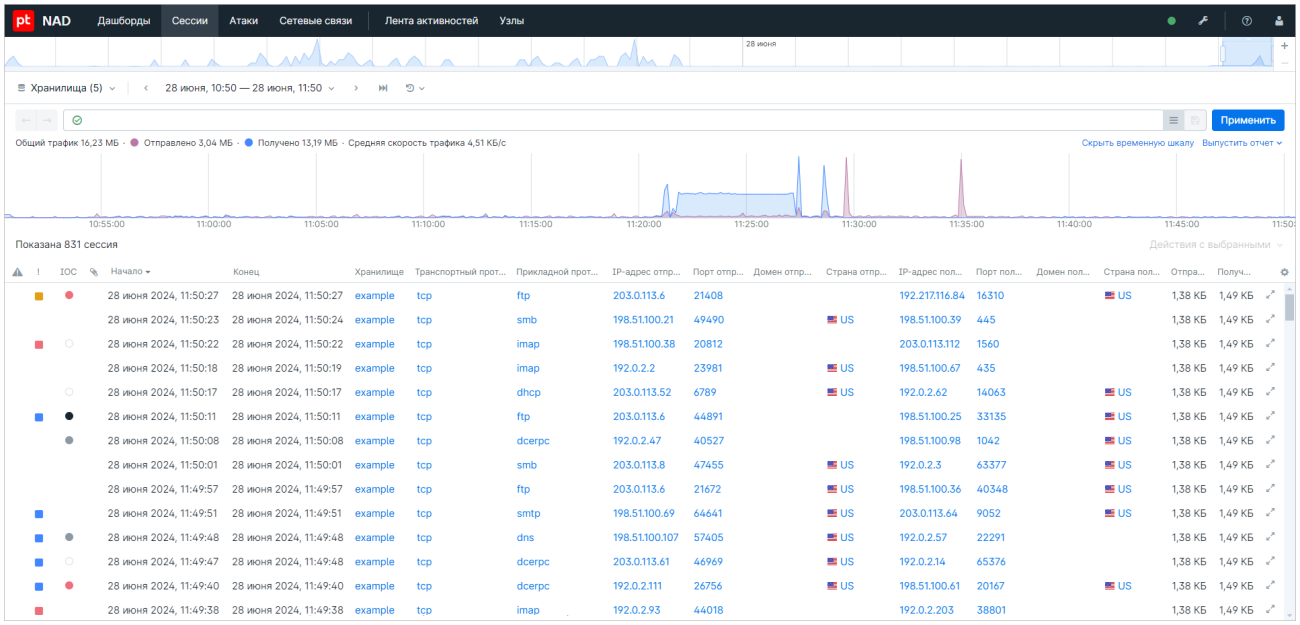


Рисунок 18. Просмотр списка сессий

Вы можете фильтровать данные на странице с помощью диаграммы интенсивности трафика (см. раздел 6.3) и панели фильтрации (см. раздел 6.5).

Под панелью фильтрации находится строка со сводной информацией о трафике за период, выбранный на диаграмме интенсивности трафика.

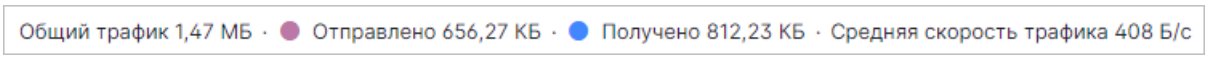


Рисунок 19. Просмотр сводной информации о трафике

Информация в строке также соответствует примененным параметрам фильтрации.

По умолчанию в таблице сессий отображаются столбцы:

- **Ошибки обработки сессии** ( ) — наличие значка в строке сессии говорит о том, что при обработке трафика сессии были обнаружены ошибки (см. приложение Е).
- **!** — уровень опасности атаки или другого события ИБ; если в записи была добавлена отметка о ложном срабатывании правила (см. раздел 10.12.1), значок уровня опасности зачеркнут.
- **IOC** — обнаруженные индикаторы компрометации (см. раздел А.6).
- **Файлы** ( ) — признак того, что во время сессии были переданы файлы, распознанные PT NAD.
- **Начало** — дата и время начала сессии.
- **Конец** — дата и время окончания сессии; если сессия еще активна, вместо времени отображается значок (при наведении на него курсора во всплывающей подсказке отображается время получения последней информации о сессии).

- **Дочерняя система** — метка дочерней системы (см. раздел 8), из которой получены данные о трафике. Отображается в интерфейсе центральной консоли (см. раздел 2.4) для экземпляров PT NAD, объединенных в иерархию.
- **Хранилище** — название выделенного хранилища (см. раздел 7), в котором хранятся данные о сессии и ее трафик, или название модуля ptdpi, с которого в потоковое хранилище (см. раздел 7) поступили данные о сессии и ее трафик.
- **Транспортный протокол** — протокол транспортного уровня.
- **Прикладной протокол** — протокол прикладного уровня (см. приложение B).
- **IP-адрес отправителя** — IP-адрес узла, отправившего сетевой запрос.
- **Порт отправителя**.
- **Домен отправителя**.
- **Страна отправителя**.
- **IP-адрес получателя** — IP-адрес узла, получившего сетевой запрос.
- **Порт получателя**.
- **Домен получателя**.
- **Страна получателя**.
- **Отправленный объем** — объем данных, переданных в рамках сессии.
- **Полученный объем** — объем данных, полученных в рамках сессии.

По умолчанию сессии в таблице отсортированы по времени начала (сессии, которые начались позднее, отображаются выше).

В таблице сессий вы можете:

- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- изменять набор столбцов по нажатию ⚙.

Параметры таблицы сохраняются для вашей учетной записи при переходе на другие страницы или выходе из продукта.

Вы можете восстановить состояние таблицы по умолчанию, нажав **Восстановить по умолчанию** во всплывающем окне со списком столбцов.

Из таблицы вы можете получать подробную информацию об IP-адресах, доменах и идентификаторах узлов. Если узел известен продукту (см. раздел 15), то вы можете просмотреть сводку об этом узле (см. раздел 15.3). Если IP-адрес или домен относятся к

неизвестному узлу, то вы можете перейти к просмотру статистики по этому IP-адресу или домену на дашбордах (см. раздел 17.1), а также получить информацию о них на внешних ресурсах (см. раздел 17.2).

9.2. Просмотр подробной информации о сессии

В таблице на странице **Сессии** доступны только основные сведения о сессиях. Полную информацию о каждой сессии вы можете просмотреть в ее карточке (см. рисунок 20).

- Чтобы просмотреть подробную информацию об отдельной сессии:

  1. В главном меню выберите **Сессии**.
  2. Откройте карточку сессии, нажав ⤢ в строке этой сессии.

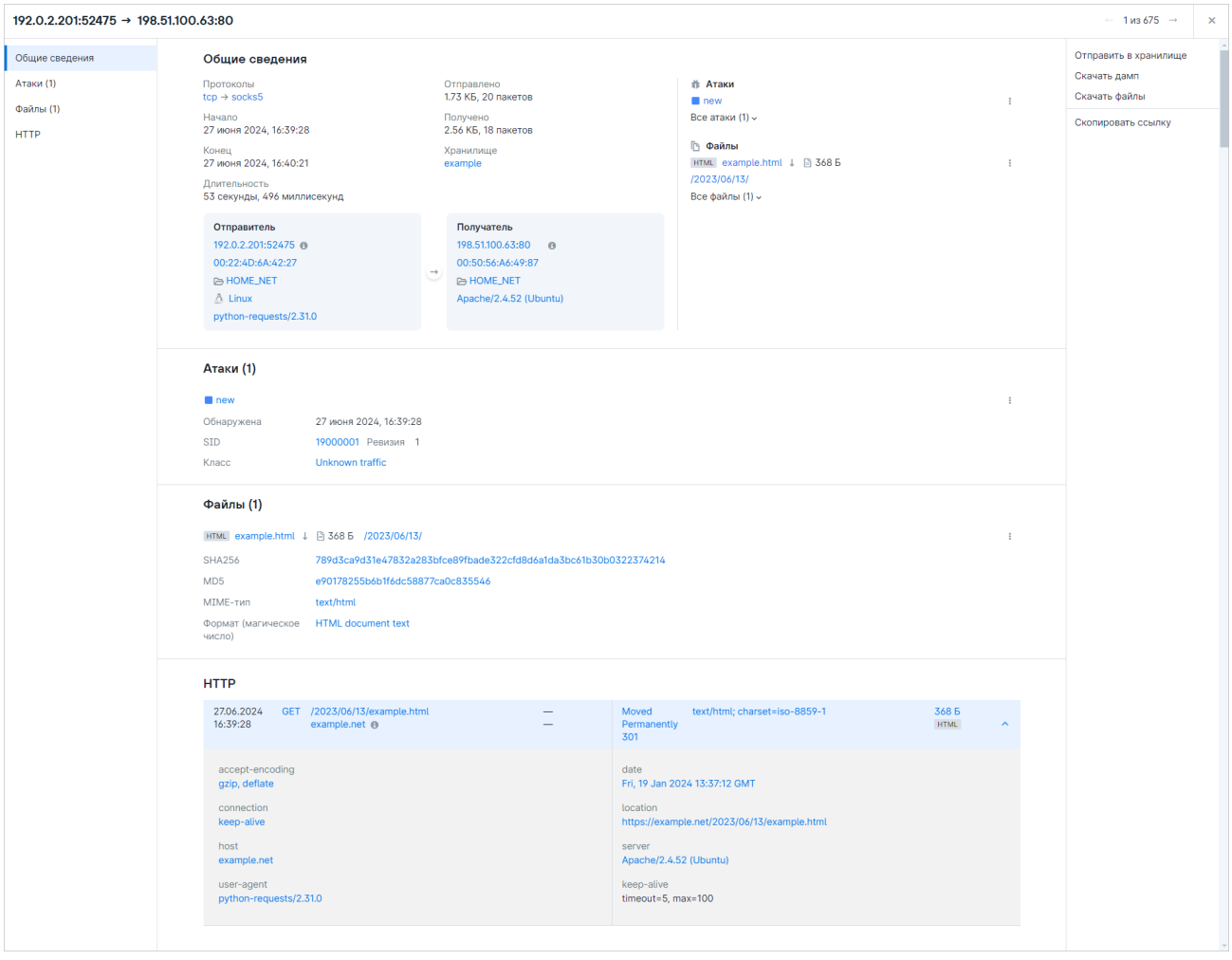


Рисунок 20. Просмотр карточки сессии

На вкладке **Общие сведения** отображается основная информация о сессии:

- время начала и завершения;
- длительность;
- отправители и получатели;
- список задействованных протоколов;
- в интерфейсе центральной консоли — метка дочерней системы, из которой получены данные о трафике;
- название хранилища с трафиком;
- обнаруженные атаки;
- переданные файлы;
- индикаторы компрометации, обнаруженные в сетевых транзакциях.

Если во время сессии были обнаружены атаки или переданы файлы, вы можете просмотреть подробную информацию о них на одноименных вкладках.

Если во время сессии был задействован прикладной протокол и PT NAD разобрал его сообщения (см. приложение B), вы можете просмотреть эти сообщения на вкладке с названием протокола.

Если вы включили показ расширенной информации в личном кабинете (см. раздел 9.3), в карточке сессии будет также отображаться вкладка **Расширенные сведения** с метаданными сессии в формате JSON.

Вы можете скопировать расширенную информацию в буфер обмена, нажав .

Если вы находитесь в интерфейсе центральной консоли (см. раздел 2.4), то в названии карточки отображаются название и метка дочерней системы, которая зарегистрировала сессию. Вы можете перейти в интерфейс этой системы по кнопке **Перейти в дочерний NAD**. В новой вкладке браузера откроется карточка этой же сессии в дочерней системе.

- Чтобы просмотреть подробную информацию о следующей сессии, показанной в таблице,

  нажмите .

- Чтобы просмотреть подробную информацию о предыдущей сессии, показанной в таблице,

  нажмите .

- Чтобы закрыть карточку,

  нажмите .

9.3. Включение показа расширенных данных сессии

Вы можете включить показ расширенных сведений о сессии в ее карточке (см. рисунок 21). Расширенные сведения — это метаданные сессии в формате JSON, сформированные в ходе обогащения сессии. Эти данные могут понадобиться для экспертного анализа сессий или экспорта в другие продукты.

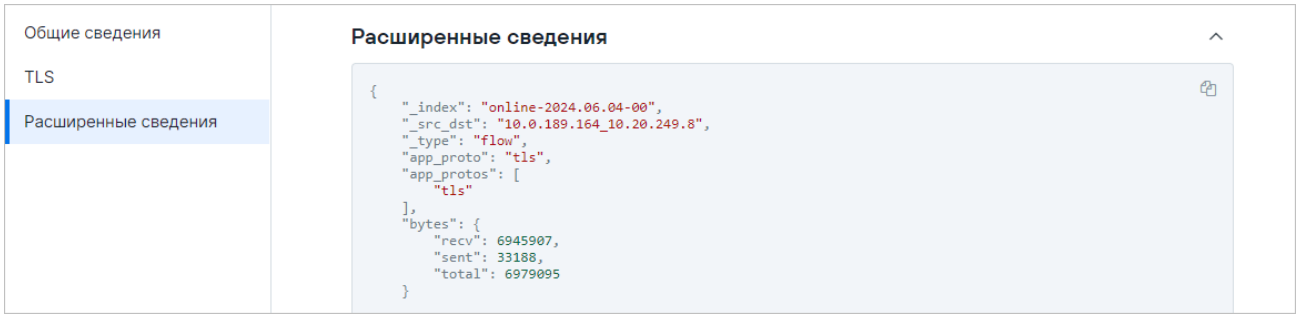


Рисунок 21. Просмотр расширенных данных сессии

- Чтобы включить показ расширенных данных сессии:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. Включите показ расширенной информации в карточках сессий и атак.
  3. Нажмите **Сохранить**.

См. также

Просмотр подробной информации о сессии (см. раздел 9.2)

Включение экспертного режима просмотра флагов и ошибок обработки сессий (см. раздел 9.7)

9.4. Просмотр объемов трафика, переданных за период

PT NAD позволяет просматривать объемы трафика, переданные за определенные периоды. Это может пригодиться при расследовании инцидентов ИБ для выявления закономерностей, например аномального увеличения обмена трафиком между двумя наблюдаемыми узлами в одни и те же дни недели.

- Чтобы просмотреть объем трафика, переданный за выбранный период:

  1. В главном меню выберите **Сессии**.
  2. Если требуется, отфильтруйте данные по периоду (см. раздел 9.5).
  3. Под строкой со сводной информацией о трафике выделите участок на диаграмме объемов отправленного и полученного трафика.

     В строке со сводной информацией о трафике отобразятся значения за выбранный период.

Под строкой со сводной информацией о трафике располагается диаграмма с областями (см. рисунок 22). Диаграмма показывает изменение интенсивности отправленного ( ) и полученного ( ) трафика. При наведении курсора на диаграмму отображаются дата, время и объемы трафика, которые были отправлены и получены в это время в среднем за секунду. Когда вы выделяете участок на диаграмме, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

> **Примечание.** На странице **Дашборды** аналогичную функцию выполняет виджет «Объем трафика (см. раздел A.1)».

Рисунок 22. Просмотр объемов отправленного и полученного трафика

Вы можете управлять отображением диаграммы на странице с помощью кнопки **Скрыть временную шкалу** или **Показать временную шкалу** под панелью фильтрации (см. раздел 6.5).

9.5. Фильтрация сессий по периоду

По умолчанию при входе в PT NAD на странице **Сессии** отображаются данные за последний час. Вы можете изменить период фильтрации данных.

- Чтобы отфильтровать сессии по периоду:

  1. В главном меню выберите **Сессии**.
  2. Нажмите на период для фильтрации.

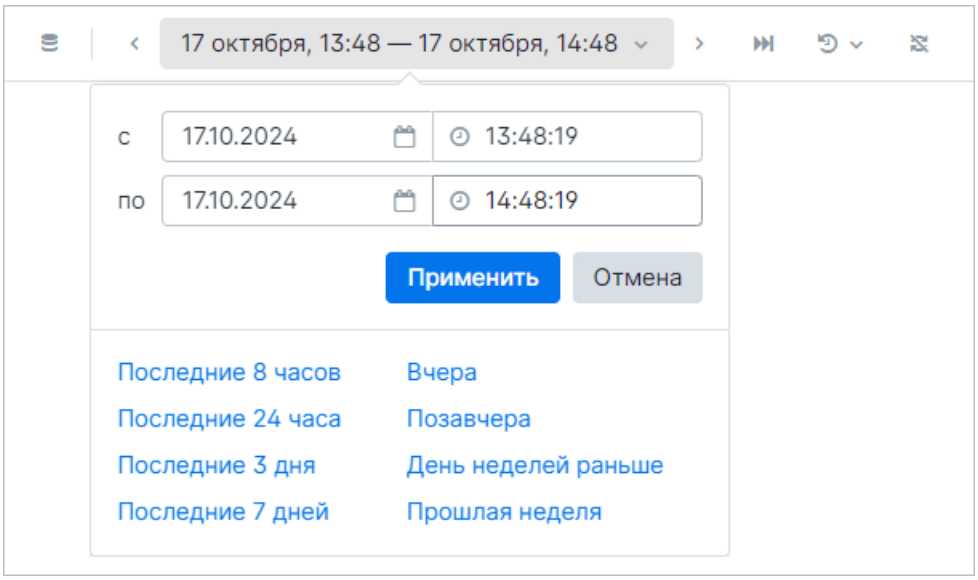


Рисунок 23. Настройка периода фильтрации данных

3. Укажите период и нажмите **Применить**.

- Чтобы сместить период на половину его длины влево,

  нажмите < .

- Чтобы сместить период на половину его длины вправо,

  нажмите > .

Вы также можете детализировать период фильтрации данных, выделяя с помощью курсора интервал на диаграммах интенсивности трафика (см. раздел 6.3) и объемов отправленного и полученного трафика (см. раздел 9.4).

Кроме того, вы можете выбрать один из ранее установленных периодов фильтрации, нажав .

- Чтобы вернуть период по умолчанию (данные за последний час),

  нажмите .

9.6. Фильтрация сессий по метаданным трафика

Вы можете фильтровать список сессий по метаданным трафика. Например, вы можете найти сессии, в которых использовался протокол HTTP и были обнаружены индикаторы компрометации. Для этого требуется применить фильтр с набором условий.

- Чтобы отфильтровать сессии по метаданным трафика:

  1. В главном меню выберите **Сессии**.
  2. В панели фильтрации (см. раздел 6.5) добавьте условия одним из способов:
     - Введите параметры для фильтрации, значения параметров и операторы на языке фильтрации продукта (см. приложение Б).

       Примечание. Вы можете просмотреть полный список доступных параметров для фильтрации, нажав комбинацию клавиш Ctrl+Space в строке фильтрации.

Рисунок 24. Ввод параметров фильтрации

При вводе параметров в строке фильтрации вы можете выбрать их значения из списка (только строковые и булевы). Значения собираются из метаданных трафика, отфильтрованного по периоду.

Рисунок 25. Выбор значений параметров фильтрации

- Добавьте параметры фильтрации с их значениями по ссылкам в таблице сессий.

3. Нажмите **Применить**.

Добавленные условия фильтрации можно сохранить, чтобы не указывать их снова в дальнейшем. Для этого нужно создать личный (см. раздел 13.1) или общий фильтр (см. раздел 13.2).

Вы можете просматривать историю примененных вами фильтров по нажатию ← и →. PT NAD хранит в истории 100 последних фильтров.

Кроме того, вы можете добавлять метаданные трафика в строку фильтрации по ссылкам в карточке сессии (см. раздел 9.2).

9.7. Включение экспертного режима просмотра флагов и ошибок обработки сессий

При анализе соединения и обработке сессии PT NAD может добавлять в свойства сессии дополнительную информацию об анализе пакетов сессии, сборке сессии и записи трафика в хранилище. По умолчанию вы можете просматривать эту информацию в карточках сессии и атаки по нажатию на значок ⚠ в заголовках карточек.

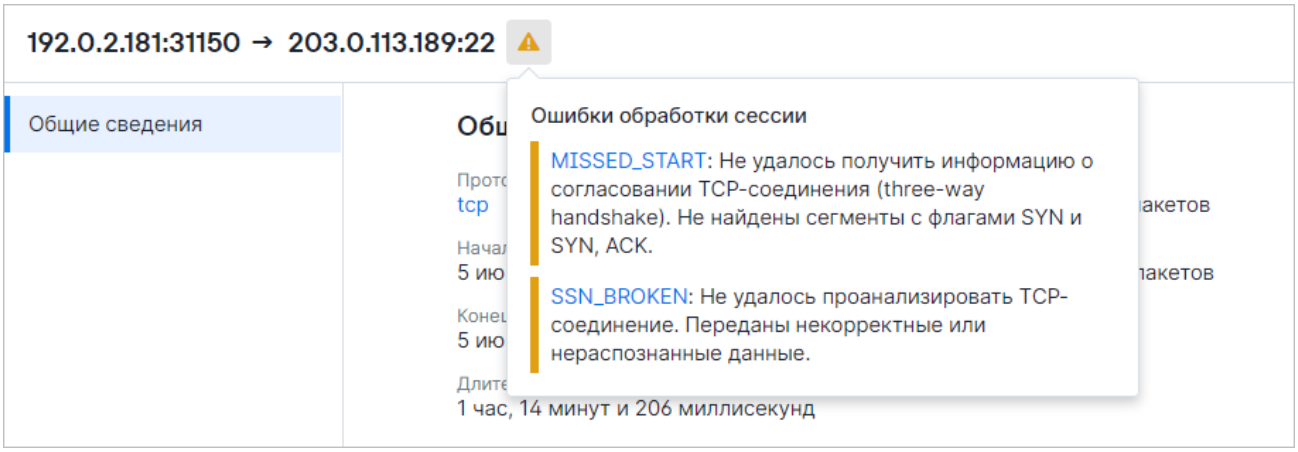


Рисунок 26. Стандартный режим просмотра флагов и ошибок обработки сессии

В экспертном режиме информация о флагах и ошибках отображается в карточке сразу при ее открытии.

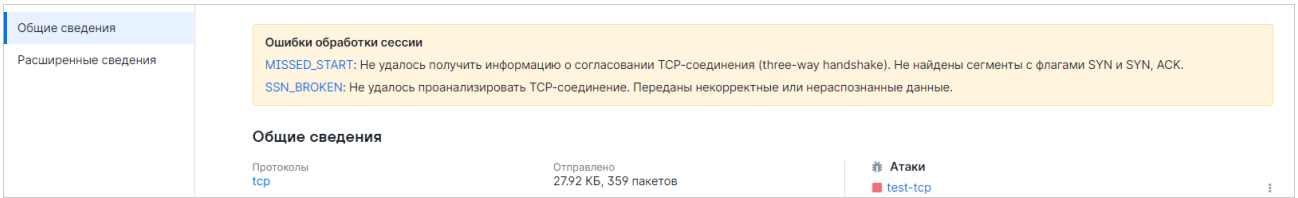


Рисунок 27. Экспертный режим просмотра флагов и ошибок обработки сессии

Вы можете включить экспертный режим, если активно используете флаги и ошибки для диагностики неполадок сетевого оборудования и исправления неправильной сетевой конфигурации.

- Чтобы включить экспертный режим просмотра:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. Включите показ расширенной информации в карточках сессий и атак.
  3. Нажмите **Сохранить**.

См. также

Флаги и ошибки обработки сессий (см. приложение E)

Включение показа расширенных данных сессии (см. раздел 9.3)

9.8. Просмотр обнаруженных DGA-доменов в таблице сессий

При обнаружении DGA-домена (см. раздел 2.3) PT NAD добавляет метку DGA в таблицу сессий в столбец **IOC**. Вы можете узнать, какие домены сгенерированы с использованием DGA, в деталях конкретной сессии.

- Чтобы посмотреть обнаруженный DGA-домен в таблице сессий:

  1. В главном меню выберите **Сессии**.
  2. В панели фильтрации (см. раздел 6.5) введите `rpt.type == "dga"` и нажмите клавишу Enter.

     В списке отобразятся только те сессии, в которых были обнаружены DGA-домены.

Примечание. Вы также можете использовать параметр фильтрации (см. раздел 13) `rpt.verdict` для поиска сессий с DGA-доменами по названию вредоносной программы, которая сгенерировала или использовала DGA-домен, например `rpt.verdict == "bebloh"`.

3. Откройте карточку сессии, нажав ↙↗ в строке этой сессии.

Метку DGA можно увидеть рядом с названиями доменов, например, в общих сведениях об отправителе и получателе или в деталях сетевых транзакций. Если PT NAD при обнаружении DGA-домена распознал вредоносную программу, которая использовала или сгенерировала этот домен, вы можете увидеть ее название рядом с меткой DGA.

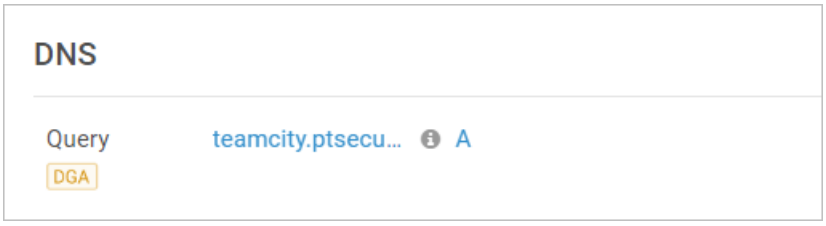


Рисунок 28. Метка DGA-домена и название вредоносной программы

9.9. Экспорт дампа трафика сессий в формате PCAP

Вы можете экспортировать исходную копию трафика в виде файла формата PCAP (дампа). Впоследствии вы можете использовать такие дампы для ретроспективного анализа и для импорта в другие системы.

Примечание. Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

- Чтобы экспортировать дамп трафика сессий:

1. В главном меню выберите **Сессии**.
2. Выберите сессии в таблице.

   Примечание. Вы можете выбрать несколько сессий, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных сессий (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
3. В панели инструментов выберите **Действия с выбранными** → **Скачать в формате PCAP**.

   PT NAD начнет формировать дамп трафика выбранных сессий. По завершении этого процесса появится сообщение «Дамп сформирован».
4. Нажмите **Скачать**.

   Файл с дампом будет сохранен браузером в папке по умолчанию.

Кроме того, дамп трафика одной сессии вы можете экспортировать из карточки сессии по кнопке **Скачать дамп**.

9.10. Копирование трафика сессий в формате PCAP в хранилище

Чтобы избежать переполнения дискового пространства, PT NAD удаляет старые данные из потоковых хранилищ. Новые PCAP-файлы с исходной копией трафика записываются поверх старых в зависимости от занятого ими места на диске. Чтобы не потерять нужный трафик, вы можете скопировать его в виде файла формата PCAP (дампа трафика) в выделенное хранилище.

При копировании трафика PT NAD повторно разбирает его (см. раздел 2.1.3). Поскольку одним из этапов разбора является поиск атак с использованием актуальной базы знаний, вы можете воспользоваться копированием, чтобы проверить наличие новых атак в ранее проанализированном трафике.

> **Примечание.** Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

- Чтобы скопировать дамп трафика сессий в хранилище:

  1. В главном меню выберите **Сессии**.
  2. Выберите сессии в таблице.

     Примечание. Вы можете выбрать несколько сессий, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных сессий (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **Отправить в хранилище**.
  4. Выберите хранилище или добавьте новое.
  5. Нажмите **Перенести**.

     PT NAD сформирует дамп трафика сессий, загрузит его в выбранное хранилище и выполнит разбор этого трафика (см. раздел 2.1.3) — за исключением поиска активностей, флуда и сканирования, а также сбора информации об узлах. По окончании загрузки PT NAD отобразит период, за который был загружен трафик.

Кроме того, дамп трафика одной сессии вы можете скопировать в хранилище из карточки сессии по кнопке **Отправить в хранилище**.

См. также

Работа с хранилищами (см. раздел 7)

Копирование трафика сессий с атаками в формате PCAP в хранилище (см. раздел 10.9)

9.11. Экспорт метаданных трафика сессий из PT NAD

Вы можете экспортировать метаданные трафика сессий в виде файлов JSON или CSV. Впоследствии вы можете использовать такие файлы для ретроспективного анализа и для импорта в другие продукты.

- Чтобы экспортировать файл с метаданными трафика сессий:

  1. В главном меню выберите **Сессии**.
  2. Выберите сессии в таблице.

     Примечание. Вы можете выбрать несколько сессий, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных сессий (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **JSON** (или **CSV**).

     PT NAD сформирует файл с метаданными трафика сессий, который будет сохранен браузером в папке по умолчанию.

9.12. Скачивание файлов, переданных в сессиях

При передаче информации от одного узла сети к другому среди прочего могут передаваться и файлы. Вы можете скачивать эти файлы на свой компьютер, чтобы продолжить их анализ в другой системе (например, в антивирусной программе).

Примечание. Вы можете скачивать не более 100 уникальных файлов за один раз.

Примечание. Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

- Чтобы скачать файлы, переданные в сессиях:

  1. В главном меню выберите **Сессии**.
  2. Выберите сессии, в которых передавались файлы.

     Примечание. Вы можете найти такие сессии, введя `files` в строке фильтрации и нажав клавишу Enter.

     Примечание. Вы можете выбрать несколько сессий, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных сессий (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **Скачать извлеченные файлы**.
  4. Выберите файлы для скачивания.

Примечание. Вы можете найти в списке нужный вам файл, введя в поле поиска его название или формат.

5. Нажмите **Скачать**.

   PT NAD начнет подготавливать архив с выбранными файлами. По завершении подготовки PT NAD уведомит о том, что архив готов к скачиванию.

6. При необходимости введите название для скачиваемого архива с выбранными файлами.

7. Нажмите **Скачать**.

   Браузер сохранит файлы в папке по умолчанию.

Кроме того, вы можете скачивать файлы, переданные в одной конкретной сессии, из карточки сессии по кнопке **Скачать файлы** или выбрав пункт **Скачать файл** в контекстном меню отдельного файла.

См. также

Скачивание файлов, переданных во время атак (см. раздел 10.11)

Категория виджетов Файлы (см. раздел A.9)

9.13. Получение ссылки на карточку сессии

Вы можете получить ссылку на карточку сессии и поделиться ею с любым человеком, у которого есть доступ к интерфейсу PT NAD. Вы также можете сохранить эту ссылку для себя, чтобы просмотреть информацию о сессии позднее.

- Чтобы получить ссылку на карточку сессии:

  1. В главном меню выберите **Сессии**.
  2. Откройте карточку сессии, нажав ⤢ в строке этой сессии.
  3. Нажмите **Скопировать ссылку**.

     Примечание. Вы также можете скопировать URL страницы из адресной строки браузера.

Ссылка на карточку сессии будет работать до тех пор, пока запись об этой сессии не будет удалена (см. раздел 7).

См. также

Получение ссылки на карточку атаки (см. раздел 10.13)

10. Работа с атаками

При разборе трафика (см. раздел 2.1.3) PT NAD регистрирует атаки — зафиксированные факты передачи информации между узлами, которые продукт рассматривает как целенаправленную угрозу информационной безопасности. Продукт обнаруживает атаки на основе правил (см. раздел 20.2) и в ходе выявления активностей (см. раздел 14).

Если правило сработало, PT NAD записывает информацию об обнаружении атаки или другого события ИБ в информационной инфраструктуре организации. Список срабатываний правил отображается на странице **Атаки**, доступной из одноименного раздела главного меню.

В этом разделе

10.1. Просмотр списка атак

- Чтобы просмотреть список атак,

  в главном меню выберите раздел **Атаки**.

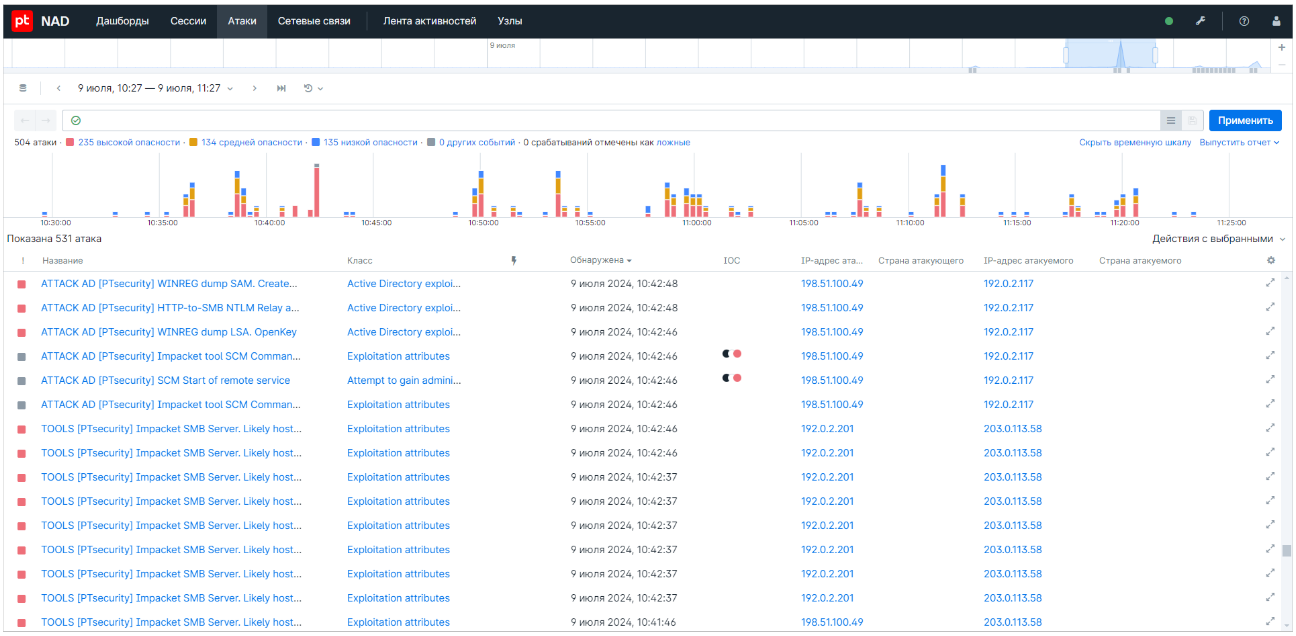


Рисунок 29. Просмотр списка атак

Вы можете фильтровать данные на странице с помощью диаграммы интенсивности трафика (см. раздел 6.3) и панели фильтрации (см. раздел 6.5).

Под панелью фильтрации находится сводная информация о количестве атак и других событий ИБ за период, выбранный на диаграмме интенсивности трафика.

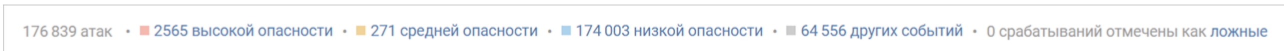


Рисунок 30. Просмотр сводной информации об атаках

Информация в строке также соответствует примененным параметрам фильтрации.

По умолчанию в таблице атак отображаются столбцы:

— **!** — уровень опасности атаки или другого события ИБ; если в записи была добавлена отметка о ложном срабатывании правила (см. раздел 10.12.1), значок уровня опасности зачеркнут.

— **Название** — название правила (см. раздел 20.2), по срабатыванию которого была сгенерирована запись; если в записи была добавлена отметка о ложном срабатывании (см. раздел 10.12.1), название зачеркнуто.

— **Класс** — класс атаки или другого события ИБ.

— **Риск эксплуатации** (⚡) — информация о риске эксплуатации уязвимости, полученная от MaxPatrol 10 (при настроенной интеграции с этим продуктом).

— **Обнаружена** — дата и время срабатывания правила (см. раздел 20.2).

- **Дочерняя система** — метка дочерней системы (см. раздел 8), из которой получены данные о трафике. Отображается в интерфейсе центральной консоли (см. раздел 2.4) для экземпляров PT NAD, объединенных в иерархию.
- **IOC** — обнаруженные индикаторы компрометации (см. раздел A.6).
- **IP-адрес атакующего** — IP-адрес узла, который является источником атаки.
- **Страна атакующего** — страна, в которой находится узел, являющийся источником атаки.
- **IP-адрес атакуемого** — IP-адрес узла, который является целью атаки.
- **Страна атакуемого** — страна, в которой находится узел, являющийся целью атаки.

По умолчанию срабатывания правил в таблице отсортированы по времени обнаружения (недавно обнаруженные срабатывания отображаются выше).

Более светлые строки в таблице содержат информацию о ложных срабатываниях правил (см. раздел 10.12).

В таблице атак вы можете:

- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- изменять набор столбцов (см. раздел 10.4).

Параметры таблицы сохраняются для вашей учетной записи при переходе на другие страницы или выходе из продукта.

Вы можете восстановить состояние таблицы по умолчанию, нажав **Восстановить по умолчанию** во всплывающем окне со списком столбцов.

Из таблицы вы можете получать подробную информацию об IP-адресах, доменах и идентификаторах узлов. Если узел известен продукту (см. раздел 15), то вы можете просмотреть сводку об этом узле (см. раздел 15.3). Если IP-адрес или домен относятся к неизвестному узлу, то вы можете перейти к просмотру статистики по этому IP-адресу или домену на дашбордах (см. раздел 17.1), а также получить информацию о них на внешних ресурсах (см. раздел 17.2).

10.2. Просмотр подробной информации об атаке

В таблице на странице **Атаки** отображается краткая информация об атаках. Подробная информация о каждой атаке отображается в карточке атаки (см. рисунок 31).

Чтобы просмотреть подробную информацию об атаке:

1. В главном меню выберите **Атаки**.
2. Откройте карточку атаки по кнопке ↙↗ в строке этой атаки.

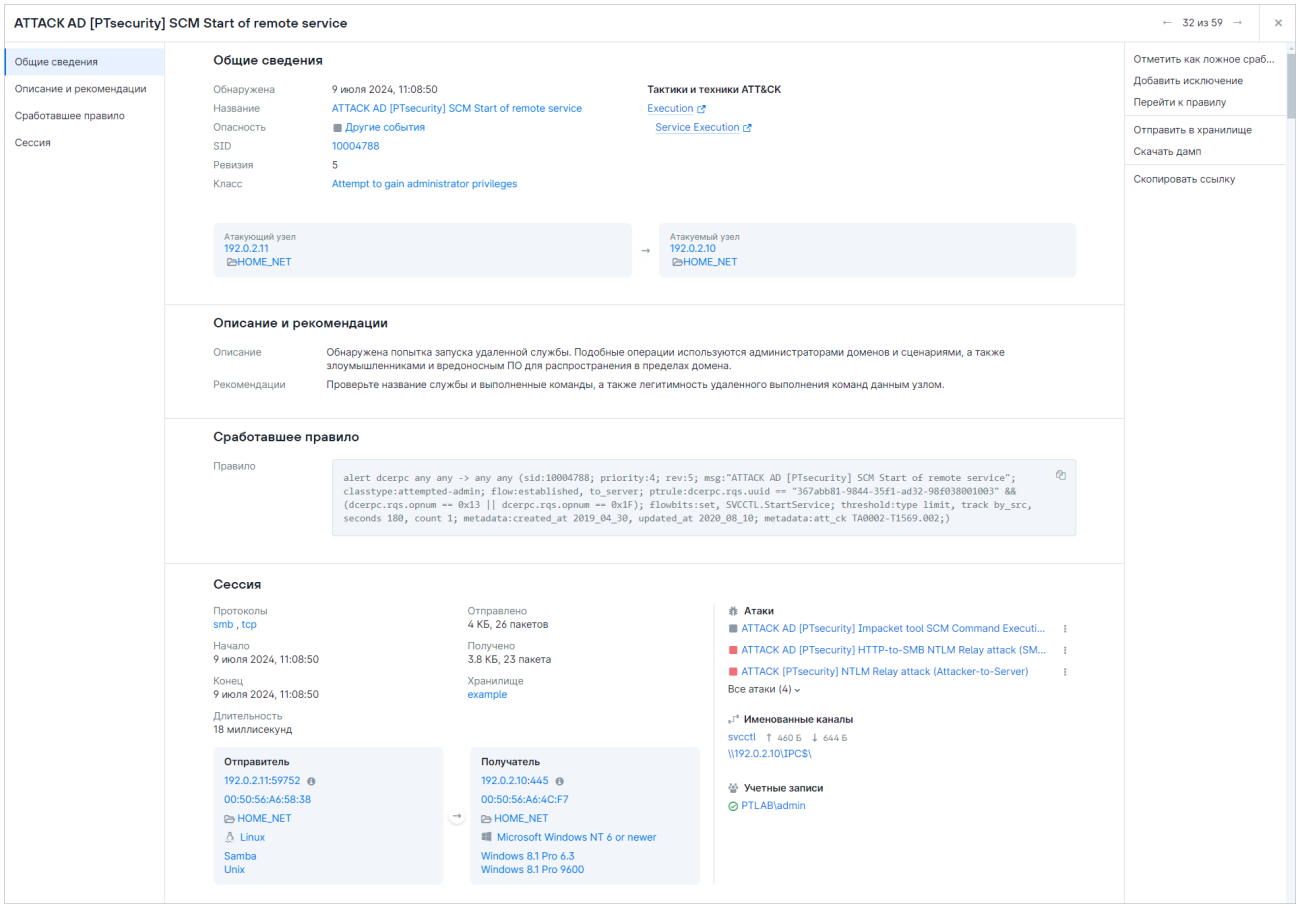


Рисунок 31. Карточка атаки

В карточке атаки отображается информация о правиле (см. раздел 20.2), по срабатыванию которого PT NAD создал запись об атаке. Вендор может поставлять вместе с самим правилом информацию об атаках, которые оно обнаруживает. Эта информация отображается в разделе **Описание и рекомендации** карточки атаки и может включать в себя:

— описание уязвимости, эксплуатируемой злоумышленниками для совершения атаки;

— наименование ПО, используемого для совершения атаки;

— последовательность действий злоумышленников;

— рекомендации для операторов при обнаружении атаки;

— ссылки на описание атаки в базах знаний CVE, Securelist и других.

Вендор правила также может предоставлять информацию о действиях злоумышленников и методах, используемых ими при совершении атаки. Вы можете просмотреть эту информацию по ссылкам в блоке **Тактики и техники ATT&CK** раздела **Общие сведения**.

Вы можете просмотреть правило, по срабатыванию которого PT NAD создал запись об атаке, в поле **Правило** раздела **Сработавшее правило**. В этом поле приводится версия правила на момент срабатывания; она может отличаться от последней версии, доступной в карточке правила. Сегмент трафика сессии, при анализе которого произошло срабатывание правила, отображается в поле **Payload**.

Если PT NAD обнаружил атаку с помощью правила обнаружения аномалий, вместо раздела **Сработавшее правило** отображается раздел **Причина срабатывания**.

Рисунок 32. Причина срабатывания

В разделе **Причина срабатывания** отображается та часть метаданных сессии, которая привела к генерации записи об атаке.

> **Примечание.** PT NAD может обнаружить атаку в ходе детектирования опасной или потенциально опасной активности. В таких случаях (если атака не связана с флудом, сканированиями и ICMP-туннелями) из карточки атаки вы можете перейти к карточке правила для активности, связанной с этой атакой.

Если вы находитесь в интерфейсе центральной консоли (см. раздел 2.4), то в названии карточки отображаются название и метка дочерней системы, которая обнаружила атаку. Вы можете перейти к карточке атаки или к карточке правила в этой системе, используя соответствующие кнопки **Перейти в дочерний NAD** и **Перейти к правилу**. В новой вкладке браузера в интерфейсе дочерней системы откроется карточка этой же атаки или правила, по срабатыванию которого сгенерирована карточка.

- Чтобы просмотреть подробную информацию о следующей атаке, показанной в таблице, нажмите →.
- Чтобы просмотреть подробную информацию о предыдущей атаке, показанной в таблице, нажмите ←.
- Чтобы закрыть карточку, нажмите ×.

10.3. Просмотр распределения атак по времени

PT NAD позволяет просматривать распределение атак по времени на диаграмме. Это может быть полезно для выявления закономерностей (например, всплеск числа атак в определенные дни) при расследовании инцидентов ИБ.

- Чтобы просмотреть распределение атак по времени:

  1. В главном меню выберите **Атаки**.

     Откроется страница **Атаки**. Распределение атак по времени отобразится на диаграмме под строкой со сводной информацией об атаках (см. раздел 10.1).

     Примечание. На диаграмме атаки сгруппированы по времени и уровню опасности. При наведении курсора на диаграмму отображаются дата, время, количество атак и уровни их опасности.

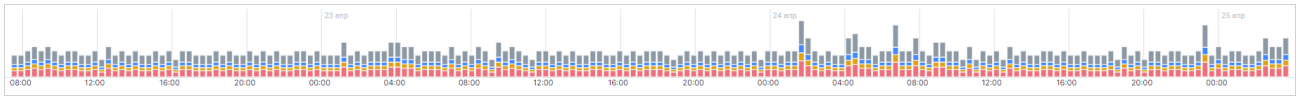


Рисунок 33. Просмотр распределения атак по времени на диаграмме атак

  2. Если вам нужно детализировать период распределения атак, выделите интересующий период на диаграмме атак.

     На диаграмме атак отобразятся значения за уточненный период. Список атак в таблице (см. раздел 10.1) будет также отфильтрован в соответствии с новым периодом.

Вы можете управлять отображением диаграммы на странице с помощью кнопки **Скрыть временную шкалу** или **Показать временную шкалу** под панелью фильтрации (см. раздел 6.5).

10.4. Изменение набора столбцов в таблице атак

- Чтобы изменить набор столбцов в таблице:

  1. В главном меню выберите **Атаки**.
  2. По кнопке ⚙ откройте всплывающее окно со списком столбцов.
  3. Установите флажки напротив названий столбцов, которые нужно отображать в таблице.
  4. Нажмите в любом месте за пределами всплывающего окна.

10.5. Фильтрация атак по периоду

По умолчанию при входе в PT NAD в рабочей области на странице **Атаки** отображаются данные за последний час. Вы можете изменить период фильтрации данных.

- Чтобы отфильтровать атаки по периоду:

  1. В главном меню выберите **Атаки**.
  2. Нажмите на период для фильтрации.

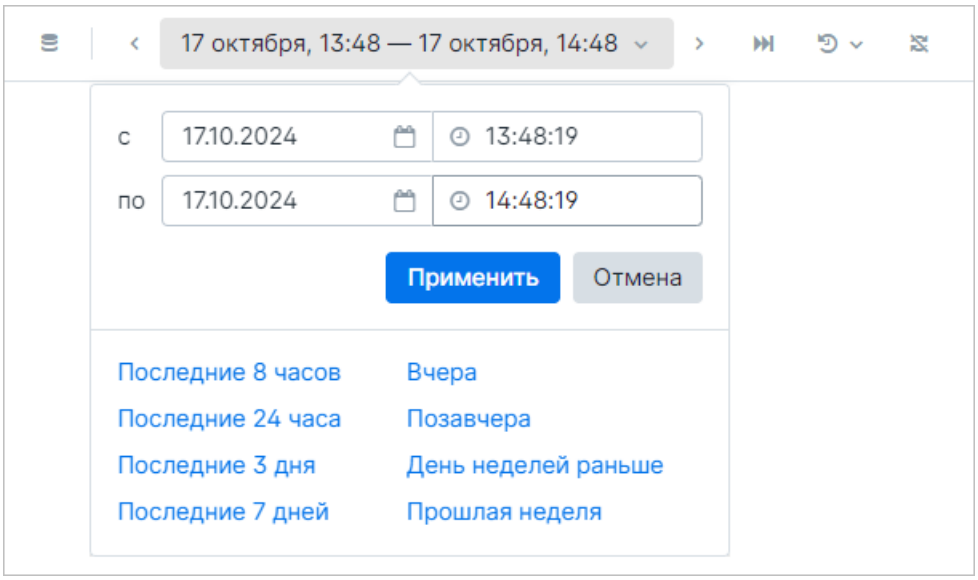


Рисунок 34. Настройка периода фильтрации данных

  3. Укажите период и нажмите **Применить**.

- Чтобы сместить период на половину его длины влево,

  нажмите < .

- Чтобы сместить период на половину его длины вправо,

  нажмите > .

Вы также можете детализировать период фильтрации данных, выделяя с помощью курсора интервал на диаграмме интенсивности трафика (см. раздел 6.3) и диаграмме атак (см. раздел 10.3).

Кроме того, вы можете выбрать один из ранее установленных периодов фильтрации, нажав .

- Чтобы вернуть период по умолчанию (данные за последний час),

  нажмите .

10.6. Фильтрация атак по метаданным трафика

Вы можете фильтровать список зарегистрированных атак по метаданным трафика. Например, вы можете найти атаки, в ходе которых узел 198.51.100.13 передавал файлы, определенные как опасные по результатам поведенческого анализа в PT Sandbox. Для этого требуется применить фильтр с набором условий.

- Чтобы отфильтровать атаки по метаданным трафика:

1. В главном меню выберите **Атаки**.
2. В панели фильтрации (см. раздел 6.5) добавьте условия одним из способов:
   - Введите параметры для фильтрации, значения параметров и операторы на языке фильтрации продукта (см. приложение Б).

     Примечание. Вы можете просмотреть полный список доступных параметров для фильтрации, нажав комбинацию клавиш Ctrl+Space в строке фильтрации.

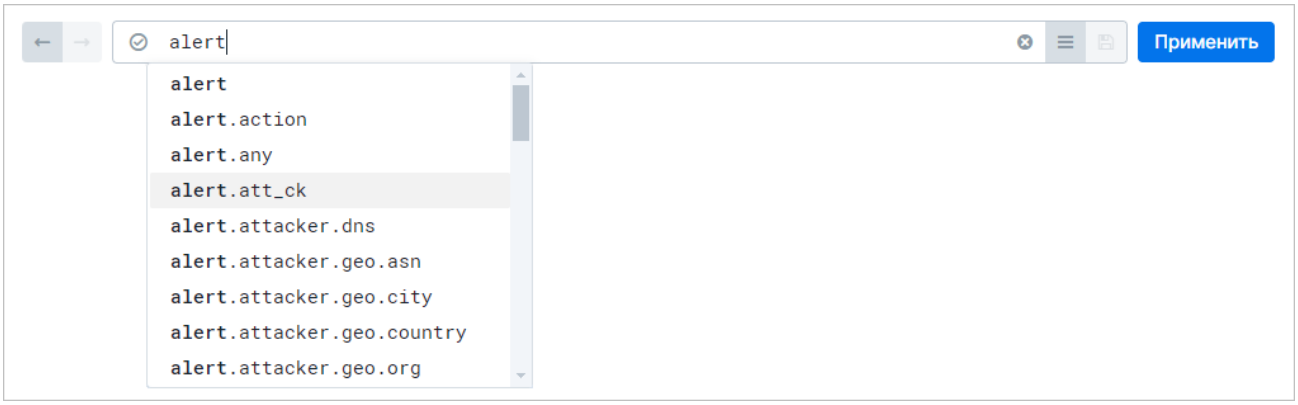


Рисунок 35. Ввод параметров фильтрации

При вводе параметров в строке фильтрации вы можете выбрать их значения из списка (только строковые и булевы). Значения собираются из метаданных трафика, отфильтрованного по периоду.

Рисунок 36. Выбор значений параметров фильтрации

   - Добавьте параметры фильтрации с их значениями по ссылкам в таблице атак.
3. Нажмите **Применить**.

Добавленные условия фильтрации можно сохранить, чтобы не указывать их снова в дальнейшем. Для этого нужно создать личный (см. раздел 13.1) или общий фильтр (см. раздел 13.2).

Вы можете просматривать историю примененных вами фильтров по нажатию ← и →. PT NAD хранит в истории 100 последних фильтров.

Кроме того, вы можете добавлять метаданные трафика в строку фильтрации по ссылкам в карточке атаки (см. раздел 10.2).

10.7. Просмотр обнаруженных DGA-доменов в таблице атак

При обнаружении DGA-домена (см. раздел 2.3) PT NAD добавляет метку DGA в таблицу атак в столбец **IOC**. Вы можете узнать, какие домены сгенерированы с использованием DGA, в деталях конкретной атаки.

- Чтобы посмотреть обнаруженный DGA-домен в таблице атак:

  1. В главном меню выберите **Атаки**.
  2. В панели фильтрации (см. раздел 6.5) введите `rpt.type == "dga"` и нажмите клавишу Enter.

     В списке отобразятся только те атаки, в которых были обнаружены DGA-домены.

     Примечание. Вы также можете использовать параметр фильтрации (см. раздел 13) `rpt.verdict` для поиска атак с DGA-доменами по названию вредоносной программы, которая сгенерировала или использовала DGA-домен, например `rpt.verdict == "bebloh"`.
  3. Откройте карточку атаки по кнопке ↙↗ в строке этой атаки.

Метку DGA можно увидеть рядом с названиями доменов, например, в общих сведениях об отправителе и получателе или в деталях сетевых транзакций. Если PT NAD при обнаружении DGA-домена распознал вредоносную программу, которая использовала или сгенерировала этот домен, вы можете увидеть ее название рядом с меткой DGA.

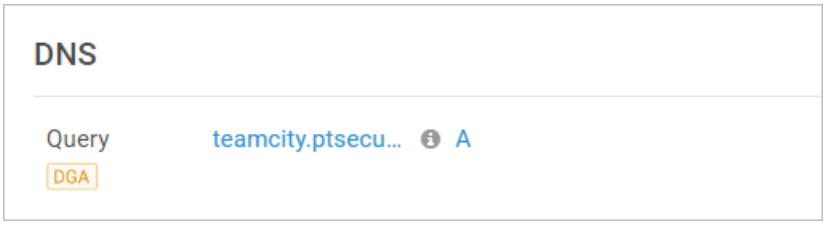


Рисунок 37. Метка DGA-домена и название вредоносной программы

10.8. Экспорт дампа трафика с атаками в формате PCAP

Вы можете экспортировать исходную копию трафика в виде файла формата PCAP (дампа). Впоследствии вы можете использовать такие дампы для ретроспективного анализа и для импорта в другие системы.

> **Примечание.** Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

- Чтобы экспортировать дамп трафика с атаками:

  1. В главном меню выберите **Атаки**.
  2. Выберите атаки в таблице.

     Примечание. Вы можете выбрать несколько атак, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных атак (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **Скачать в формате PCAP**.

     PT NAD начнет формировать дамп трафика выбранных атак. По завершении этого процесса появится сообщение «Дамп сформирован».
  4. Нажмите **Скачать**.

     Файл с дампом будет сохранен браузером в папке по умолчанию.

Кроме того, дамп вы можете экспортировать из карточки атаки по кнопке **Скачать дамп**.

10.9. Копирование трафика сессий с атаками в формате PCAP в хранилище

Чтобы избежать переполнения дискового пространства, PT NAD удаляет старые данные из потоковых хранилищ. Новые PCAP-файлы с исходной копией трафика записываются поверх старых в зависимости от занятого ими места на диске. Чтобы не потерять нужный трафик, вы можете скопировать его в виде файла формата PCAP (дампа трафика) в выделенное хранилище.

При копировании трафика PT NAD повторно разбирает его (см. раздел 2.1.3). Поскольку одним из этапов разбора является поиск атак с использованием актуальной базы знаний, вы можете воспользоваться копированием, чтобы проверить наличие новых атак в ранее проанализированном трафике.

> **Примечание.** Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

- Чтобы скопировать в хранилище дамп трафика сессий с обнаруженными атаками:

  1. В главном меню выберите **Атаки**.
  2. Выберите атаки в таблице.

     Примечание. Вы можете выбрать несколько атак, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных атак (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **Отправить в хранилище**.
  4. Выберите хранилище или добавьте новое.
  5. Нажмите **Перенести**.

     PT NAD сформирует дамп трафика сессий, загрузит его в выбранное хранилище и выполнит разбор этого трафика (см. раздел 2.1.3) — за исключением поиска активностей, флуда и сканирования, а также сбора информации об узлах. По окончании загрузки PT NAD отобразит период, за который был загружен трафик.

Кроме того, дамп трафика сессии с атакой вы можете скопировать в хранилище из карточки этой атаки по кнопке **Отправить в хранилище**.

См. также

Работа с хранилищами (см. раздел 7)

Копирование трафика сессий в формате PCAP в хранилище (см. раздел 9.10)

10.10. Экспорт метаданных трафика с атаками из PT NAD

Вы можете экспортировать метаданные трафика сессий в виде файлов JSON или CSV. Впоследствии вы можете использовать такие файлы для ретроспективного анализа и для импорта в другие продукты.

- Чтобы экспортировать файл с метаданными трафика сессий, содержащих атаки:

  1. В главном меню выберите **Атаки**.
  2. Выберите атаки в таблице.

     Примечание. Вы можете выбрать несколько атак, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных атак (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
  3. В панели инструментов выберите **Действия с выбранными** → **JSON** (или **CSV**).

     PT NAD сформирует файл с метаданными трафика сессий, содержащих атаки. Файл будет сохранен браузером в папке по умолчанию.

10.11. Скачивание файлов, переданных во время атак

При передаче информации от одного узла сети к другому среди прочего могут передаваться и файлы. Вы можете скачивать эти файлы на свой компьютер, чтобы продолжить их анализ в другой системе (например, в антивирусной программе).

Примечание. Вы можете скачивать не более 100 уникальных файлов за один раз.

Примечание. Описанная в этом разделе возможность отсутствует в версии PT NAD Sensor (см. раздел 2.5), а также в интерфейсе центральной консоли для экземпляров PT NAD, объединенных в иерархию.

► Чтобы скачать файлы, переданные во время атак:

1. В главном меню выберите **Атаки**.
2. Выберите атаки, во время которых передавались файлы.

   Примечание. Вы можете найти такие атаки, введя `files` в строке фильтрации и нажав клавишу Enter.

   Примечание. Вы можете выбрать несколько атак, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных атак (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.
3. В панели инструментов выберите **Действия с выбранными** → **Скачать извлеченные файлы**.
4. Выберите файлы для скачивания.

   Примечание. Вы можете найти в списке нужный вам файл, введя в поле поиска его название или формат.
5. Нажмите кнопку **Скачать**.

   PT NAD начнет подготавливать архив с выбранными файлами. По завершении подготовки PT NAD уведомит о том, что архив готов к скачиванию.
6. При необходимости введите название для скачиваемого архива с выбранными файлами.

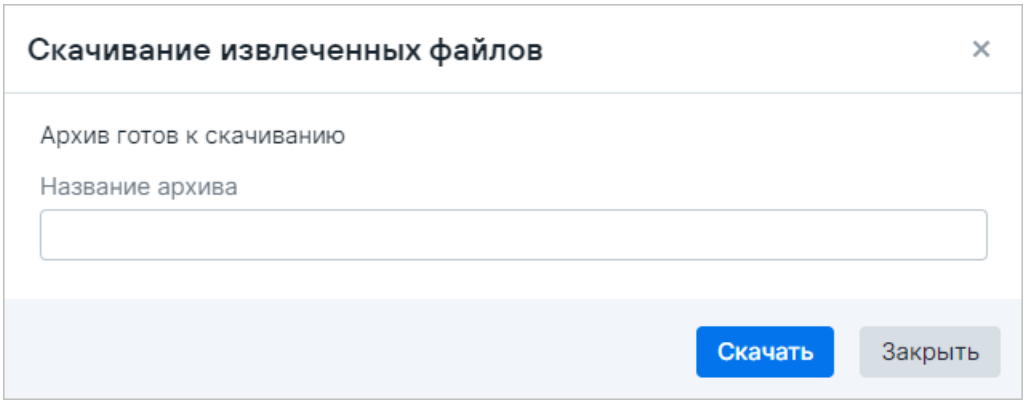


Рисунок 38. Скачивание файлов, переданных во время атак

7. Нажмите кнопку **Скачать**.

   Браузер сохранит файлы в папке по умолчанию.

Кроме того, вы можете скачивать файлы, переданные во время одной конкретной атаки, из карточки атаки по кнопке **Скачать файлы** или по кнопке напротив отдельного файла.

См. также

Скачивание файлов, переданных в сессиях (см. раздел 9.12)

Категория виджетов Файлы (см. раздел A.9)

10.12. Работа с ложными срабатываниями правил для обнаружения атак

При анализе атак вы можете отмечать в интерфейсе PT NAD те атаки, записи о которых были сгенерированы вследствие ложных срабатываний правил (см. раздел 20.2). В дальнейшем вы можете фильтровать (см. раздел 13) список атак по этому свойству, например чтобы собирать статистику атак без учета ложных срабатываний.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В информации о трафике за выбранный вами период количество срабатываний правил, которые были отмечены как ложные, отображается на странице **Атаки** под панелью фильтрации.

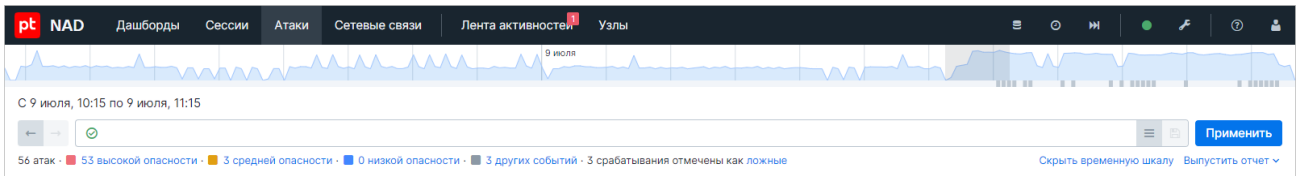


Рисунок 39. Просмотр информации о количестве ложных срабатываний правил

В этом разделе

Добавление отметки о ложном срабатывании правила (см. раздел 10.12.1)

Снятие отметки о ложном срабатывании правила (см. раздел 10.12.2)

См. также

Работа со справочниками (см. раздел 20.4)

10.12.1. Добавление отметки о ложном срабатывании правила

Вы можете отметить одну или несколько записей об атаках, которые были сгенерированы вследствие ложного срабатывания правила. При добавлении отметки вы можете ввести свой комментарий о причинах отметки. Введенный комментарий будет виден другим пользователям PT NAD и может использоваться при фильтрации (см. раздел 13).

- Чтобы отметить ложное срабатывание правила:

1. В главном меню выберите **Атаки**.
2. Выберите записи об атаках, которые были сгенерированы вследствие ложного срабатывания правила.
3. В панели инструментов нажмите кнопку **Действия с выбранными** и в раскрывшемся меню выберите пункт **Отметить как ложное срабатывание** или **Отметить как ложные срабатывания**.

   Примечание. Вы можете добавить к отметке комментарий в окне подтверждения (например, о причинах ложного срабатывания).

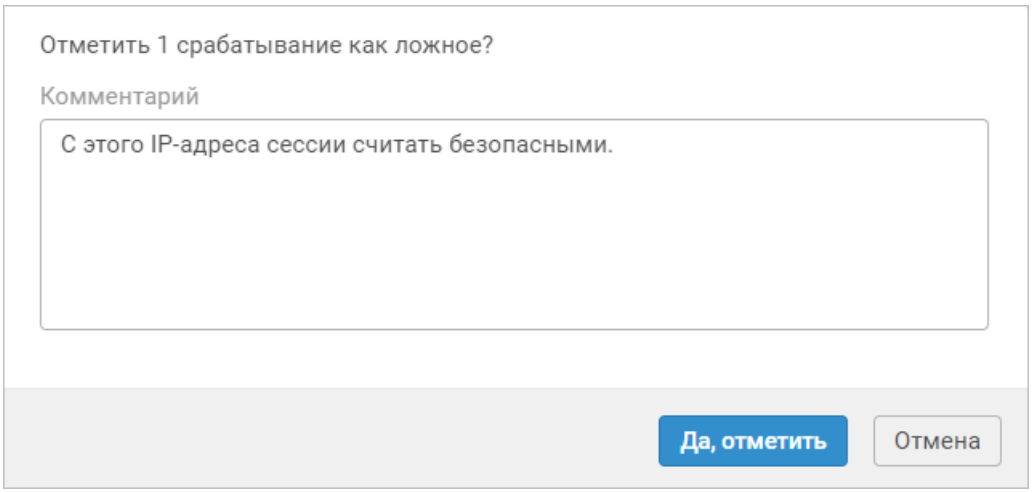


Рисунок 40. Ввод комментария о причинах отметки

4. Нажмите кнопку **Да, отметить**.

В таблице обнаружений (см. раздел 10.1) строки с выбранными атаками станут более светлыми. В карточке каждой такой атаки (см. раздел 10.2) появится блок с отметкой о ложном срабатывании правила.

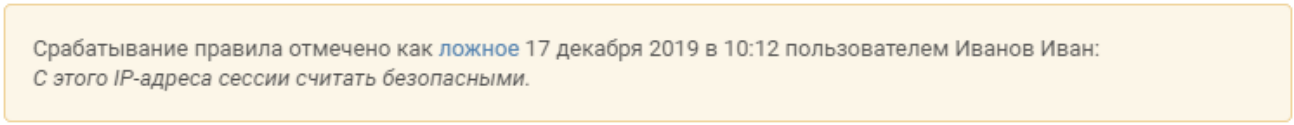


Рисунок 41. Просмотр отметки о ложном срабатывании правила

Срабатывание правила отмечено как ложное.

Вы также можете отметить ложное срабатывание правила в карточке атаки (см. раздел 10.2) по кнопке **Отметить как ложное срабатывание** или в карточке сессии (см. раздел 9.2), в ходе которой произошла атака, выбрав пункт **Отметить как ложное срабатывание** в контекстном меню блока с информацией об атаке.

Вы можете снимать добавленные отметки.

10.12.2. Снятие отметки о ложном срабатывании правила

Вы можете снять отметку о ложном срабатывании правила с одной или нескольких атак, если эти отметки были добавлены по ошибке.

- Чтобы снять отметки о ложном срабатывании правила:

  1. В главном меню выберите **Атаки**.
  2. Выберите атаки, с которых вы хотите снять отметки.
  3. В панели инструментов нажмите кнопку **Действия с выбранными**, в раскрывшемся меню выберите пункт **Снять отметку о ложном срабатывании** или **Снять отметки о ложном срабатывании** и подтвердите снятие.

  Отметки о ложном срабатывании правила сняты.

Вы также можете снять отметку в карточке атаки (см. раздел 10.2) по кнопке **Снять отметку о ложном срабатывании** или в карточке сессии (см. раздел 9.2), в ходе которой произошла атака, выбрав пункт **Снять отметку о ложном срабатывании** в контекстном меню блока с информацией об атаке.

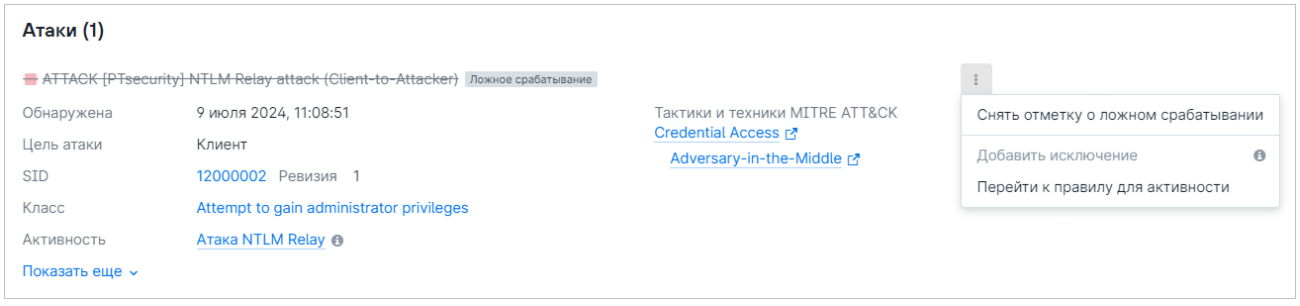


Рисунок 42. Снятие отметки о ложном срабатывании

10.13. Получение ссылки на карточку атаки

Вы можете получить ссылку на карточку атаки и поделиться ею с любым человеком, у которого есть доступ к интерфейсу PT NAD. Вы также можете сохранить эту ссылку для себя, чтобы просмотреть информацию об атаке позднее.

- Чтобы получить ссылку на карточку атаки:

  1. В главном меню выберите **Атаки**.
  2. Откройте карточку атаки по кнопке  в строке этой атаки.
  3. Нажмите **Скопировать ссылку**.

     Примечание. Вы также можете скопировать URL страницы из адресной строки браузера.

Ссылка на карточку атаки будет работать до тех пор, пока запись об этой атаке не будет удалена (см. раздел 7).

См. также

Получение ссылки на карточку сессии (см. раздел 9.13)

11. Работа с дашбордами и виджетами

Вы можете просматривать статистические данные о трафике в сети организации в наглядном представлении с помощью графических модулей — виджетов. Виджеты отображаются на странице **Дашборды**.

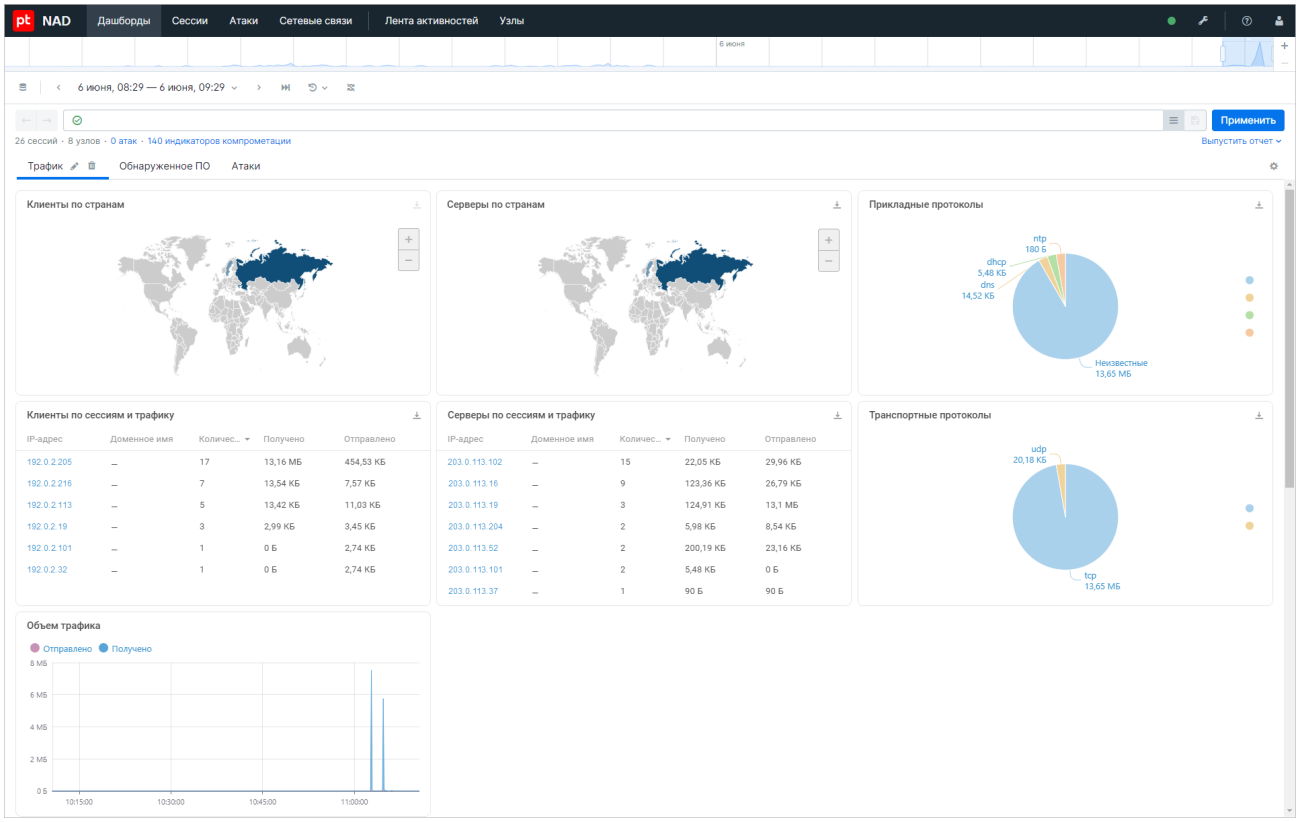


Рисунок 43. Просмотр статистических данных на странице **Дашборды**

Для группировки виджетов используются дашборды. По умолчанию виджеты разнесены по дашбордам **Трафик**, **Обнаруженное ПО** и **Атаки**.

Вы можете:

— управлять дашбордами — изменять состав виджетов на них, переименовывать, создавать и удалять;

— использовать системные виджеты (см. приложение А), которые поставляются с продуктом, и пользовательские виджеты (см. раздел 11.8);

— фильтровать данные на странице с помощью диаграммы интенсивности трафика (см. раздел 6.3) и панели фильтрации (см. раздел 6.5).

Под панелью фильтрации находится строка со сводной информацией о количестве сессий, узлов, атак и индикаторов компрометации (см. раздел 2.1.4) за период, выбранный на диаграмме интенсивности трафика.

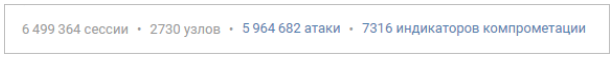


Рисунок 44. Сводная информация об объектах в трафике

Информация в строке также соответствует примененным параметрам фильтрации.

Под строкой со сводной информацией в рабочей области располагаются дашборды, содержащие в себе виджеты.

В этом разделе

Фильтрация данных на дашбордах по периоду (см. раздел 11.1)

Фильтрация данных на дашбордах по метаданным трафика (см. раздел 11.2)

Включение автообновления данных на дашбордах (см. раздел 11.3)

Добавление виджетов на дашборд (см. раздел 11.4)

Удаление виджета с дашборда (см. раздел 11.5)

Изменение максимального количества записей в виджете (см. раздел 11.6)

Экспорт данных виджета (см. раздел 11.7)

Управление пользовательскими виджетами (см. раздел 11.8)

Управление дашбордами (см. раздел 11.9)

См. также

Системные виджеты в PT NAD (см. приложение А)

11.1. Фильтрация данных на дашбордах по периоду

По умолчанию при входе в PT NAD в рабочей области на странице **Дашборды** отображаются данные за последний час. Вы можете изменить период фильтрации данных.

- Чтобы отфильтровать данные на дашбордах по периоду:

  1. В главном меню выберите раздел **Дашборды**.
  2. Нажмите на период для фильтрации.

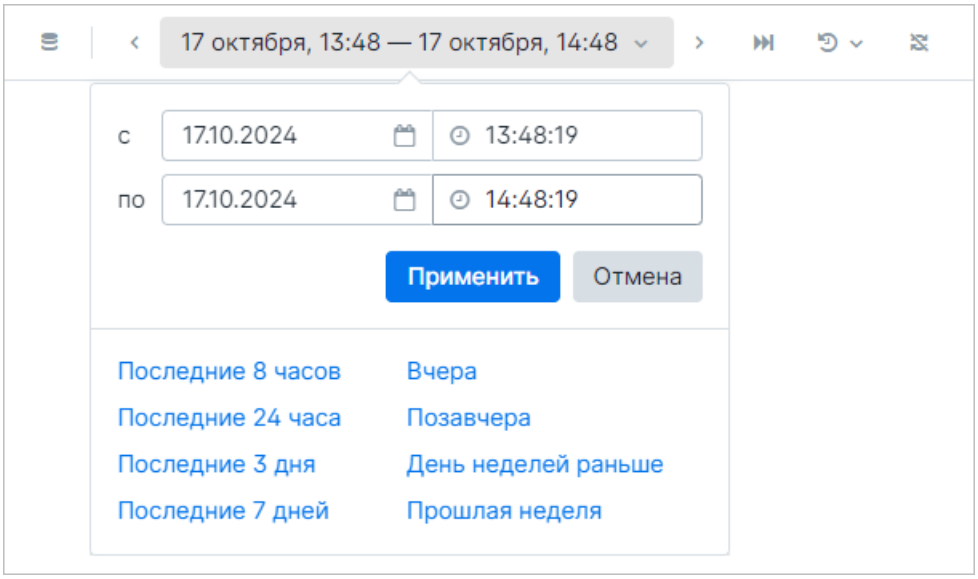


Рисунок 45. Настройка периода фильтрации данных

3. Укажите период и нажмите **Применить**.

- Чтобы сместить период на половину его длины влево,

  нажмите < .

- Чтобы сместить период на половину его длины вправо,

  нажмите > .

Вы также можете детализировать период фильтрации данных, выделяя с помощью курсора интервал на диаграмме интенсивности трафика (см. раздел 6.3).

Кроме того, вы можете выбрать один из ранее установленных периодов фильтрации, нажав .

- Чтобы вернуть период по умолчанию (данные за последний час),

  нажмите .

11.2. Фильтрация данных на дашбордах по метаданным трафика

Вы можете фильтровать данные на дашбордах по метаданным трафика. Например, вы можете посмотреть наглядную статистику по DNS-запросам на картах. Для этого требуется применить фильтр с набором условий.

► Чтобы отфильтровать данные на дашбордах по метаданным трафика:

1. В главном меню выберите раздел **Дашборды**.
2. В панели фильтрации (см. раздел 6.5) добавьте условия одним из способов:
   - Введите параметры для фильтрации, значения параметров и операторы на языке фильтрации продукта (см. приложение Б).

     Примечание. Вы можете просмотреть полный список доступных параметров для фильтрации, нажав комбинацию клавиш Ctrl+Space в строке фильтрации.

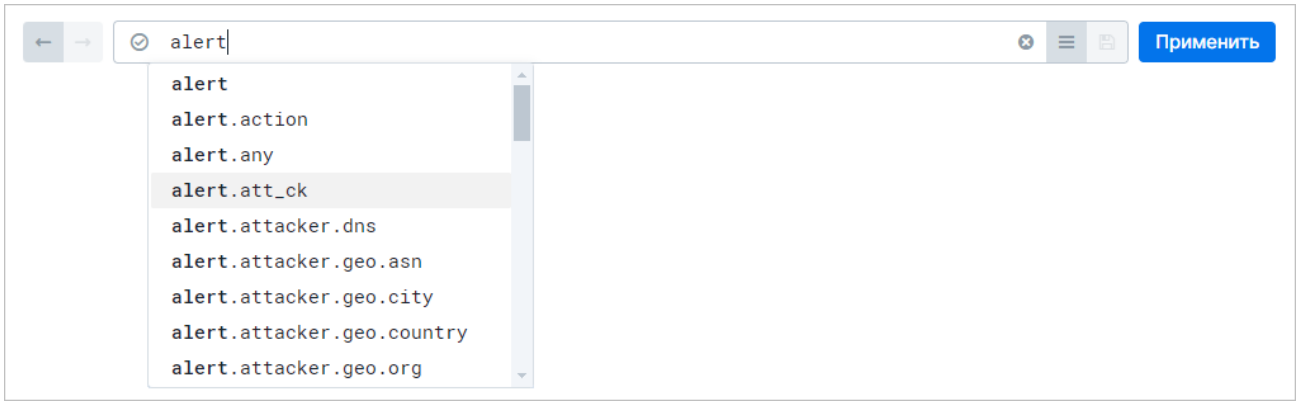


Рисунок 46. Ввод параметров фильтрации

При вводе параметров в строке фильтрации вы можете выбрать их значения из списка (только строковые и булевы). Значения собираются из метаданных трафика, отфильтрованного по периоду.

Рисунок 47. Выбор значений параметров фильтрации

   - Добавьте параметры фильтрации с их значениями по ссылкам на виджетах.
3. Нажмите **Применить**.

Добавленные условия фильтрации можно сохранить, чтобы не указывать их снова в дальнейшем. Для этого нужно создать личный (см. раздел 13.1) или общий фильтр (см. раздел 13.2).

Вы можете просматривать историю примененных вами фильтров по нажатию ← и →. PT NAD хранит в истории 100 последних фильтров.

11.3. Включение автообновления данных на дашбордах

Иногда требуется долго следить за изменениями в трафике с помощью PT NAD. Чтобы делать это было удобнее, вы можете включить автоматическое обновление данных на дашбордах. Частота обновления зависит от выбранного вами периода фильтрации данных (см. раздел 9.5).

Таблица 2. Частота автообновления данных на дашбордах

Период фильтрации	Частота автообновления
Короче 24 часов	Каждые 5 минут
От 24 часов до 7 дней	Каждые 10 минут
От 7 дней и дольше	Каждые 30 минут

Перед выполнением инструкции вам нужно убедиться, что для показа данных на дашбордах выбрано потоковое хранилище (см. раздел 7).

- Чтобы включить автообновление данных на дашбордах:

  1. В главном меню выберите раздел **Дашборды**.
  2. Если требуется, скорректируйте фильтрацию по периоду (см. раздел 9.5), настроив показ данных за желаемый период.

     Примечание. Если вы укажете период, который заканчивается в прошлом, то при каждом автообновлении PT NAD будет сдвигать выбранный период на время, равное частоте автообновления. Например, если вы выбрали период с 7:00 до 9:00 прошлого дня, то при следующем автообновлении PT NAD изменит период на 7:05—9:05 прошлого дня.

  3. Над панелью фильтрации нажмите  .

  Автообновление данных на дашбордах включено.

Помимо данных на дашбордах, PT NAD также автоматически обновляет числа в строке сводной информации (см. раздел 11) под панелью фильтрации.

Вы можете выключить автообновление над панелью фильтрации. Автообновление также выключается, когда вы переходите на другую страницу интерфейса, выбираете для показа данных только выделенные хранилища, переходите по ссылкам из уведомлений, завершаете работу из-под своей учетной записи, закрываете браузер или вкладку с интерфейсом PT NAD.

11.4. Добавление виджетов на дашборд

- Чтобы добавить виджеты на дашборд:

  1. В главном меню выберите раздел **Дашборды**.
  2. Выберите дашборд.

3. В панели инструментов нажмите ⚙.

   Появятся кнопки управления дашбордами и виджетами.

4. В панели инструментов нажмите кнопку **Добавить виджеты**.

   Откроется окно **Добавление виджетов на дашборд**.

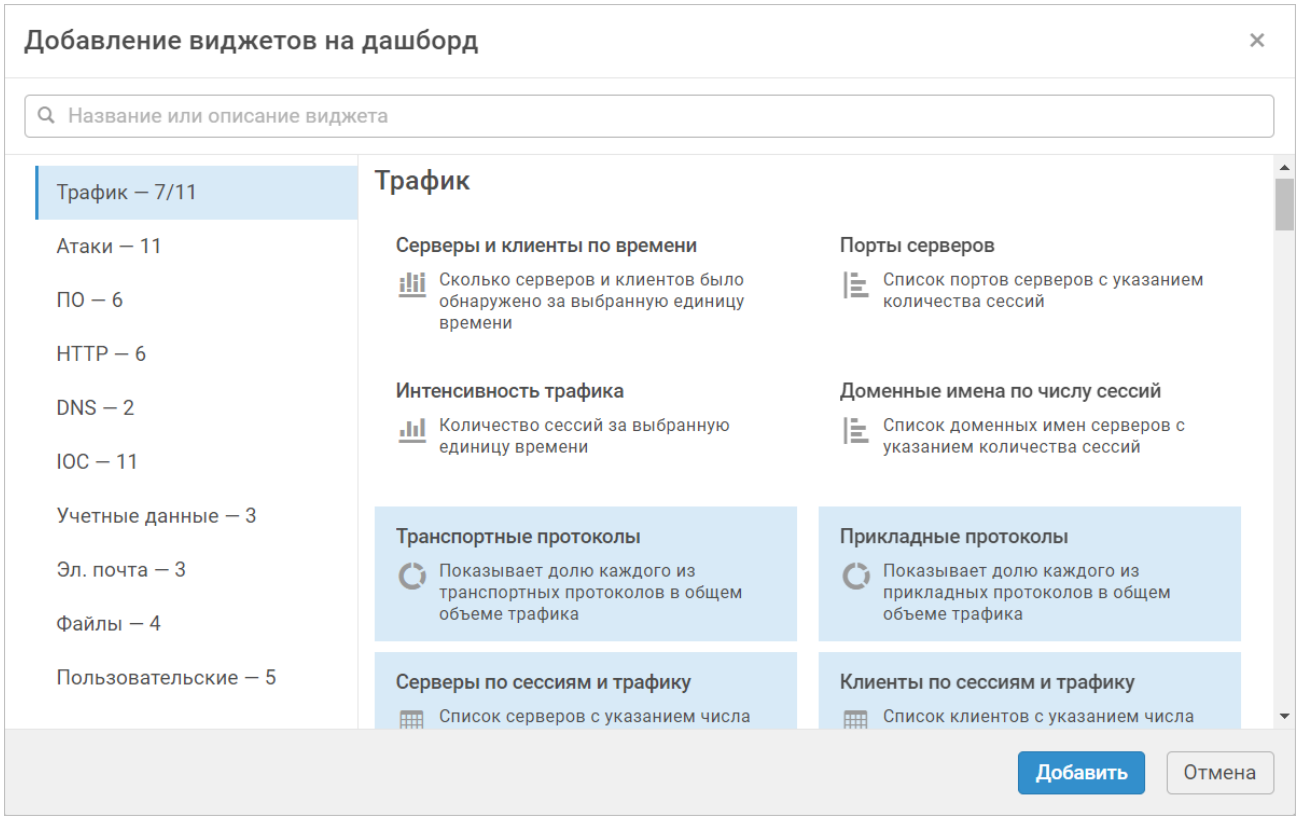


Рисунок 48. Поиск и добавление виджетов

5. В окне выберите хотя бы один виджет.

   Примечание. Чтобы найти нужные вам виджеты, вы можете воспользоваться полем поиска и вкладками, представляющими категории виджетов (см. приложение А).

6. Нажмите кнопку **Добавить**.

   Выбранные виджеты появятся на дашборде.

7. При необходимости измените положение и (или) размеры виджетов путем их перетаскивания, растягивания, уменьшения курсором.

Виджеты добавлены на дашборд.

11.5. Удаление виджета с дашборда

- Чтобы удалить виджет с дашборда:

  1. В главном меню выберите раздел **Дашборды**.
  2. Выберите дашборд.
  3. В панели инструментов нажмите ⚙.

     Появятся кнопки управления дашбордами и виджетами.
  4. В углу виджета нажмите 🗑.

  Виджет удален с дашборда.

11.6. Изменение максимального количества записей в виджете

Вы можете изменять максимальное количество записей в виджете, данные которого отображаются на дашборде в формате:

- горизонтальной столбчатой диаграммы;
- горизонтальной гистограммы;
- таблицы.

- Чтобы изменить максимальное количество записей в виджете:

  1. В главном меню выберите раздел **Дашборды**.
  2. Выберите дашборд.
  3. В панели инструментов нажмите ⚙.

     Появятся кнопки управления дашбордами и виджетами.
  4. В углу виджета нажмите 🔧.
  5. Во всплывающем окне укажите максимальное количество записей, которое требуется отображать в виджете.

     Примечание. Значение по умолчанию — 50. Вы можете указать число от 1 до 1000.
  6. Нажмите кнопку **Применить**.

  Максимальное количество записей в виджете изменено.

11.7. Экспорт данных виджета

Вы можете экспортировать данные, используемые PT NAD для построения виджета, в файл формата JSON или CSV. Впоследствии вы можете использовать этот файл для самостоятельного анализа и импорта в другие продукты.

> **Примечание.** При экспорте PT NAD не учитывает ограничения, накладываемые на количество отображаемых на виджете данных. PT NAD записывает в файл экспорта все данные, соответствующие характеру виджета, примененному фильтру и периоду, выбранному на диаграмме интенсивности трафика (см. раздел 6.3).

- Чтобы экспортировать данные из виджета,

  нажмите ⬇ и в раскрывшемся меню выберите пункт **Скачать в формате JSON** или **Скачать в формате CSV**.

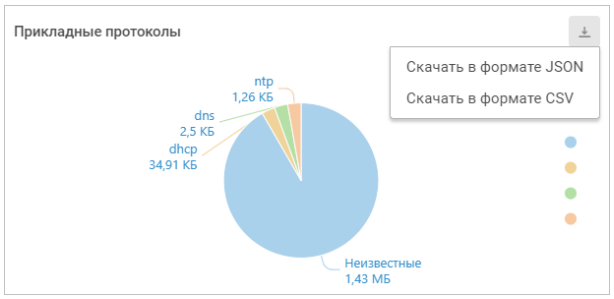


Рисунок 49. Экспорт данных виджета

PT NAD сформирует файл с данными, который будет сохранен браузером в папке по умолчанию.

11.8. Управление пользовательскими виджетами

Если системных виджетов не хватает, чтобы отобразить нужные данные о трафике, вы можете создать собственный виджет или воспользоваться виджетами других пользователей. Такие виджеты входят в категорию **Пользовательские**.

Доступный формат пользовательского виджета — таблица, в которой отображаются данные для выбранных параметров сессии.

Пользовательские виджеты доступны для просмотра, изменения, копирования и удаления всем пользователям.

В этом разделе

Создание виджета (см. раздел 11.8.1)

Изменение виджета (см. раздел 11.8.2)

Копирование виджета (см. раздел 11.8.3)

Удаление виджета (см. раздел 11.8.4)

11.8.1. Создание виджета

► Чтобы создать виджет:

1. В главном меню выберите раздел **Дашборды**.
2. В панели инструментов нажмите ⚙.

   Появятся кнопки управления дашбордами и виджетами.
3. В панели инструментов нажмите кнопку **Добавить виджеты**.

   Откроется окно **Добавление виджетов на дашборд**.
4. В нижней части окна в разделе **Пользовательские** нажмите кнопку **Создать**.

   Примечание. Вы можете быстро перейти к этому разделу, выбрав категорию **Пользовательские** в списке в левой части окна.

   Откроется окно **Создание виджета**.
5. В поле **Название** введите уникальное название виджета.
6. В блоке **Настройка столбцов виджета** настройте параметры виджета:
   - Выберите параметр сессии, для которого необходимо отображать данные в столбце виджета.
   - Выберите функцию, которую PT NAD должен применить к значениям параметра.
   - Выберите параметр сессии, по которому необходимо группировать столбцы виджета.

     Примечание. Вы также можете выбрать параметр сессии, по значениям которого необходимо сортировать записи в виджете, и направление сортировки — в порядке возрастания или убывания значений параметра.
   - Если требуется, измените максимальное количество записей в виджете.

     Примечание. Значение по умолчанию — 50. Вы можете указать число от 1 до 1000.
7. Если требуется, по кнопке **Добавить условие фильтрации** добавьте фильтр для трафика.
8. Нажмите кнопку **Создать**.

Виджет создан.

Созданный виджет появится в окне **Добавление виджетов на дашборд** в категории **Пользовательские**.

11.8.2. Изменение виджета

- Чтобы изменить виджет:

  1. В главном меню выберите раздел **Дашборды**.
  2. В панели инструментов нажмите ⚙.

     Появятся кнопки управления дашбордами и виджетами.
  3. В панели инструментов нажмите кнопку **Добавить виджеты**.

     Откроется окно **Добавление виджетов на дашборд**.
  4. В нижней части окна в разделе **Пользовательские** выберите виджет.

     Примечание. Вы можете быстро перейти к этому разделу, выбрав категорию **Пользовательские** в списке в левой части окна.
  5. Нажмите ⋮ и в раскрывшемся меню выберите пункт **Изменить**.

     Откроется окно **Изменение виджета «<Название виджета>»**.
  6. Измените параметры виджета.

     Примечание. В окне изменения виджета вы можете удалить виджет по кнопке **Удалить**.
  7. Нажмите кнопку **Сохранить**.

  Виджет изменен.

Вы также можете изменять пользовательские виджеты, добавленные на дашборд, по кнопке ✎.

Примечание. Действие доступно в режиме изменения дашбордов.

11.8.3. Копирование виджета

- Чтобы скопировать виджет:

  1. В главном меню выберите раздел **Дашборды**.
  2. В панели инструментов нажмите ⚙.

     Появятся кнопки управления дашбордами и виджетами.
  3. В панели инструментов нажмите кнопку **Добавить виджеты**.

     Откроется окно **Добавление виджетов на дашборд**.
  4. В нижней части окна в разделе **Пользовательские** выберите виджет.

     Примечание. Вы можете быстро перейти к этому разделу, выбрав категорию **Пользовательские** в списке в левой части окна.

5. Нажмите ⋮ и в раскрывшемся меню выберите пункт **Создать копию**.

   Откроется окно **Создание копии виджета «<Название виджета>»**.

6. Если требуется, измените параметры виджета.
7. Нажмите кнопку **Создать копию**.

Виджет скопирован.

11.8.4. Удаление виджета

- Чтобы удалить виджет:

  1. В главном меню выберите раздел **Дашборды**.
  2. В панели инструментов нажмите ⚙.

     Появятся кнопки управления дашбордами и виджетами.

  3. В панели инструментов нажмите кнопку **Добавить виджеты**.

     Откроется окно **Добавление виджетов на дашборд**.

  4. В нижней части окна в разделе **Пользовательские** выберите виджет.

     Примечание. Вы можете быстро перейти к этому разделу, выбрав категорию **Пользовательские** в списке в левой части окна.

  5. Нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

  Виджет удален.

Вы также можете удалить виджет при его изменении (см. раздел 11.8.2).

11.9. Управление дашбордами

Вы можете управлять дашбордами: создавать их, удалять и переименовывать, а также восстанавливать состояние дашбордов по умолчанию.

В этом разделе

11.9.1. Создание дашборда

На странице **Дашборды** по умолчанию находятся дашборды **Трафик**, **Обнаруженное ПО**, **Атаки**. Вы можете создавать новые дашборды и добавлять на них виджеты.

Примечание. Максимальное количество дашбордов — 10.

- Чтобы создать дашборд:

1. В главном меню выберите раздел **Дашборды**.
2. В панели инструментов нажмите ⚙.

   Появятся кнопки управления дашбордами и виджетами.
3. В панели инструментов нажмите +.

   Откроется новый дашборд.
4. На дашборде нажмите кнопку **Добавить виджеты**.

   Откроется окно **Добавление виджетов на дашборд**.
5. В окне выберите хотя бы один виджет.
6. Нажмите кнопку **Добавить**.
7. Рядом с названием созданного дашборда (**Без названия**) по кнопке ✎ откройте поле, в котором введите желаемое название.
8. В панели инструментов нажмите ⚙.

11.9.2. Переименование дашборда

Вы можете переименовать дашборд, если в его названии содержится ошибка или оно больше не отражает действительность.

- Чтобы переименовать дашборд:

1. В главном меню выберите раздел **Дашборды**.
2. В панели инструментов нажмите ⚙.
3. Рядом с названием дашборда по кнопке ✎ откройте поле, в котором введите новое название.
4. В панели инструментов нажмите ⚙.

Дашборд переименован.

11.9.3. Удаление дашборда

► Чтобы удалить дашборд:

1. В главном меню выберите раздел **Дашборды**.
2. Выберите дашборд.
3. В панели инструментов нажмите ⚙.

   Появятся кнопки управления дашбордами и виджетами.
4. Рядом с названием дашборда нажмите 🗑 и подтвердите удаление.
5. В панели инструментов нажмите ⚙.

Дашборд удален.

11.9.4. Восстановление состояния дашбордов по умолчанию

Измененные вами параметры дашбордов и виджетов сохраняются только для вашей учетной записи. Вы можете вернуть состояние дашбордов по умолчанию.

► Чтобы вернуть состояние дашбордов по умолчанию:

1. В панели инструментов нажмите ⚙.

   Появятся кнопки управления дашбордами и виджетами.
2. В панели инструментов нажмите кнопку **Восстановить по умолчанию** и подтвердите восстановление.

Все дашборды заменены дашбордами по умолчанию.

12. Работа с сетевыми связями

PT NAD автоматически генерирует схему сетевых связей между узлами сети, обнаруженными в ходе анализа трафика. Схему можно использовать для визуального представления сетевых взаимосвязей между узлами в границах интересующего трафика, в дополнение к табличному виду. Схема представлена на странице **Сетевые связи**, доступной из одноименного раздела главного меню.

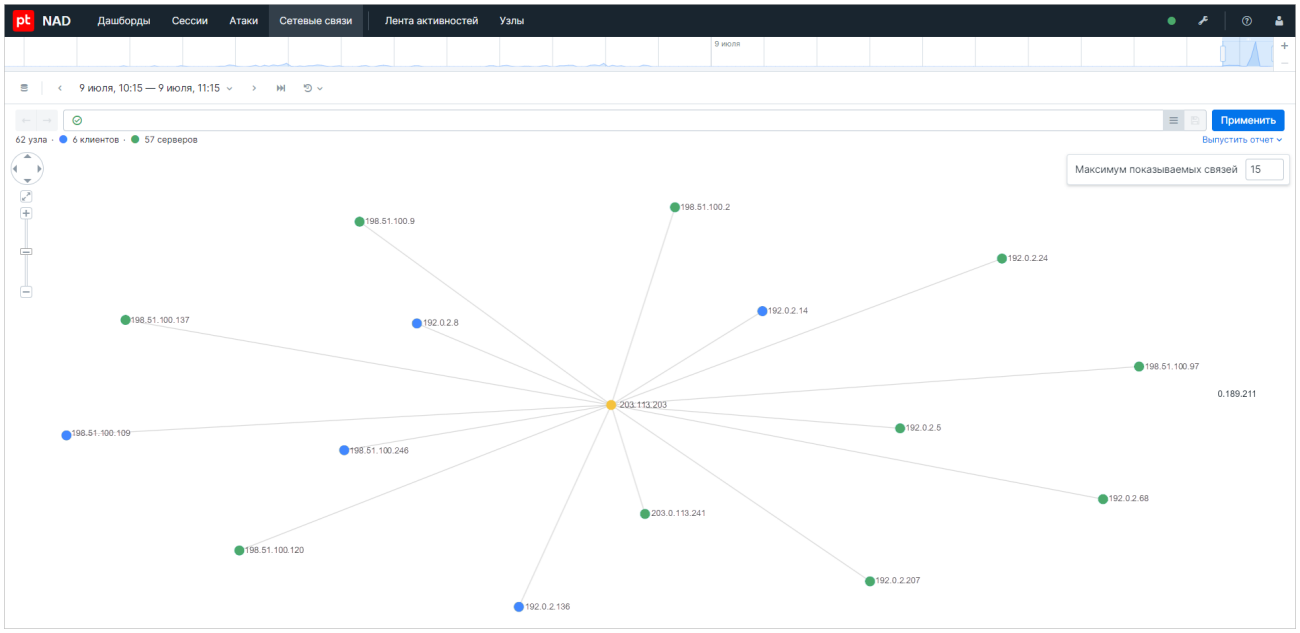


Рисунок 50. Работа с сетевыми связями

Вы можете фильтровать данные на странице с помощью диаграммы интенсивности трафика (см. раздел 6.3) и панели фильтрации (см. раздел 6.5).

Под панелью фильтрации находится строка со сводной информацией о количестве узлов, обнаруженных за период, который был выбран на диаграмме интенсивности трафика.

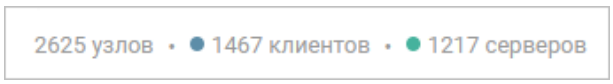


Рисунок 51. Сводная информация об узлах

Информация в строке также соответствует примененным параметрам фильтрации.

Под строкой со сводной информацией в рабочей области располагается схема сетевых связей.

В этом разделе

12.1. Просмотр сетевых связей узла

- Чтобы просмотреть информацию об узле и его связях:

  1. В главном меню выберите раздел **Сетевые связи**.

     По умолчанию отображается 15 связей между самыми активными узлами-отправителями и узлами-получателями.

  2. Если вам нужно изменить максимальное количество сетевых связей на схеме, введите новое число в поле в правом верхнем углу схемы сетевых связей.

  3. Нажмите на узел.

     Отобразятся его IP-адрес и, если были обнаружены, доменные имена.

  4. Нажмите на линию между узлами.

     Откроется всплывающее окно с информацией о взаимодействии между узлами.

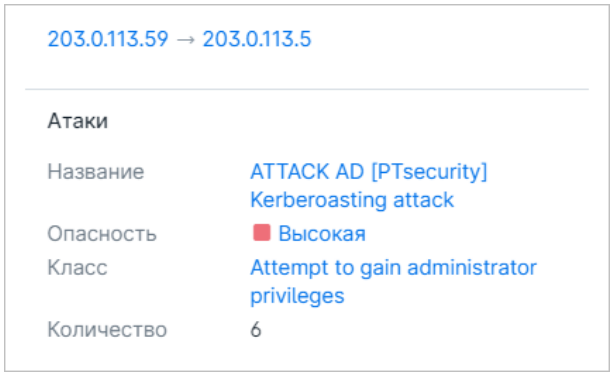


Рисунок 52. Просмотр информации о взаимодействии между узлами

По ссылкам в этом окне вы можете быстро добавлять в строку фильтрации (см. раздел 13) метаданные трафика: IP-адреса и DNS-имена отдельных узлов, а также класс, тип атаки и уровень опасности атаки.

12.2. Фильтрация сетевых связей по периоду

По умолчанию при входе в PT NAD в рабочей области на странице **Сетевые связи** отображаются данные за последний час. Вы можете изменить период фильтрации.

- Чтобы отфильтровать сетевые связи по периоду:

  1. В главном меню выберите раздел **Сетевые связи**.
  2. Нажмите на период для фильтрации.

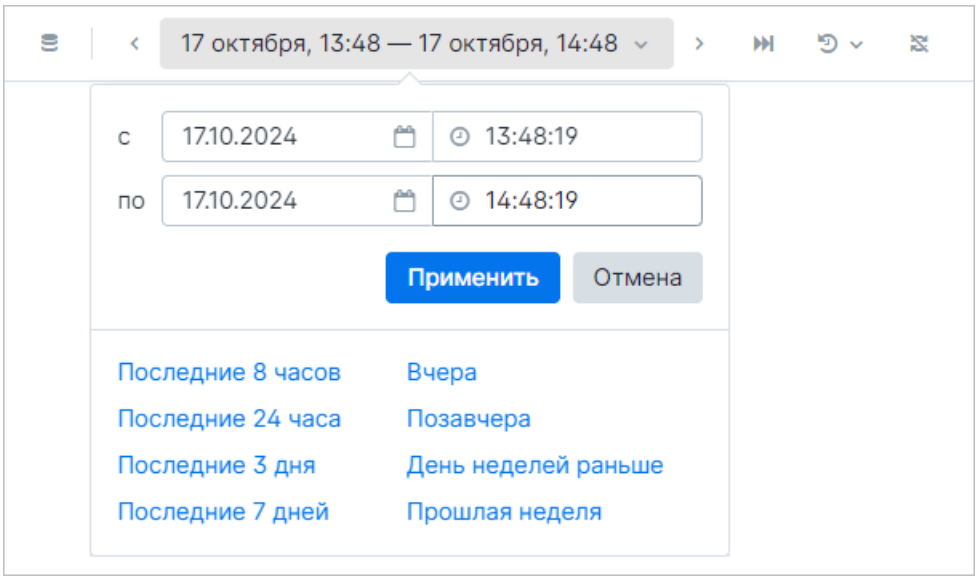


Рисунок 53. Настройка периода фильтрации данных

  3. Укажите период и нажмите **Применить**.

- Чтобы сместить период на половину его длины влево,

  нажмите ‹ .

- Чтобы сместить период на половину его длины вправо,

  нажмите › .

Вы также можете детализировать период фильтрации данных, выделяя с помощью курсора интервал на диаграмме интенсивности трафика (см. раздел 6.3).

Кроме того, вы можете выбрать один из ранее установленных периодов фильтрации, нажав ↺.

- Чтобы вернуть период по умолчанию (данные за последний час),

  нажмите ⏭.

12.3. Фильтрация сетевых связей по метаданным трафика

Вы можете фильтровать сетевые связи по метаданным трафика. Например, вы можете посмотреть связи между узлами, которые участвовали в сессиях с зарегистрированными атаками. Для этого требуется применить фильтр с набором условий.

► Чтобы отфильтровать сетевые связи по метаданным трафика:

1. В главном меню выберите раздел **Сетевые связи**.
2. В панели фильтрации (см. раздел 6.5) добавьте условия одним из способов:
   - Введите параметры для фильтрации, значения параметров и операторы на языке фильтрации продукта (см. приложение Б).

     Примечание. Вы можете просмотреть полный список доступных параметров для фильтрации, нажав комбинацию клавиш Ctrl+Space в строке фильтрации.

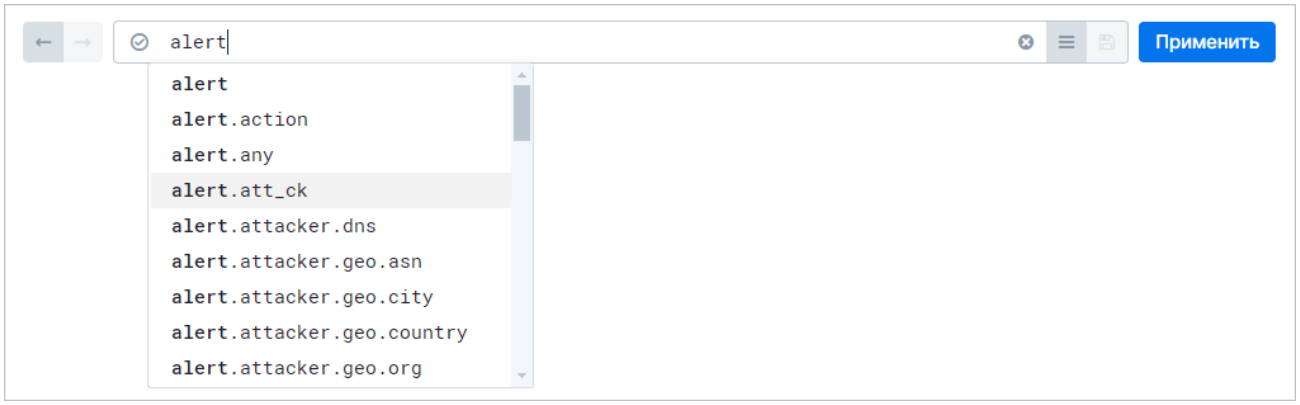


Рисунок 54. Ввод параметров фильтрации

При вводе параметров в строке фильтрации вы можете выбрать их значения из списка (только строковые и булевы). Значения собираются из метаданных трафика, отфильтрованного по периоду.

Рисунок 55. Выбор значений параметров фильтрации

   - Добавьте параметры фильтрации с их значениями по ссылкам, появляющимся по нажатиям на узлы и связи между ними.
3. Нажмите **Применить**.

Добавленные условия фильтрации можно сохранить, чтобы не указывать их снова в дальнейшем. Для этого нужно создать личный (см. раздел 13.1) или общий фильтр (см. раздел 13.2).

Вы можете просматривать историю примененных вами фильтров по нажатию ← и →. PT NAD хранит в истории 100 последних фильтров.

13. Управление фильтрами

В PT NAD постоянно поступает новый трафик из сети организации. Для удобства работы на страницах **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** вы можете настроить отображение не всех данных, а только их части, фильтруя события ИБ по метаданным трафика. Например, вы можете задать условие фильтрации: все сессии с IP-адреса 203.0.113.0 по протоколу сетевого уровня IPv4.

Условия фильтрации можно сохранять для дальнейшего использования: быстрой фильтрации метаданных трафика на страницах (см. раздел 13.3), настройки регулярных отчетов по отфильтрованному трафику (см. раздел 16.2), создания правил для активностей. Сохраненные фильтры бывают двух типов: личные и общие. Личные фильтры созданы вами и доступны для просмотра, изменения и удаления только вам. Общими фильтрами могут управлять любые пользователи.

> **Примечание.** Для настройки регулярных отчетов можно использовать только личные фильтры.

Список сохраненных фильтров отображается по нажатию ☰ в панели фильтрации (см. раздел 6.5).

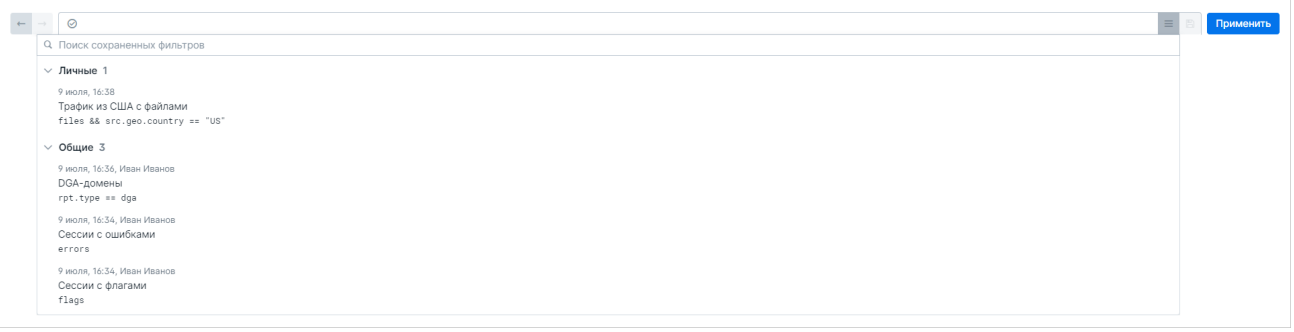


Рисунок 56. Панель фильтрации и список сохраненных фильтров

В этом разделе

См. также

Фильтры и полнотекстовый поиск (см. приложение Б)

13.1. Создание личного фильтра

Отфильтровав данные, вы можете сохранить условия фильтрации для дальнейшего личного использования. Личный фильтр также нужен для создания личных правил для активностей (см. раздел 20.3.8) и настройки регулярной генерации отчетов по отфильтрованному трафику (см. раздел 16.2).

С нуля

- Чтобы создать личный фильтр с нуля:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите .

     Примечание. Чтобы кнопка была активной, данные на странице должны быть отфильтрованы.
  3. Во всплывающем окне в поле введите название фильтра.
  4. Нажмите кнопку **Сохранить**.

  Личный фильтр создан.

На основе другого фильтра

Вы можете создать личный фильтр, взяв за основу условия из другого ранее созданного фильтра.

- Чтобы создать личный фильтр на основе другого фильтра:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите .

     Откроется список сохраненных фильтров.
  3. Выберите фильтр в списке.

     Метаданные трафика будут добавлены в строку фильтрации.
  4. Измените условия фильтрации и нажмите клавишу Enter.

     В рабочей области страниц **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** отобразятся данные, соответствующие новым условиям фильтра.
  5. В панели фильтрации нажмите и в раскрывшемся меню выберите **Сохранить как новый фильтр**.

6. Во всплывающем окне в поле введите название фильтра.
7. Нажмите кнопку **Сохранить**.

Личный фильтр создан.

См. также

Копирование общего фильтра в личные (см. раздел 13.6)

Удаление фильтра (см. раздел 13.7)

Фильтрация сессий по метаданным трафика (см. раздел 9.6)

Фильтрация атак по метаданным трафика (см. раздел 10.6)

Фильтрация данных на дашбордах по метаданным трафика (см. раздел 11.2)

Фильтрация сетевых связей по метаданным трафика (см. раздел 12.3)

13.2. Создание общего фильтра

Отфильтровав данные, вы можете сохранить условия фильтрации для дальнейшего использования любым пользователем PT NAD. Общий фильтр также нужен для создания общих правил для активностей (см. раздел 20.3.8).

Примечание. По общему фильтру нельзя создавать правила генерации отчетов по расписанию. Для этого используются личные фильтры (см. раздел 13.1).

С нуля

- Чтобы создать общий фильтр с нуля:

1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
2. В панели фильтрации нажмите  .

   Примечание. Чтобы кнопка была активной, данные на странице должны быть отфильтрованы.
3. Во всплывающем окне в поле введите название фильтра.
4. Выберите вариант **Общий**.
5. Нажмите кнопку **Сохранить**.

Общий фильтр создан.

На основе другого фильтра

Вы можете создать общий фильтр, взяв за основу условия из другого ранее созданного фильтра.

- Чтобы создать общий фильтр на основе другого фильтра:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. Выберите фильтр в списке.

     Метаданные трафика будут добавлены в строку фильтрации.
  4. Измените условия фильтрации и нажмите клавишу Enter.

     В рабочей области страниц **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** отобразятся данные, соответствующие новым условиям фильтра.
  5. В панели фильтрации нажмите 💾 и в раскрывшемся меню выберите **Сохранить как новый фильтр**.
  6. Во всплывающем окне в поле введите название фильтра.
  7. Выберите вариант **Общий**.
  8. Нажмите кнопку **Сохранить**.

  Общий фильтр создан.

См. также

Копирование личного фильтра в общие (см. раздел 13.5)

Удаление фильтра (см. раздел 13.7)

Фильтрация сессий по метаданным трафика (см. раздел 9.6)

Фильтрация атак по метаданным трафика (см. раздел 10.6)

Фильтрация данных на дашбордах по метаданным трафика (см. раздел 11.2)

Фильтрация сетевых связей по метаданным трафика (см. раздел 12.3)

13.3. Применение фильтра

Вы можете отфильтровать метаданные трафика согласно условиям, записанным в ранее сохраненный фильтр. Для этого вам нужно его применить.

- Чтобы применить фильтр:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. Выберите фильтр в списке.

Метаданные трафика будут добавлены в строку фильтрации.

Фильтр применен.

13.4. Изменение сохраненного фильтра

Вы можете изменять сохраненный фильтр — удалять или добавлять параметры фильтрации и логические операции между ними.

- Чтобы изменить сохраненный фильтр:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. Выберите фильтр в списке.

     Метаданные трафика будут добавлены в строку фильтрации.
  4. Измените условия фильтрации и нажмите клавишу Enter.

     В рабочей области страниц **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи** отобразятся данные, соответствующие новым условиям фильтра.
  5. Нажмите 💾 и в раскрывшемся меню выберите пункт **Перезаписать <Название фильтра>**.

  Фильтр изменен.

См. также

Фильтрация сессий по метаданным трафика (см. раздел 9.6)

Фильтрация атак по метаданным трафика (см. раздел 10.6)

Фильтрация данных на дашбордах по метаданным трафика (см. раздел 11.2)

Фильтрация сетевых связей по метаданным трафика (см. раздел 12.3)

13.5. Копирование личного фильтра в общие

Вы можете поделиться с коллегами личным фильтром по метаданным трафика. Для этого нужно скопировать его в список общих фильтров. Копирование также может понадобиться для создания общего правила активности (см. раздел 20.3.8).

- Чтобы скопировать личный фильтр в общие:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

Откроется список сохраненных фильтров.

3. В списке **Личные** наведите курсор на фильтр и нажмите ссылку **Скопировать в общие**.

   Откроется окно **Копирование личного фильтра в общие**.

4. Если вам нужно изменить название общего фильтра, в поле введите новое название.
5. Нажмите кнопку **Скопировать**.

Личный фильтр скопирован в общие.

См. также

Создание общего фильтра (см. раздел 13.2)

13.6. Копирование общего фильтра в личные

Если вам нужно использовать условие общего фильтра для создания правил генерации отчетов по расписанию (см. раздел 16.2) или создания личного правила для активности (см. раздел 20.3.8), необходимо скопировать этот фильтр в список личных.

- Чтобы скопировать общий фильтр в личные:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. В списке **Общие** наведите курсор на фильтр и нажмите ссылку **Скопировать в личные**.
  4. Если вам нужно изменить название личного фильтра, введите новое название в поле.
  5. Нажмите кнопку **Скопировать**.

  Общий фильтр скопирован в личные.

См. также

Создание личного фильтра (см. раздел 13.1)

13.7. Удаление фильтра

Вы можете удалять сохраненные фильтры по метаданным трафика. Вместе с фильтром удаляются связанные с ним правила для активностей и параметры автоматической генерации отчетов.

Внимание! Общий фильтр удаляется у всех пользователей PT NAD.

- Чтобы удалить фильтр:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. Наведите курсор на фильтр в списке, нажмите ссылку **Удалить фильтр** и подтвердите удаление.

  Фильтр удален.

См. также

Создание личного фильтра (см. раздел 13.1)

Создание общего фильтра (см. раздел 13.2)

14. Работа с лентой активностей

PT NAD уведомляет операторов о подозрительных активностях, обнаруженных в информационной инфраструктуре организации. В отличие от атак, каждая из которых привязана к конкретной сессии, активность обнаруживается в цепочке сессий.

Список обнаруженных активностей отображается на странице **Лента активностей**, доступной из главного меню.

PT NAD обнаруживает активности в результате:

- **Анализа трафика.** PT NAD обнаруживает опасные и потенциально опасные активности в ходе потокового анализа трафика и при периодическом анализе сохраненных метаданных трафика. Такие активности обнаруживаются при помощи правил (см. раздел 2.2).
- **Ретроспективного анализа по репутационным спискам.** PT NAD периодически анализирует ранее завершенные сессии с использованием новых и измененных репутационных списков (см. раздел 20.5). Для отображения результатов такого анализа в ленте активностей нужно установить флажок **Показывать в ленте активностей** в параметрах уведомлений (см. раздел 14.14).

В этом разделе

См. также

Работа с правилами для обнаружения активностей (см. раздел 20.3)

Работа со справочниками (см. раздел 20.4)

14.1. Просмотр списка обнаруженных активностей

- Чтобы просмотреть список обнаруженных активностей:

  1. В главном меню выберите **Лента активностей**.

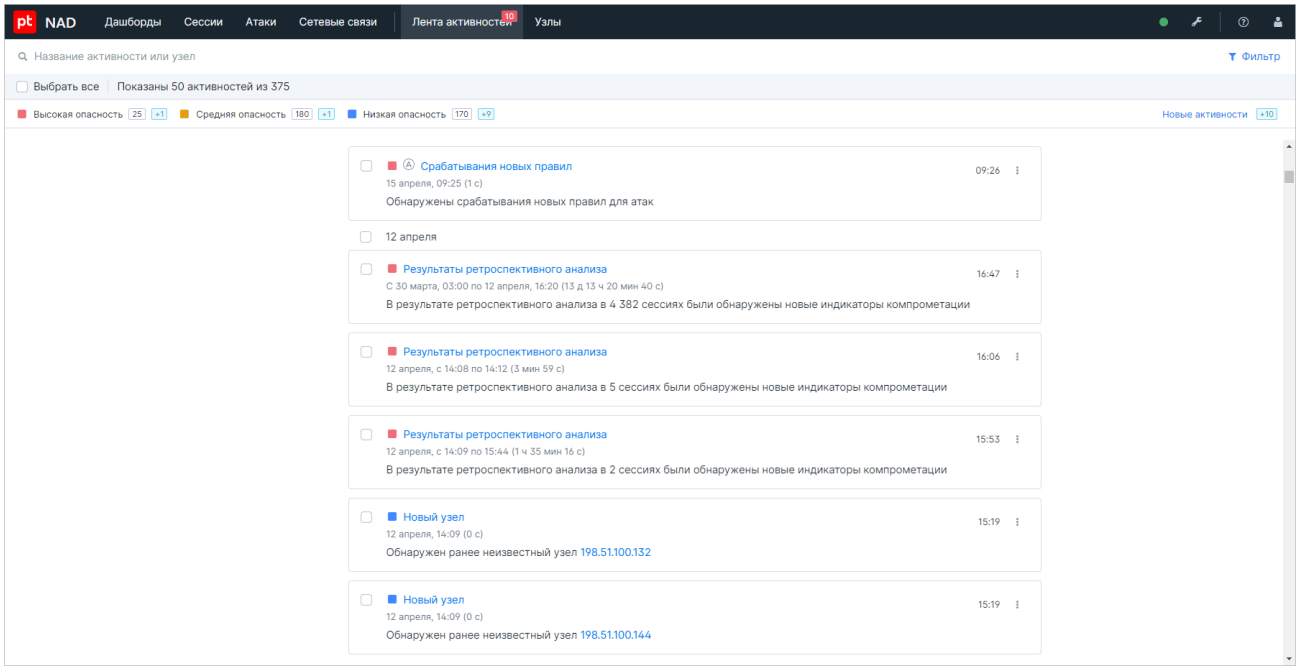


Рисунок 57. Просмотр списка обнаруженных активностей

  2. Если в процессе работы со списком активностей появились новые или обновленные активности и вам нужно их просмотреть, нажмите **Новые активности** → **Обновить**.

Напротив активностей, которые были сгенерированы по срабатыванию пользовательских правил по личным или общим фильтрам, отображаются значки и соответственно.

Если вы находитесь в интерфейсе центральной консоли (см. раздел 2.4), то для каждой активности в списке отображается название и метка обнаружившей ее дочерней системы.

14.2. Просмотр подробной информации об активности

В списке на странице **Лента активностей** доступны только основные сведения об активностях. Полную информацию о каждой активности вы можете просмотреть в ее карточке (см. рисунок 58).

- Чтобы просмотреть подробную информацию об активности:

  1. В главном меню выберите **Лента активностей**.
  2. По ссылке с названием активности откройте карточку активности.

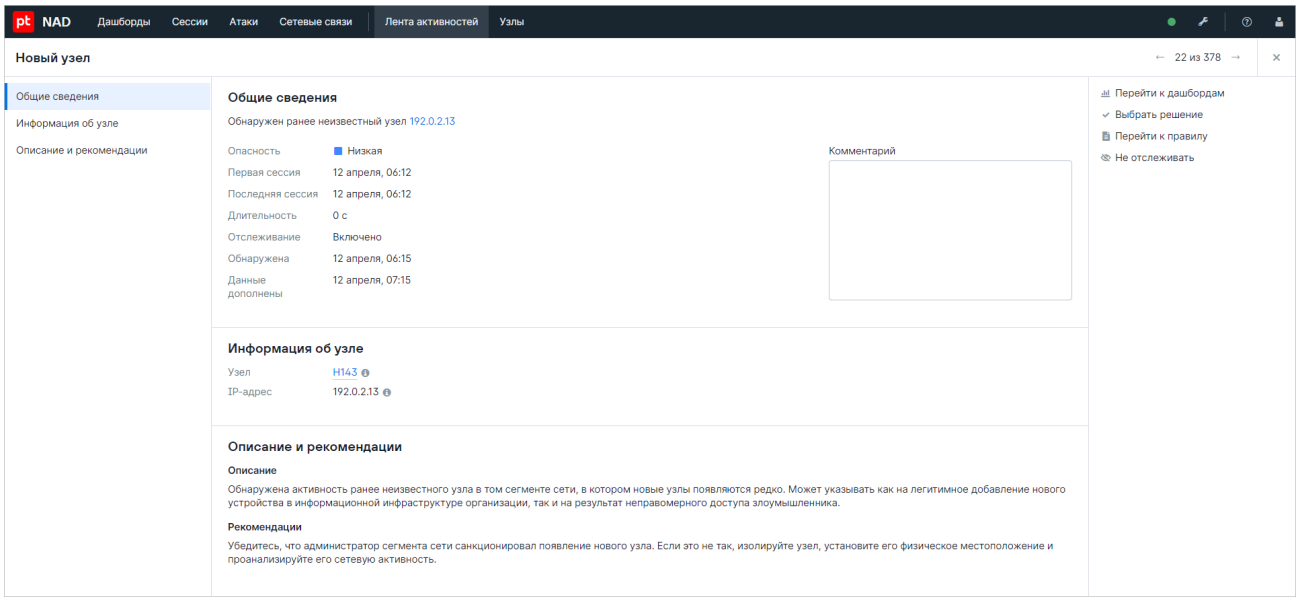


Рисунок 58. Просмотр карточки активности

Если вы находитесь в интерфейсе центральной консоли (см. раздел 2.4), то в названии карточки отображаются название и метка дочерней системы, которая обнаружила активность. Вы можете перейти к карточке активности или к карточке правила в этой системе, используя соответствующие кнопки **Перейти в дочерний NAD** и **Перейти к правилу**. В новой вкладке браузера в интерфейсе дочерней системы откроется карточка этой же активности или правила, по срабатыванию которого сгенерирована карточка.

- Чтобы просмотреть подробную информацию о следующей активности в списке,

  нажмите →.

- Чтобы просмотреть подробную информацию о предыдущей активности в списке,

  нажмите ←.

- Чтобы закрыть карточку,

  нажмите ×.

14.3. Просмотр трафика по активности

Для подробного анализа активности вы можете просмотреть связанный с ней трафик.

- Чтобы просмотреть трафик по активности:

  1. В главном меню выберите **Лента активностей**.
  2. В блоке активности нажмите ⋮ и в раскрывшемся контекстном меню выберите пункт **Перейти к дашбордам**.

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только об активности.

     Примечание. Если длительность активности превышает 24 часа, PT NAD отобразит данные только за последние 24 часа этой активности. Вы можете изменить период фильтрации (см. раздел 11.1).

Вы также можете просмотреть трафик по кнопке **Перейти к дашбордам** в карточке активности (см. раздел 14.2).

14.4. Выбор решения по активности

После просмотра данных об активности вам нужно принять решение по ней. Например, получив информацию о том, что сотрудник организации использует словарный пароль, вы можете обратиться к нему с требованием сменить пароль на более надежный. После этого вам нужно указать для активности, что проблема была решена.

Примечание. Выбранное решение отображается для всех пользователей с правами на просмотр общих сведений о трафике.

Вы можете выбрать одинаковое решение по нескольким активностям сразу (см. раздел 14.5).

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы выбрать решение по активности:

  1. В главном меню выберите **Лента активностей**.
  2. В блоке активности нажмите ⋮ и в раскрывшемся контекстном меню выберите пункт **Выбрать решение**.

     Откроется окно **Выбор решения**.

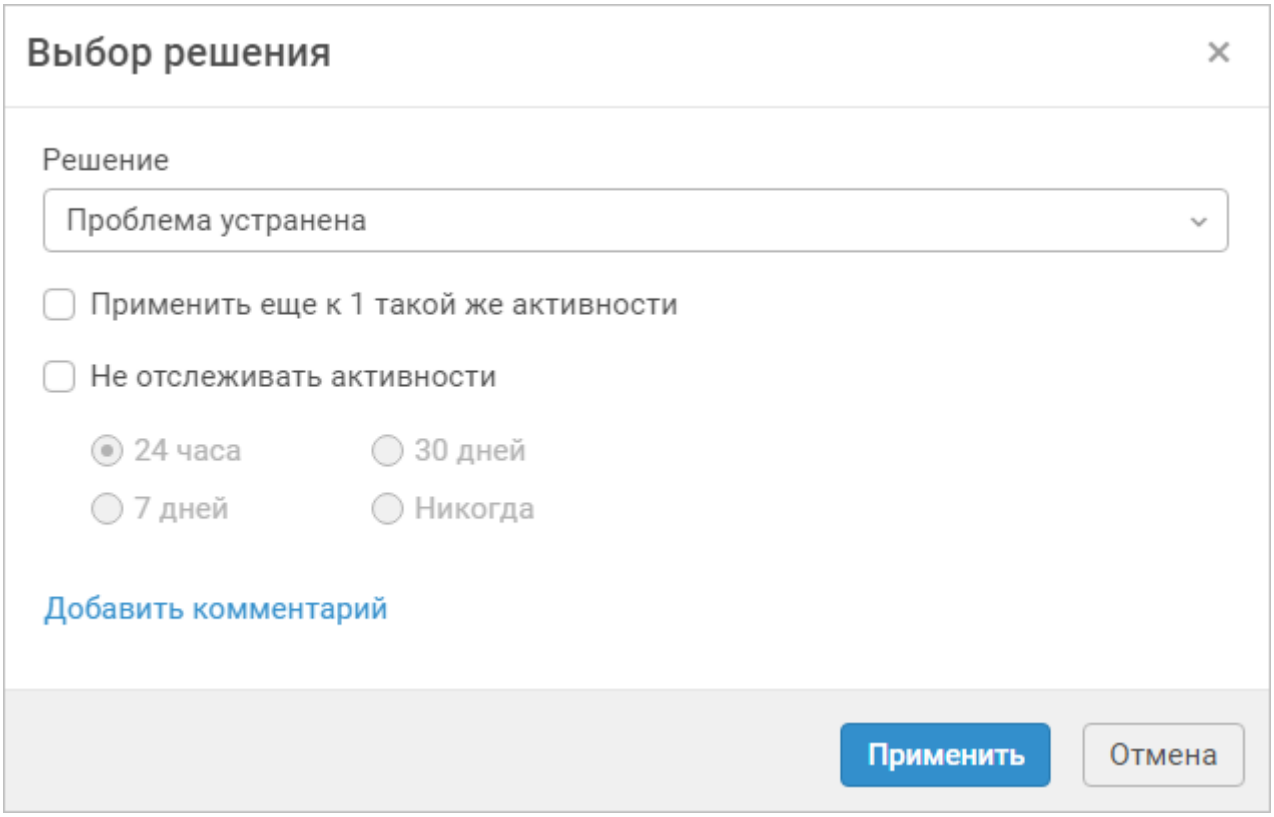


Рисунок 59. Выбор решения по активности

3. В раскрывающемся списке выберите решение.
4. Если в ленте активностей есть записи про аналогичные активности на том же узле и вам нужно применить выбранное решение ко всем этим активностям, установите флажок **Применить еще к <Количество аналогичных активностей> таким же активностям**.
5. Если вам нужно отключить отслеживание активности, установите флажок **Не отслеживать активность** и выберите период отключения.
6. Если вам нужно прокомментировать решение, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее, поле с этим комментарием отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).
7. Нажмите кнопку **Применить**.

Решение по активности выбрано.

Вы также можете выбрать решение по активности в ее карточке по кнопке **Выбрать решение**.

См. также

Отмена решения по активности (см. раздел 14.6)

14.5. Выбор решения по нескольким активностям

После просмотра данных об активностях вам нужно принять решение по ним. Например, получив информацию об активности вредоносного ПО в организации, вам нужно принять меры по его удалению с зараженных узлов. После этого вам нужно указать для всех связанных с этим ПО активностей, что проблема была решена.

> **Примечание.** Выбранное решение отображается для всех пользователей с правами на просмотр общих сведений о трафике.

Если вы считаете, что решения по активностям должны отличаться, вы можете выбрать решение по каждой отдельной активности (см. раздел 14.4).

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы выбрать решение по нескольким активностям:

  1. В главном меню выберите **Лента активностей**.
  2. Установите флажки напротив нужных активностей.

     Примечание. Вы можете выбрать все показанные активности за день, установив флажок рядом с соответствующей датой. Для выбора всех показанных активностей нужно нажать кнопку **Выбрать все**.

     Примечание. Вы можете не снимать флажки с активностей, решение по которым было выбрано ранее. Даже если такие активности будут выбраны, PT NAD не будет их обновлять.
  3. Нажмите кнопку **Выбрать решение**.

     Откроется окно **Выбор решения**.

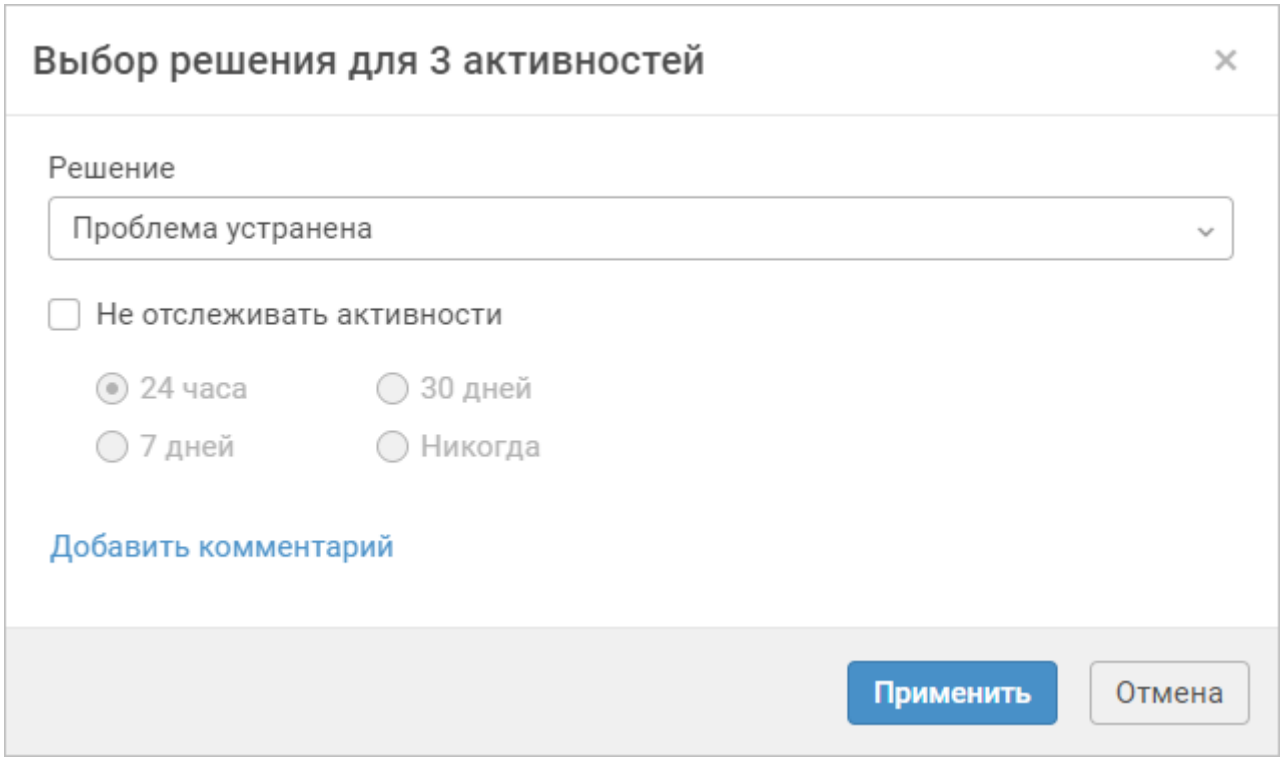


Рисунок 60. Выбор решения по нескольким активностям

4. В раскрывающемся списке выберите решение.
5. Если вам нужно отключить отслеживание активностей, установите флажок **Не отслеживать активности** и выберите период отключения.
6. Если вам нужно прокомментировать решение, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее и совпадает у всех выбранных активностей, поле с ним отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).
7. Нажмите кнопку **Применить**.

Решение по нескольким активностям выбрано.

См. также

Отмена решения по нескольким активностям (см. раздел 14.7)

14.6. Отмена решения по активности

Вы можете отменить решение по активности и выбрать другое.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы отменить решение по активности:

1. В главном меню выберите **Лента активностей**.
2. В блоке активности нажмите ⋮ и в раскрывшемся контекстном меню выберите пункт **Отменить решение**.

   Откроется окно **Отмена решения**.

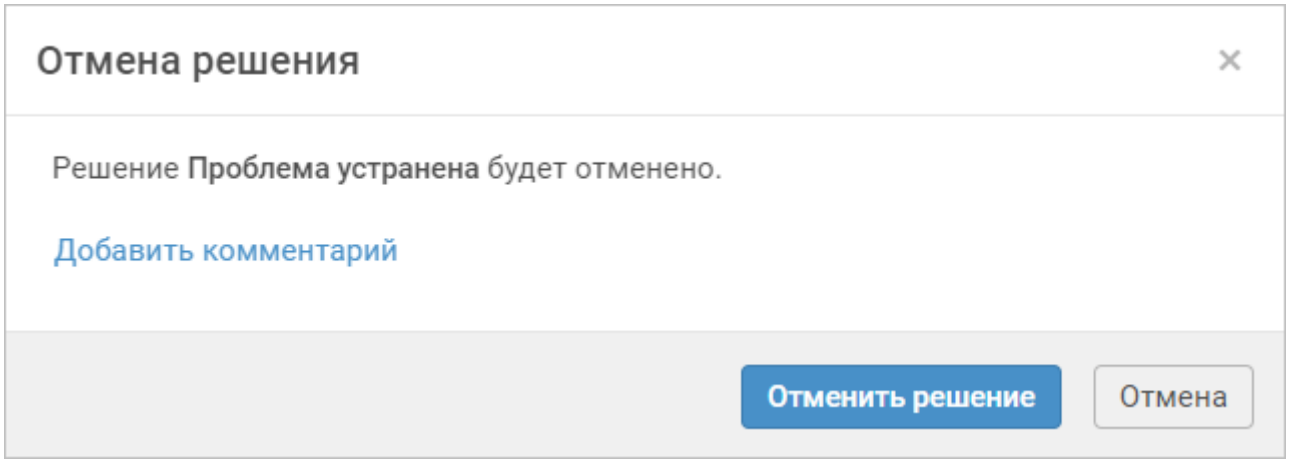


Рисунок 61. Отмена решения по активности

3. Если активность не отслеживается и вам нужно возобновить ее отслеживание, установите флажок **Возобновить отслеживание**.
4. Если вам нужно прокомментировать отмену решения, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее, поле с этим комментарием отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).
5. Нажмите кнопку **Отменить решение**.

Решение по активности отменено.

Вы также можете отменить решение по активности в ее карточке по кнопке **Отменить решение**.

Теперь вы можете выбрать новое решение (см. раздел 14.4).

См. также

Отмена решения по нескольким активностям (см. раздел 14.7)

14.7. Отмена решения по нескольким активностям

Вы можете отменить решение сразу по нескольким активностям и выбрать другое.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы отменить решение по нескольким активностям:

1. В главном меню выберите **Лента активностей**.
2. Установите флажки напротив нужных активностей.

   Примечание. Вы можете выбрать все показанные активности за день, установив флажок рядом с соответствующей датой. Для выбора всех показанных активностей нужно нажать кнопку **Выбрать все**.

   Примечание. Вы можете не снимать флажки с активностей, решения по которым были отменены ранее. Даже если такие активности выбраны, PT NAD не будет их обновлять.
3. Нажмите кнопку **Отменить решение**.

   Откроется окно **Отмена решения**.

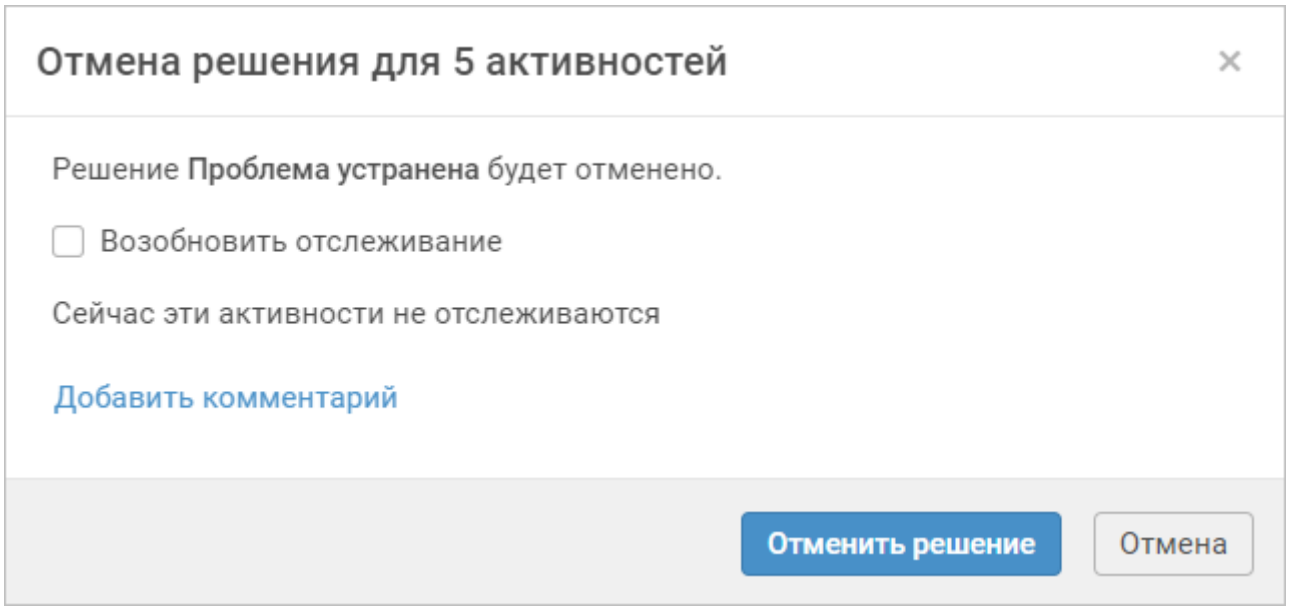


Рисунок 62. Отмена решения по нескольким активностям

4. Если выбранные активности не отслеживаются и вам нужно возобновить их отслеживание, установите флажок **Возобновить отслеживание**.
5. Если вам нужно прокомментировать отмену решения, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее и совпадает у всех выбранных активностей, поле с ним отобразится в окне сразу.

Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).

6. Нажмите кнопку **Отменить решение**.

Решение по нескольким активностям отменено.

Теперь вы можете выбрать новое решение (см. раздел 14.5).

См. также

Отмена решения по активности (см. раздел 14.6)

14.8. Отключение отслеживания активности

Если активность больше не представляет интереса, вы можете отключить ее отслеживание навсегда или на определенный период. Сообщения о ней не будут попадать в ленту активностей для всех пользователей.

Примечание. Вы не можете отключить отслеживание активностей, сгенерированных по срабатыванию пользовательских правил и связанных с результатами ретроспективного анализа. Для последних вы можете отключить только показ в ленте. Для этого нужно снять флажок **Показывать в ленте активностей** в параметрах уведомлений о результатах ретроспективного анализа (см. раздел 14.14).

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы отключить отслеживание активности:

1. В главном меню выберите **Лента активностей**.
2. В блоке активности нажмите ⋮ и в раскрывшемся контекстном меню выберите пункт **Не отслеживать**.

   Откроется окно **Прекращение отслеживания**.

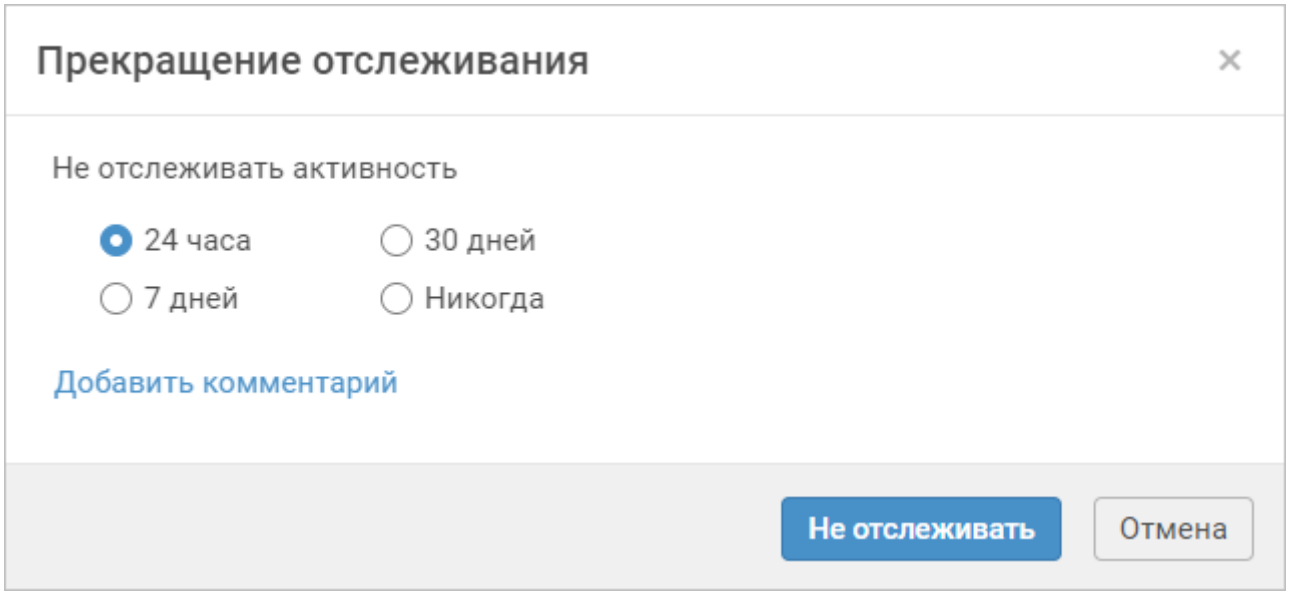


Рисунок 63. Отключение отслеживания активности

3. Выберите период, на который нужно отключить отслеживание.
4. Если вам нужно прокомментировать отключение отслеживания, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее, поле с этим комментарием отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).
5. Нажмите кнопку **Не отслеживать**.

Отслеживание активности отключено.

Неотслеживаемые активности помечаются значком в списке активностей.

Вы также можете отключить отслеживание активности в ее карточке по кнопке **Не отслеживать**. Кроме того, отслеживание можно отключить при выборе решения по активности (см. раздел 14.4).

См. также

Возобновление отслеживания активности (см. раздел 14.10)

Отключение отслеживания нескольких активностей (см. раздел 14.9)

14.9. Отключение отслеживания нескольких активностей

Если активности больше не представляют интереса, вы можете отключить их отслеживание навсегда или на определенный период. Сообщения о них не будут попадать в ленту активностей для всех пользователей.

Примечание. Вы не можете отключить отслеживание активностей, сгенерированных по срабатыванию пользовательских правил и связанных с результатами ретроспективного анализа. Для последних вы можете отключить только показ в ленте. Для этого нужно снять флажок **Показывать в ленте активностей** в параметрах уведомлений о результатах ретроспективного анализа (см. раздел 14.14).

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы отключить отслеживание нескольких активностей:

1. В главном меню выберите **Лента активностей**.
2. Установите флажки напротив нужных активностей.

   Примечание. Вы можете выбрать все показанные активности за день, установив флажок рядом с соответствующей датой. Для выбора всех показанных активностей нужно нажать кнопку **Выбрать все**.

   Примечание. Вы можете не снимать флажки с активностей, отслеживание которых было отключено ранее. Даже если такие активности будут выбраны, PT NAD не будет их обновлять.
3. Нажмите кнопку **Не отслеживать**.

   Откроется окно **Прекращение отслеживания**.

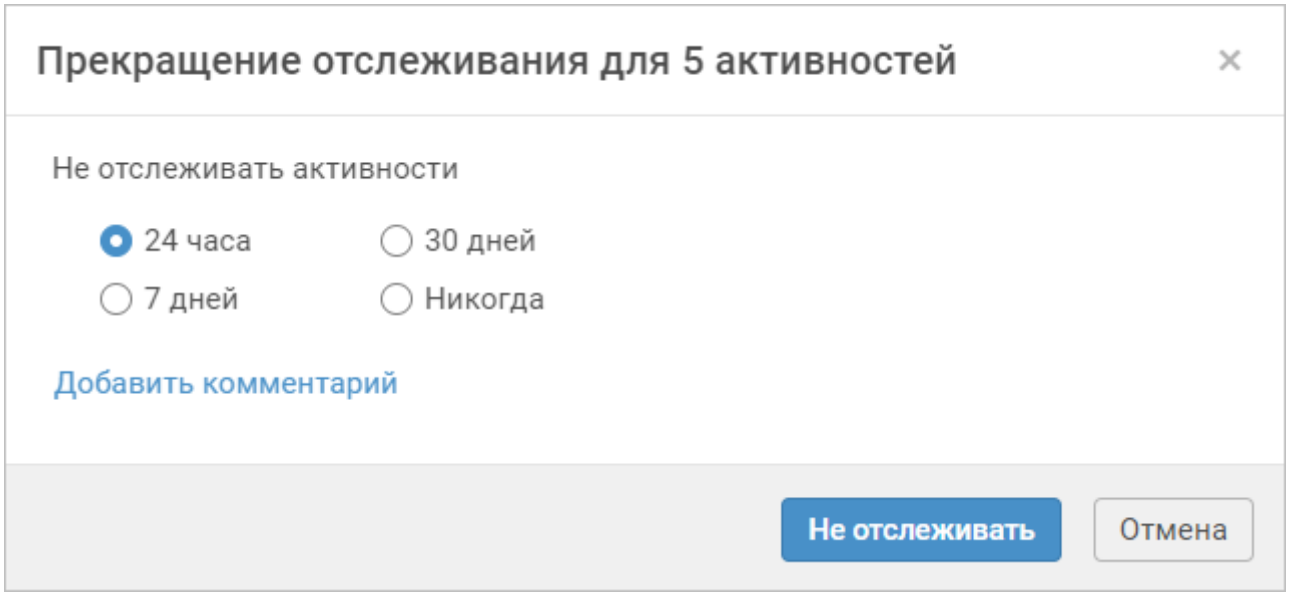


Рисунок 64. Отключение отслеживания нескольких активностей

4. Выберите период, на который нужно отключить отслеживание.
5. Если вам нужно прокомментировать отключение отслеживания, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

Примечание. Если комментарий был добавлен ранее и совпадает у всех выбранных активностей, поле с ним отобразится в окне сразу.

Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).

6. Нажмите кнопку **Не отслеживать**.

Отслеживание нескольких активностей отключено.

Неотслеживаемые активности помечаются значком в списке активностей.

Кроме того, отслеживание можно отключить при выборе решения по активности (см. раздел 14.5).

См. также

Возобновление отслеживания нескольких активностей (см. раздел 14.11)

Отключение отслеживания активности (см. раздел 14.8)

14.10. Возобновление отслеживания активности

Если вы отключили отслеживание активности по ошибке, вы можете возобновить его.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

► Чтобы возобновить отслеживание активности:

1. В главном меню выберите **Лента активностей**.
2. В блоке активности нажмите и в раскрывшемся контекстном меню выберите пункт **Отслеживать снова**.

   Откроется окно **Возобновление отслеживания**.

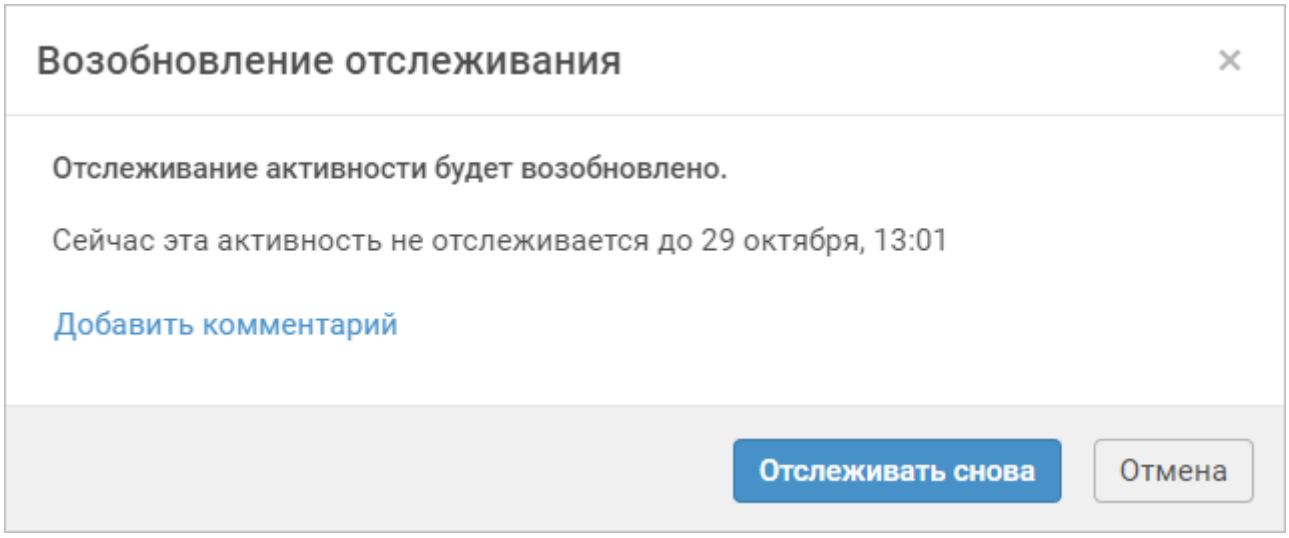


Рисунок 65. Возобновление отслеживания активности

3. Если вам нужно прокомментировать возобновление отслеживания, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее, поле с этим комментарием отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).

4. Нажмите кнопку **Отслеживать снова**.

Отслеживание активности возобновлено.

Вы также можете возобновить отслеживание активности в ее карточке по кнопке **Отслеживать снова** или при отмене решения по активности (см. раздел 14.6).

См. также

Возобновление отслеживания нескольких активностей (см. раздел 14.11)

14.11. Возобновление отслеживания нескольких активностей

Если вы отключили отслеживание активностей, вы можете возобновить его.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы возобновить отслеживание нескольких активностей:

  1. В главном меню выберите **Лента активностей**.
  2. Установите флажки напротив нужных активностей.

Примечание. Вы можете выбрать все показанные активности за день, установив флажок рядом с соответствующей датой. Для выбора всех показанных активностей нужно нажать кнопку **Выбрать все**.

Примечание. Вы можете не снимать флажки с активностей, отслеживание которых было возобновлено ранее. Даже если такие активности будут выбраны, PT NAD не будет их обновлять.

3. Нажмите кнопку **Отслеживать снова**.

   Откроется окно **Возобновление отслеживания**.

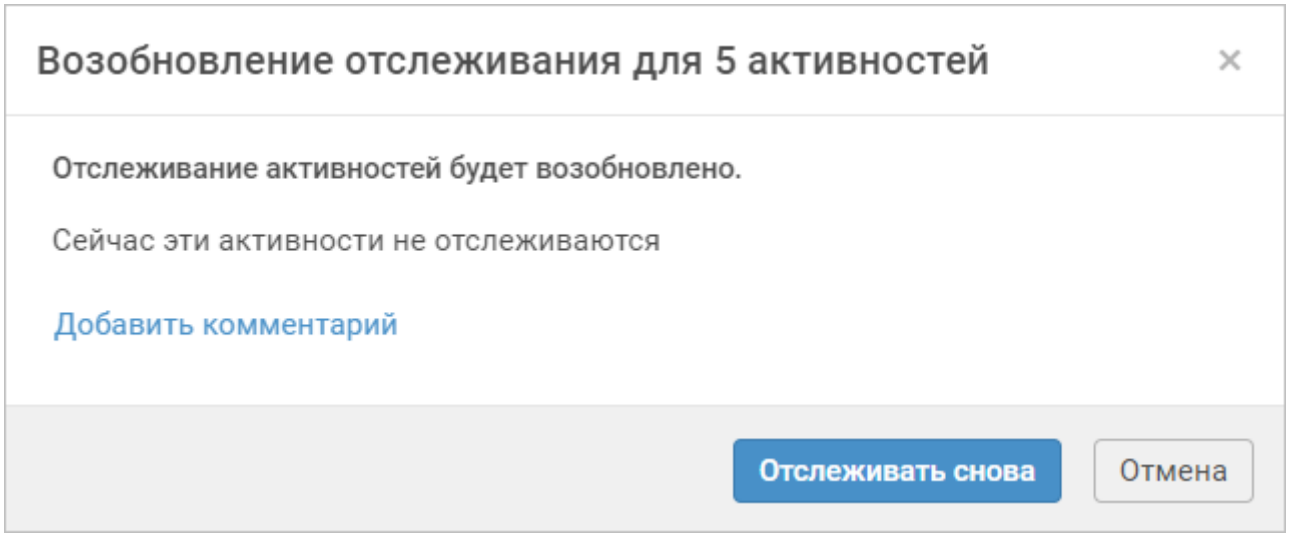


Рисунок 66. Возобновление отслеживания нескольких активностей

4. Если вам нужно прокомментировать возобновление отслеживания, нажмите на ссылку **Добавить комментарий** и в открывшемся поле введите комментарий.

   Примечание. Если комментарий был добавлен ранее и совпадает у всех выбранных активностей, поле с ним отобразится в окне сразу.

   Комментарий будет доступен в списке активностей и в карточке активности (см. раздел 14.2).

5. Нажмите кнопку **Отслеживать снова**.

Отслеживание нескольких активностей возобновлено.

Вы также можете возобновить отслеживание активностей при отмене решения по ним (см. раздел 14.7).

См. также

Возобновление отслеживания активности (см. раздел 14.10)

14.12. Добавление комментария к активности

Вы можете оставлять комментарии к обнаруженным активностям. Это может пригодиться, например, если вам нужно оставить заметку о выборе решения для себя или других операторов.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы добавить комментарий к активности:

  1. В главном меню выберите **Лента активностей**.
  2. По ссылке с названием активности откройте карточку активности.
  3. Введите комментарий в поле.

  Комментарий к активности добавлен.

Помимо карточек, комментарии также отображаются в списке активностей.

Кроме того, вы можете добавлять комментарии при выборе решения по активности (см. раздел 14.4), отмене этого решения (см. раздел 14.6), отключении отслеживания активности (см. раздел 14.8) и возобновлении этого отслеживания (см. раздел 14.10).

14.13. Поиск активностей

- Чтобы найти активности:

  1. В главном меню выберите **Лента активностей**.
  2. Если вам нужно найти активности по их названиям и (или) узлам, которые принимали в них участие, в поле поиска введите название активности и (или) данные узла: его IP-адрес, доменное имя, идентификатор или группу узлов (см. раздел 20.7), в которую он входит.
  3. Если вам нужно найти активности по другим параметрам, нажмите **Фильтр** и выберите параметры фильтрации.

     Вы можете выбрать уровни опасности, решения, статусы отслеживания и типы активностей. Кроме того, вы можете искать типы активностей с помощью поля поиска, а также по типу правил для активностей (личные, общие или системные).

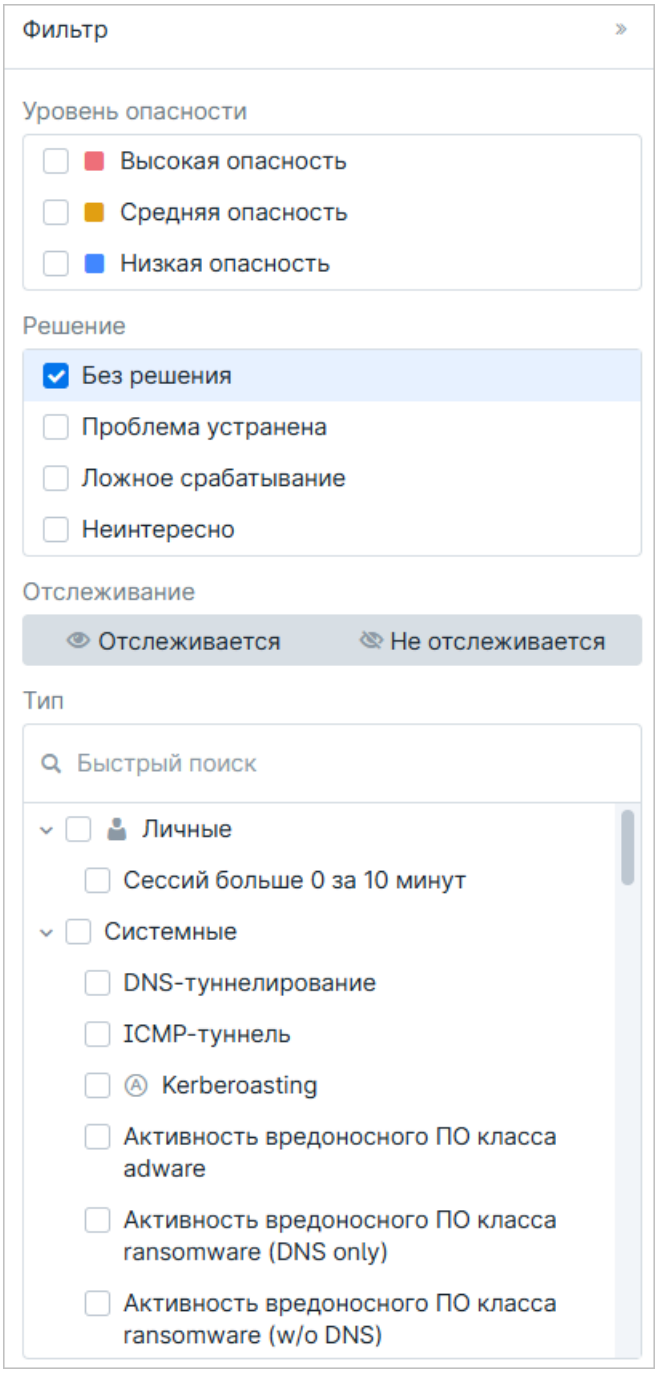


Рисунок 67. Фильтрация активностей

Вы можете сбросить параметры фильтрации и очистить поле поиска по кнопке **Сбросить все**.

14.14. Настройка уведомлений о результатах ретроспективного анализа

Вы можете оперативно узнавать об обновлении репутации сессий по результатам ретроспективного анализа (см. раздел 20.5), получая уведомления по электронной почте или просматривая их в ленте активностей (см. раздел 14).

> **Примечание.** Для настройки уведомлений о результатах ретроспективного анализа вашей учетной записи должна быть присвоена роль с привилегией на просмотр общих сведений о трафике. Для получения прав вам нужно обратиться к администратору PT NAD.
>
> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы настроить уведомления о результатах ретроспективного анализа:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Настройка уведомлений**.

   Откроется страница **Настройка уведомлений**.

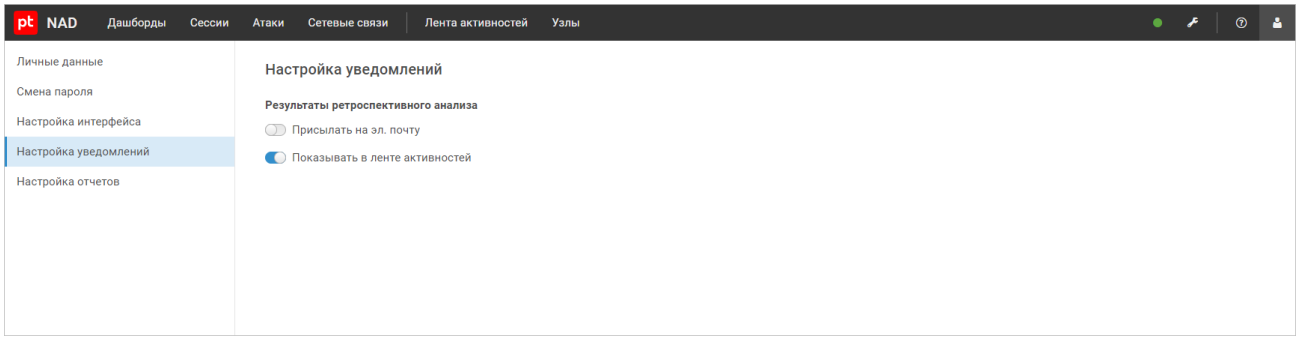


Рисунок 68. Просмотр правил уведомлений

2. Если требуется, включите отправку уведомлений на электронную почту.

   > **Примечание.** Вы можете указать свой адрес электронной почты во вкладке **Личные данные**.

3. Если требуется, включите отображение уведомлений в ленте активностей.

Уведомления о результатах ретроспективного анализа настроены.

Вы можете просмотреть подробную информацию о сессиях, репутация которых была обновлена в ходе ретроспективного анализа. Для этого вам нужно перейти к дашбордам из связанной с уведомлением активности (см. раздел 14.3) или нажать ссылку в столбце **Сессий** в карточке активности или в письме-уведомлении.

15. Работа с узлами

При анализе трафика PT NAD собирает информацию об узлах, которые участвовали в сессиях. При расследовании инцидентов информационной безопасности вы можете просматривать эту информацию на странице **Узлы**, доступной в главном меню.

PT NAD удаляет записи о тех узлах, которые были неактивны более 30 дней. Таким же образом удаляется информация об отдельной активности узла. Например, PT NAD удалит информацию об использовании операционной системы узлом через 30 дней после последней сессии, в которой узел использовал эту операционную систему. Период хранения может быть изменен администратором PT NAD.

В этом разделе

15.1. Просмотр списка узлов

- Чтобы просмотреть список узлов,

  в главном меню выберите раздел **Узлы**.

  Откроется страница **Узлы**.

На странице расположена строка со сводной информацией о количестве найденных узлов: общее число узлов и число узлов определенных типов.

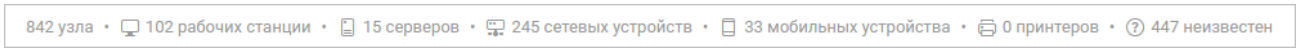
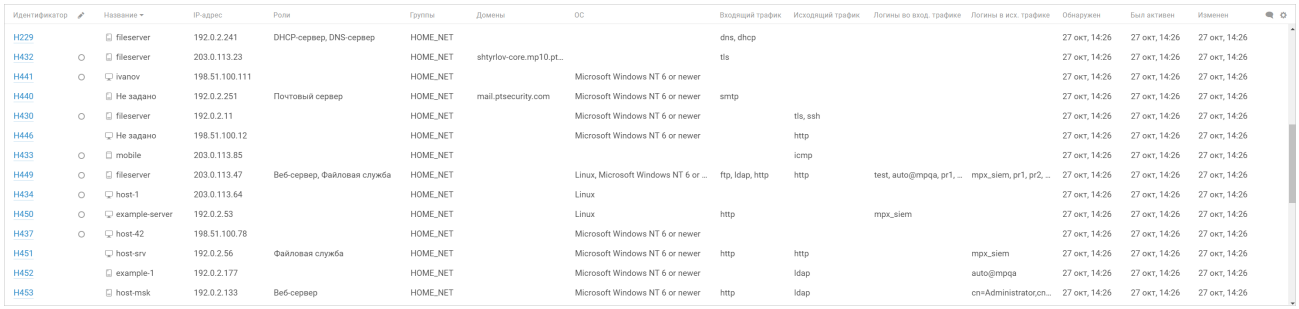


Рисунок 69. Просмотр сводной информации об узлах

Под строкой со сводной информацией находится таблица с перечнем узлов.



Идентификатор	Название	IP-адрес	Роли	Группы	Домены	ОС	Входящий трафик	Исходящий трафик	Логины во вход. трафике	Логины в исх. трафике	Обнаружен	Был активен	Изменен
H229	fileserver	192.0.2.241	DHCP-сервер, DNS-сервер	HOME_NET			dns, dhcp				27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H432	fileserver	203.0.113.23		HOME_NET	shtyrlov-core.mp10.pt...		tls				27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H441	ivanov	198.51.100.111		HOME_NET		Microsoft Windows NT 6 or newer					27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H440	Не задано	192.0.2.251	Почтовый сервер	HOME_NET	mail.ptsecurity.com	Microsoft Windows NT 6 or newer	smtp				27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H430	fileserver	192.0.2.11		HOME_NET		Microsoft Windows NT 6 or newer		tls, ssh			27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H446	Не задано	198.51.100.12		HOME_NET		Microsoft Windows NT 6 or newer		http			27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H433	mobile	203.0.113.85		HOME_NET				icmp			27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H449	fileserver	203.0.113.47	Веб-сервер, Файловая служба	HOME_NET		Linux, Microsoft Windows NT 6 or ...	ftp, ldap, http	http	test, auto@mpqa, pr1, ...	mpx_siem, pr1, pr2, ...	27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H434	host-1	203.0.113.64		HOME_NET		Linux					27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H450	example-server	192.0.2.53		HOME_NET		Linux	http		mpx_siem		27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H437	host-42	198.51.100.78		HOME_NET		Microsoft Windows NT 6 or newer					27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H451	host-srv	192.0.2.56	Файловая служба	HOME_NET		Microsoft Windows NT 6 or newer	http	http		mpx_siem	27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H452	example-1	192.0.2.177		HOME_NET		Microsoft Windows NT 6 or newer		ldap		auto@mpqa	27 окт, 14:26	27 окт, 14:26	27 окт, 14:26
H453	host-msk	192.0.2.133	Веб-сервер	HOME_NET		Microsoft Windows NT 6 or newer	http	ldap		cn=Administrator,cn...	27 окт, 14:26	27 окт, 14:26	27 окт, 14:26

Рисунок 70. Просмотр списка узлов

Для каждого узла указаны следующие данные:

- **Идентификатор** — идентификатор узла (назначается продуктом автоматически).
- **Пользовательские изменения** ( ) — наличие в строке узла значка ○ говорит о том, что вы или другой пользователь PT NAD изменили тип или роли узла или задали ему свое название.
- **Дочерняя система** — метка дочерней системы (см. раздел 8), из которой получены данные о трафике. Отображается в интерфейсе центральной консоли (см. раздел 2.4) для экземпляров PT NAD, объединенных в иерархию.
- **Название** — тип (см. раздел 15.9) и название (см. раздел 15.6) узла.
- **IP-адрес** — последний замеченный IP-адрес узла.
- **Роли** — роли узла (см. раздел 15.9).
- **Группы** — группы, в которые входил узел за все время наблюдения.
- **Домены** — доменные имена узла за все время наблюдения.
- **ОС** — операционные системы, использование которых было замечено на узле за все время наблюдения.
- **Входящий трафик** — прикладные протоколы, использование которых было обнаружено во входящих соединениях узла за все время наблюдения.
- **Исходящий трафик** — прикладные протоколы, использование которых было обнаружено в исходящих соединениях узла за все время наблюдения.
- **Логины во вход. трафике** — логины, которые использовались при успешной аутентификации и были обнаружены во входящем трафике на узел за все время наблюдения.
- **Логины в исх. трафике** — логины, которые использовались при успешной аутентификации и были обнаружены в исходящем трафике с узла за все время наблюдения.
- **Обнаружен** — дата и время начала первой сессии, в которой узел впервые был обнаружен.
- **Был активен** — дата и время завершения последней сессии, в которой был замечен узел.

— **Изменен** — дата и время последнего изменения информации об узле (без учета пользовательских изменений).

— **Комментарий** ( ) — пользовательский комментарий к узлу.

В таблице узлов вы можете:

— сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);

— изменять ширину столбцов;

— изменять порядок следования столбцов, перемещая заголовок столбца;

— изменять набор столбцов (см. раздел 15.2).

По умолчанию узлы в таблице отсортированы по времени обнаружения (недавно обнаруженные узлы отображаются выше).

Параметры таблицы сохраняются для вашей учетной записи при переходе на другие страницы или выходе из продукта.

Вы можете восстановить состояние таблицы по умолчанию по кнопке **По умолчанию** во всплывающем окне со списком столбцов.

15.2. Изменение набора столбцов в таблице узлов

► Чтобы изменить набор столбцов в таблице:

1. В главном меню выберите раздел **Узлы**.

   Откроется страница **Узлы**.

2. По кнопке откройте всплывающее окно со списком столбцов.
3. Установите флажки напротив названий столбцов, которые нужно отображать в таблице.
4. Нажмите кнопку **Сохранить**.

15.3. Просмотр сводной информации об узле

Вы можете просмотреть сводную информацию об узле на той странице интерфейса, где отображается его IP-адрес, домен или идентификатор. Сводная информация включает в себя такие данные, как тип узла, его название, роли, текущий IP-адрес, MAC-адрес, время обнаружения и последней активности, связанные с ним группы, домены, учетные записи и используемые им операционные системы.

> **Примечание.** Сводная информация доступна только для тех узлов, которые известны PT NAD, то есть которые присутствуют в списке узлов (см. раздел 15.1).

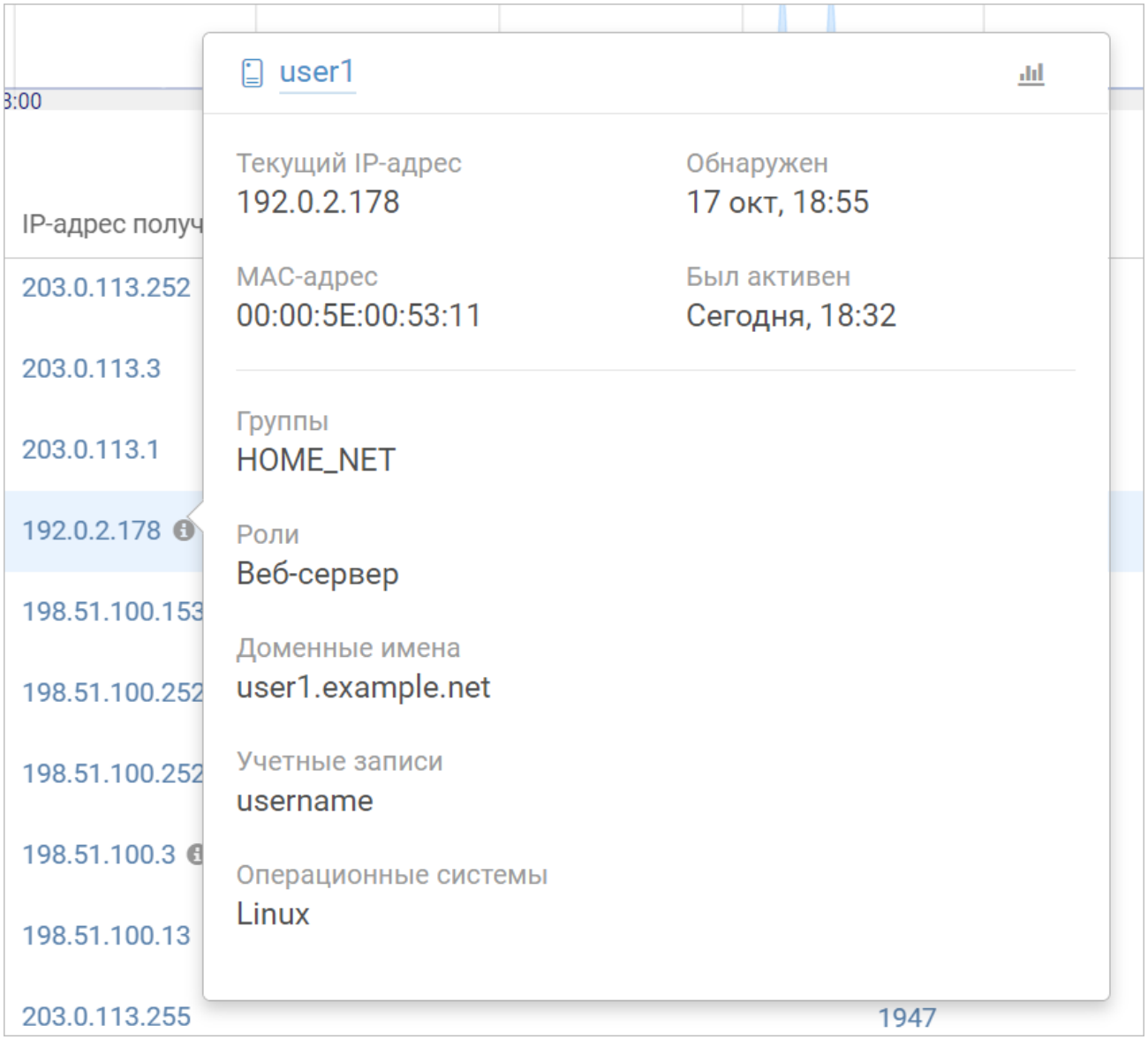


Рисунок 71. Просмотр сводной информации об узле

Из ленты активностей

- Чтобы из ленты активностей перейти к сводной информации об узле,

  нажмите на IP-адрес, домен, идентификатор узла или на значок справа от IP-адреса, домена или идентификатора узла, если этот значок есть.

  Откроется окно сводной информации об узле.

С других страниц интерфейса

- Чтобы с других страниц интерфейса перейти к сводной информации об узле,

  нажмите справа от IP-адреса, домена или идентификатора узла.

  Примечание. Если значка нет, чтобы он появился, нужно навести курсор на IP-адрес, домен или идентификатор узла.

  Откроется окно сводной информации об узле.

Если вам нужно получить больше информации об узле, вы можете перейти к его карточке (см. раздел 15.4), нажав на ссылку в заголовке окна со сводкой.

15.4. Просмотр подробной информации об узле

В таблице на странице **Узлы** доступны только основные сведения об узлах. Полную информацию о каждом узле вы можете просмотреть в его карточке (см. рисунок 72).

- Чтобы просмотреть подробную информацию об узле:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. По ссылке в столбце **Идентификатор** откройте карточку узла.

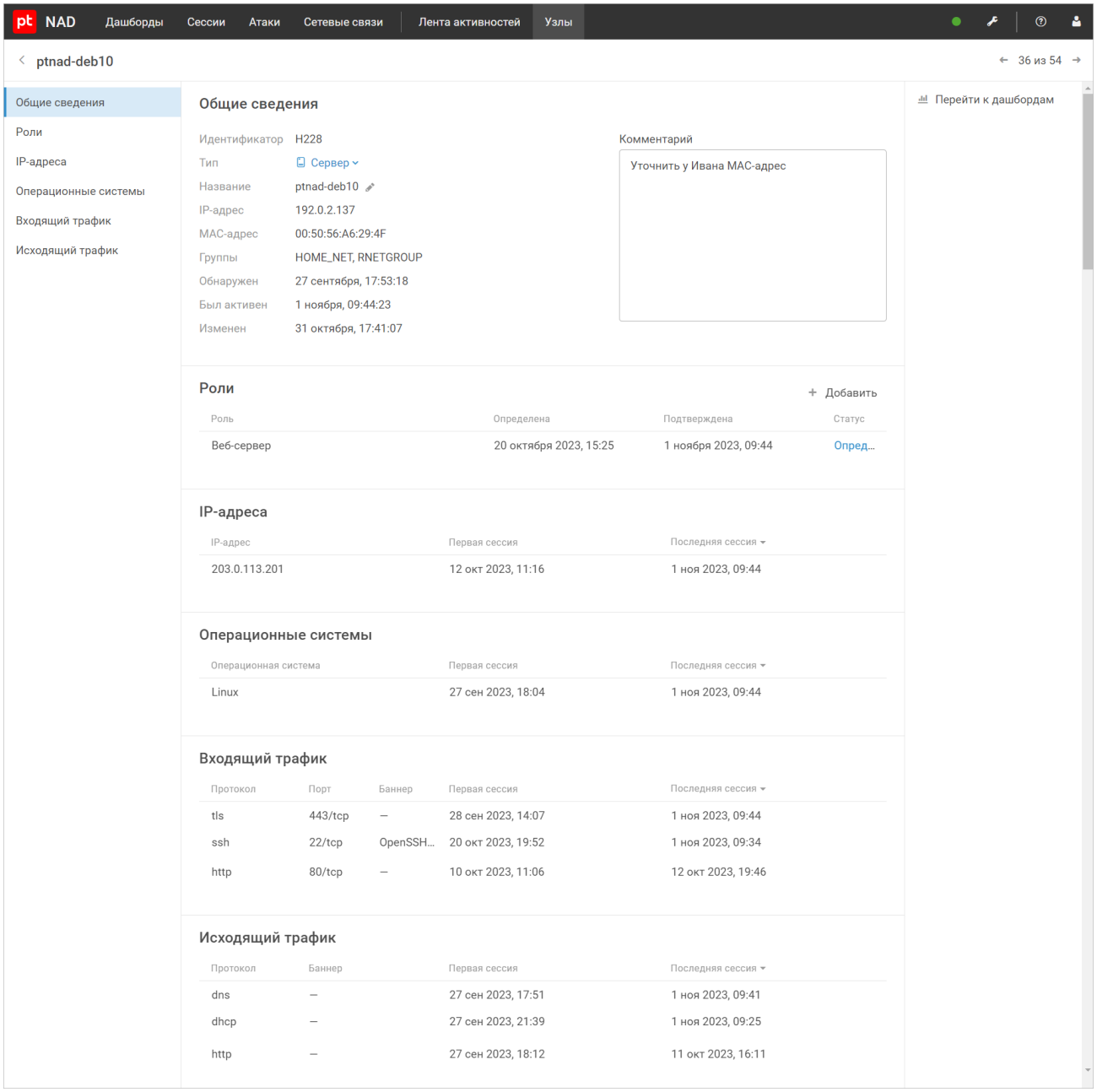


Рисунок 72. Просмотр информации об узле

Вы также можете перейти к карточке узла по ссылке в заголовке окна со сводной информацией об узле (см. раздел 15.3).

Если вы находитесь в интерфейсе центральной консоли (см. раздел 2.4), то в названии карточки отображаются название и метка дочерней системы, которая обнаружила узел. Вы можете перейти в интерфейс этой системы по кнопке **Перейти в дочерний NAD**. В новой вкладке браузера откроется карточка этого же узла в дочерней системе.

- Чтобы просмотреть подробную информацию о следующем узле, показанном в таблице,

  нажмите → .

- Чтобы просмотреть подробную информацию о предыдущем узле, показанном в таблице,

  нажмите ← .

- Чтобы закрыть карточку,

  нажмите ✕ .

15.5. Просмотр трафика по узлу

Для подробного анализа активности узла вы можете просмотреть трафик, связанный с этим узлом.

- Чтобы просмотреть трафик по узлу:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. По ссылке в столбце **Идентификатор** откройте карточку узла.

  3. Нажмите кнопку **Перейти к дашбордам**.

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только по узлу.

     Примечание. По умолчанию PT NAD отображает данные только за последний час активности узла. Вы можете изменить период фильтрации (см. раздел 9.5).

Вы также можете просмотреть трафик по узлу, нажав в сводке (см. раздел 15.3).

15.6. Переименование узлов

При сборе информации об узлах PT NAD получает их названия. Вы можете задавать свои названия, если PT NAD не удалось получить их самому или если вам нужно задать связь между несколькими интерфейсами, относящимися к одному узлу.

Впоследствии вы можете фильтровать данные (см. раздел 13) по названиям узлов, как полученным автоматически, так и пользовательским. Например, чтобы собирать статистику атак с узла host-server-example, нужно ввести в панели фильтрации `alert.attacker.hostname == "host-server-example"` и нажать клавишу Enter.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы переименовать узлы:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. Выберите узлы в таблице.

     Примечание. Для поиска нужных узлов вы можете воспользоваться панелью фильтрации (см. раздел 15.8).

     Примечание. Вы можете выбрать несколько узлов, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных узлов (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.

  3. В панели инструментов нажмите кнопку **Изменить название**.

     Откроется окно **Изменение названия**.

  4. В поле введите новое название для выбранных узлов.

  5. Нажмите кнопку **Сохранить**.

     Примечание. Если в продукте уже есть информация об узлах с введенным названием, PT NAD уведомит вас об этом. Вы можете сохранить повторяющееся название по кнопке **Все равно сохранить** или ввести новое.

  Узлы переименованы.

Вы также можете переименовать отдельный узел в его карточке (см. раздел 15.4) по кнопке в поле **Название**. В этом же поле в скобках отображается название, определенное автоматически.

Для удаления пользовательского названия нужно очистить поле **Название** при переименовании или сбросить пользовательские изменения узла (см. раздел 15.10).

Вы также можете удалить пользовательское название отдельного узла в его карточке по кнопке в поле **Название**.

15.7. Добавление комментария к узлу

Вы можете сохранить дополнительную информацию об узле или оставить заметку о нем, добавив комментарий к узлу. Добавленные комментарии доступны для просмотра всем пользователям, у которых есть доступ к странице **Узлы**.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы добавить комментарий к узлу:

  1. В главном меню выберите раздел **Узлы**.

Откроется страница **Узлы**.

2. По ссылке в столбце **Идентификатор** откройте карточку узла.
3. Введите комментарий в поле.

Комментарий к узлу добавлен.

В таблице **Узлы** в строке с выбранным узлом появится значок . При наведении курсора на этот значок откроется всплывающая подсказка с текстом комментария.

15.8. Поиск узлов

На странице под главным меню расположена панель фильтрации, с помощью которой вы можете искать интересующие вас узлы.

- Чтобы найти узел:

1. В главном меню выберите раздел **Узлы**.

   Откроется страница **Узлы**.

2. Настройте параметры фильтрации узлов в панели фильтрации.

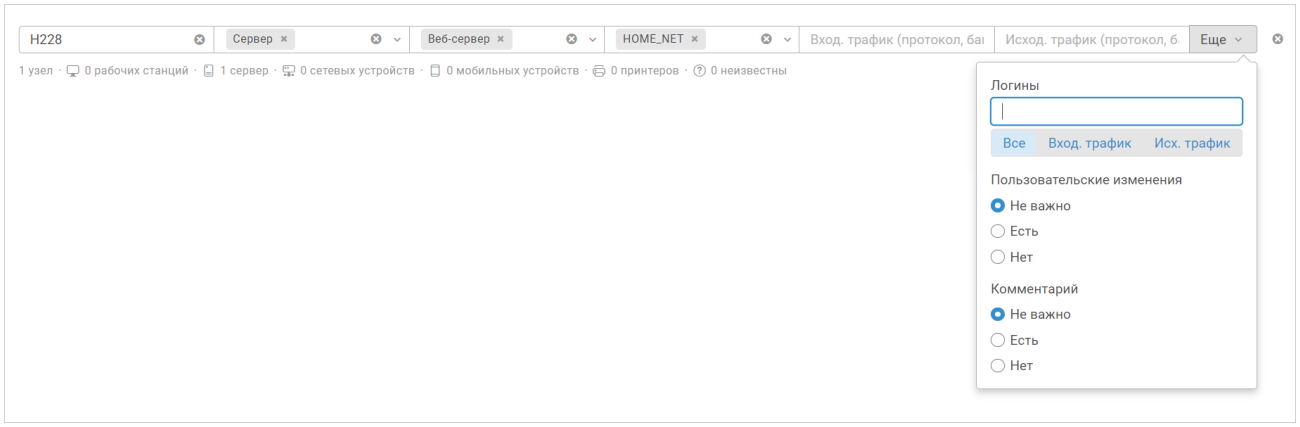


Рисунок 73. Поиск узлов в панели фильтрации

В таблице отобразятся только те узлы, которые подходят под указанные вами параметры фильтрации. Под панелью фильтрации в строке сводной информации будет показано количество найденных узлов с распределением по типам.

Панель фильтрации состоит из следующих параметров:

— **Узел** — поиск узла по его идентификатору, названию (см. раздел 15.6), IP-адресу и (или) домену.

— **Тип** — поиск узла по его типу (см. раздел 15.9) (допускается множественный выбор).

— **Роль** — поиск узла по его ролям (см. раздел 15.9).

— **Группа** — поиск узла по группам узлов, в которые он входит или когда-либо входил.

— **Вход. трафик (протокол, баннер, порт)** — поиск узла по типу поступающего на него трафика (по прикладным протоколам, баннерам и портам).

— **Исход. трафик (протокол, баннер)** — поиск узла по типу отправляемого им трафика (по прикладным протоколам и баннерам клиентов).

— **Еще** — поиск узла по логинам, которые были обнаружены в связанном с ним трафике, или по наличию в записи о нем пользовательских изменений или комментария.

В любом поле панели фильтрации можно вводить несколько значений (с запятой в качестве разделителя). Например, для поиска узла с идентификатором H1212 или IP-адресом 198.51.100.51 нужно ввести `H1212,198.51.100.51` в поле **Узел**.

В полях допускается ввод части значения (кроме номеров портов, их нужно вводить полностью). При этом для неполного поиска по идентификаторам и IP-адресам узлов допускается ввод только начальной части значений.

При выборе или вводе нескольких значений применяется фильтрация по оператору «или».

15.9. Управление типами и ролями узлов

PT NAD определяет типы и роли узлов. Тип узла — это тип устройства, которое выступает в качестве этого узла (например, сервер, рабочая станция, мобильное устройство или принтер). Роли узла определяются функциями, которые выполняет это устройство, например DHCP-сервер, служба каталогов или контроллер домена.

Типы и роли позволяют оценивать активности, в которых принимают участие узлы. Например, вы можете счесть подозрительным поведение рабочей станции, которая принимает запросы от VPN-клиентов.

PT NAD может определять тип и роли как сразу, так и через несколько часов после обнаружения узла. Время определения типа и ролей узла зависит от характера наблюдаемого трафика.

Тип и роли узла могут меняться. PT NAD анализирует трафик любых сессий, в которых узел принимает участие, на предмет обнаружения новой роли или смены типа узла. Вы можете закрепить как тип, так и роли узла, чтобы они не переопределялись автоматически. Если PT NAD определил тип и роли узла неверно, их можно скорректировать.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

Добавление ролей узла (см. раздел 15.9.6)

Закрепление роли узла (см. раздел 15.9.7)

Игнорирование роли узла (см. раздел 15.9.8)

Включение автоматического определения роли узла (см. раздел 15.9.9)

Сброс пользовательских изменений ролей узла (см. раздел 15.9.10)

15.9.1. Смена типа нескольких узлов

Если PT NAD не определил типы узлов или определил их некорректно, вы можете указать один правильный тип для всех этих узлов сразу.

- Чтобы сменить тип нескольких узлов:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. Выберите узлы в таблице.

     Примечание. Для поиска нужных узлов вы можете воспользоваться панелью фильтрации (см. раздел 15.8).

     Примечание. Вы можете выбрать несколько узлов, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных узлов (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.

  3. В панели инструментов нажмите кнопку **Изменить тип и роли**.

     Откроется окно **Изменение типа и ролей**.

  4. В раскрывающемся списке **Тип** выберите тип узлов.

  5. Нажмите кнопку **Сохранить**.

  Тип узлов изменен.

Если тип был изменен по ошибке, вы можете сбросить изменения (см. раздел 15.10).

См. также

Смена типа одного узла (см. раздел 15.9.2)

15.9.2. Смена типа одного узла

Если PT NAD не определил тип узла или определил его некорректно, вы можете указать правильный тип.

- Чтобы сменить тип узла:

  1. В главном меню выберите раздел **Узлы**.

Откроется страница **Узлы**.

2. По ссылке в столбце **Идентификатор** откройте карточку узла.
3. В раскрывающемся списке **Тип** выберите новый тип узла.

Тип узла изменен.

См. также

Смена типа нескольких узлов (см. раздел 15.9.1)

15.9.3. Закрепление типа нескольких узлов

Вы можете закрепить за несколькими узлами один тип, определенный автоматически. Закрепление нужно для того, чтобы PT NAD не изменял тип узлов.

- Чтобы закрепить тип нескольких узлов:

1. В главном меню выберите раздел **Узлы**.

   Откроется страница **Узлы**.

2. Выберите узлы в таблице.

   Примечание. Для поиска нужных узлов вы можете воспользоваться панелью фильтрации (см. раздел 15.8).

   Примечание. Вы можете выбрать несколько узлов, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных узлов (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.

3. В панели инструментов нажмите кнопку **Изменить тип и роли**.

   Откроется окно **Изменение типа и ролей**.

4. В раскрывающемся списке **Тип** выберите тип без отметки об автоопределении.
5. Нажмите кнопку **Сохранить**.

Тип узлов закреплен.

Если тип узлов был закреплен по ошибке, вы можете сбросить изменения (см. раздел 15.10).

См. также

Закрепление типа одного узла (см. раздел 15.9.4)

15.9.4. Закрепление типа одного узла

Вы можете закрепить за узлом тип, определенный автоматически. Закрепление нужно для того, чтобы PT NAD не изменял тип узла.

- Чтобы закрепить тип узла:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. По ссылке в столбце **Идентификатор** откройте карточку узла.

  3. В раскрывающемся списке **Тип** выберите тип без отметки об автоопределении.

  Тип узла закреплен.

Если вы закрепили тип узла по ошибке, нужно снова выбрать тип с пометкой автоопределения.

См. также

Закрепление типа нескольких узлов (см. раздел 15.9.3)

15.9.5. Изменение ролей нескольких узлов

Если PT NAD не определил роли узлов или определил их некорректно, вы можете указать правильный набор ролей для всех этих узлов сразу.

- Чтобы изменить роли нескольких узлов:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.

  2. Выберите узлы в таблице.

     Примечание. Для поиска нужных узлов вы можете воспользоваться панелью фильтрации (см. раздел 15.8).

     Примечание. Вы можете выбрать несколько узлов, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных узлов (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.

  3. В панели инструментов нажмите кнопку **Изменить тип и роли**.

     Откроется окно **Изменение типа и ролей**.

  4. В раскрывающемся списке **Роли** установите флажки напротив нужных ролей и снимите флажки с тех ролей, которые были определены некорректно.

     Если вы сняли флажок с роли, которая была определена автоматически, PT NAD включит игнорирование этой роли. Если вы сняли флажок с роли, которая была добавлена вручную, PT NAD удалит эту роль.

  5. Нажмите кнопку **Сохранить**.

  Роли узлов изменены.

Если роли были изменены по ошибке, вы можете сбросить изменения (см. раздел 15.10).

См. также

Добавление ролей узла (см. раздел 15.9.6)

15.9.6. Добавление ролей узла

Если PT NAD не определил роли узла, вы можете указать их в карточке узла.

- Чтобы добавить роли узла:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.
  2. По ссылке в столбце **Идентификатор** откройте карточку узла.
  3. В блоке **Роли** нажмите кнопку **Добавить**.

     Откроется окно **Добавление роли**.
  4. Установите флажки напротив нужных ролей.
  5. Нажмите кнопку **Добавить**.

  Роли узла добавлены.

Если какая-то из добавленных ролей была добавлена по ошибке, вы можете включить ее игнорирование (см. раздел 15.9.8) или автоопределение (см. раздел 15.9.9). В последнем случае роль будет удалена, если PT NAD ранее не определял эту роль или определял ее в последний раз до истечения срока хранения. Вы также можете сбросить все пользовательские изменения ролей узла (см. раздел 15.9.10).

См. также

Изменение ролей нескольких узлов (см. раздел 15.9.5)

15.9.7. Закрепление роли узла

Вы можете закрепить за узлом роль, определенную автоматически. Закрепление нужно для того, чтобы PT NAD не удалял роль узла, когда она перестает определяться автоматически.

Примечание. Добавляемые вручную роли закрепляются автоматически.

- Чтобы закрепить роль узла:

  1. В главном меню выберите раздел **Узлы**.

Откроется страница **Узлы**.

2. По ссылке в столбце **Идентификатор** откройте карточку узла.
3. В таблице **Роли** в строке с ролью, которую нужно закрепить, в столбце **Статус** выберите **Закреплена за узлом**.

Роль узла закреплена.

Для отмены закрепления роли в строке с ролью в столбце **Статус** нужно выбрать **Определяется автоматически**.

См. также

Изменение ролей нескольких узлов (см. раздел 15.9.5)

15.9.8. Игнорирование роли узла

Если PT NAD определил роль узла некорректно, вы можете включить игнорирование этой роли. Игнорируемая роль не будет отображаться для узла в списке всех узлов. Кроме того, вы не сможете найти узел по игнорируемой роли.

Игнорирование роли может также понадобиться, если вы добавили роль по ошибке или узел перестал выполнять эту роль.

- Чтобы включить игнорирование роли узла:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.
  2. По ссылке в столбце **Идентификатор** откройте карточку узла.
  3. В таблице **Роли** в строке с ролью, которую нужно игнорировать, в столбце **Статус** выберите **Игнорируется**.

  Игнорирование роли узла включено.

Для отмены игнорирования роли в строке с ролью в столбце **Статус** нужно выбрать **Определяется автоматически** или **Закреплена за узлом**.

15.9.9. Включение автоматического определения роли узла

Если роль узла была закреплена по ошибке или вам нужно отменить ее игнорирование, вы можете снова включить автоматическое определение этой роли.

- Чтобы включить автоматическое определение роли узла:

  1. В главном меню выберите раздел **Узлы**.

Откроется страница **Узлы**.

2. По ссылке в столбце **Идентификатор** откройте карточку узла.
3. В таблице **Роли** в строке с ролью, автоматическое определение которой нужно включить, в столбце **Статус** выберите **Определяется автоматически**.

Автоматическое определение роли узла включено. Если PT NAD ранее не определял эту роль или определял ее в последний раз до истечения срока хранения, роль будет удалена.

15.9.10. Сброс пользовательских изменений ролей узла

Вы можете сбросить все пользовательские изменения в наборе ролей узла. PT NAD удалит добавленные вручную роли, а для остальных включит автоматическое определение.

- Чтобы сбросить все пользовательские изменения ролей узла:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.
  2. По ссылке в столбце **Идентификатор** откройте карточку узла.
  3. В блоке **Роли** нажмите кнопку **Сбросить** и подтвердите изменения.

  Все пользовательские изменения ролей узла сброшены.

См. также

Сброс пользовательских изменений узлов (см. раздел 15.10)

15.10. Сброс пользовательских изменений узлов

Если вы внесли изменения в названия, типы и (или) роли нескольких узлов по ошибке, вы можете сбросить эти изменения. PT NAD будет снова определять названия, типы и (или) роли узлов автоматически.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы сбросить пользовательские изменения узлов:

  1. В главном меню выберите раздел **Узлы**.

     Откроется страница **Узлы**.
  2. Выберите узлы в таблице.

     Примечание. Для поиска нужных узлов вы можете воспользоваться панелью фильтрации (см. раздел 15.8).

Примечание. Вы можете выбрать несколько узлов, удерживая клавишу Ctrl или Shift. Для выбора всех отфильтрованных узлов (включая непоказанные) нужно выбрать любую строку в таблице и нажать комбинацию клавиш Ctrl+A.

3. В панели инструментов нажмите кнопку **Сбросить изменения**.

   Откроется окно **Сброс изменений**.

4. Установите флажки напротив тех изменений, которые нужно сбросить.

5. Нажмите кнопку **Сбросить**.

   Для сбрасываемых параметров включится автоматическое определение. Если вы выбрали сброс изменений ролей, добавленные вручную роли будут удалены.

См. также

Сброс пользовательских изменений ролей узла (см. раздел 15.9.10)

16. Работа с отчетами

PT NAD позволяет создавать отчеты о сетевом взаимодействии. Вы можете создать отчет вручную (см. раздел 16.1) или настроить его автоматическую генерацию по расписанию.

В последнем случае отчеты генерируются по трафику из потоковых хранилищ по выбранному фильтру (см. раздел 16.2) или по всему трафику (см. раздел 16.3) и отправляются на указанный адрес (см. раздел 21.1) электронной почты. Вы можете просматривать, создавать, изменять и удалять правила для генерации отчетов в личном кабинете на вкладке **Настройка отчетов**.

В этом разделе

16.1. Выпуск отчета о сетевом взаимодействии

Вы можете выпускать отчеты со статистикой по отфильтрованным данным о трафике.

- Чтобы выпустить отчет:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. Под панелью фильтрации (см. раздел 6.5) нажмите **Выпустить отчет** и выберите формат отчета.

     Примечание. Если кнопка **Выпустить отчет** не отображается, обратитесь к администратору PT NAD.

     Отобразится оповещение о ходе генерации отчета. После генерации отчета его скачивание начнется автоматически.

     Вы также можете скачать отчет вручную, нажав ссылку в оповещении об успешной генерации отчета.

16.2. Создание правил автоматической генерации отчетов по личному фильтру

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

PT NAD может генерировать периодические отчеты по трафику, удовлетворяющему условиям личного фильтра (см. раздел 13.1).

- Чтобы создать правила автоматической генерации отчетов по личному фильтру:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. В списке **Личные** наведите курсор на фильтр и нажмите **Настройка отчетов**.
  4. Нажмите **Добавить отчет**.
  5. Выберите формат отчетов (PDF или DOCX).
  6. Задайте период генерации и отправки отчетов.
  7. Если вам нужно создать еще одно правило генерации отчетов по тому же фильтру, нажмите **Добавить отчет** и задайте параметры генерации.
  8. Нажмите **Сохранить**.

В списке **Личные** фильтры, по которым были созданы правила генерации отчетов по расписанию, помечаются значком .

Рисунок 74. Фильтр с настроенной генерацией отчетов по расписанию

Вы также можете создавать правила автоматической генерации отчетов по созданным вами личным фильтрам из личного кабинета на вкладке **Настройка отчетов**.

16.3. Создание правила автоматической генерации отчетов по всему трафику

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы создать правило автоматической генерации отчетов по всему трафику:

  1. В главном меню выберите → **Настройка отчетов**.
  2. Нажмите **Создать**.
  3. Выберите формат отчетов (PDF или DOCX).

4. Задайте период генерации и отправки отчетов.
5. Нажмите **Создать отчет**.

17. Просмотр информации об IP-адресах и доменах

Вы можете просмотреть подробную информацию об IP-адресе или домене с той страницы интерфейса, где он отображается. Этой информацией могут быть как регистрационные данные (WHOIS), так и сведения о компрометации узла или ресурса.

Описанные в этом разделе функции применимы только к тем IP-адресам и доменам, которые не относятся к обнаруженным узлам (см. раздел 15).

В этом разделе

17.1. Просмотр статистики по IP-адресу или домену на дашбордах

Вы можете встречать IP-адреса и домены на страницах, предназначенных для мониторинга трафика и анализа метаданных трафика. Для расследования инцидента с участием конкретного IP-адреса или домена можно со страницы, на которой встречается этот IP-адрес или домен, перейти к дашбордам для просмотра статистики трафика, в котором участвовал этот IP-адрес или домен.

> **Примечание.** Инструкция применима только к тем IP-адресам и доменам, которые не относятся к обнаруженным узлам (см. раздел 15).

Из ленты активностей

- Чтобы из ленты активностей перейти к статистике по IP-адресу или домену:

  1. Нажмите на IP-адрес, домен или на значок справа от этого IP-адреса или домена, если этот значок есть.
  2. В открывшемся окне нажмите .

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только по интересующему вас IP-адресу или домену.

     > **Примечание.** PT NAD отобразит данные только за последний час, в течение которого IP-адрес или домен встречался в трафике. Вы можете изменить период фильтрации (см. раздел 9.5).

С других страниц интерфейса

- Чтобы с других страниц интерфейса перейти к статистике по IP-адресу или домену:

  1. Нажмите справа от IP-адреса или домена.

     Примечание. Если значка нет, чтобы он появился, нужно навести курсор на IP-адрес или домен.

  2. В открывшемся окне нажмите .

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только по интересующему вас IP-адресу или домену.

17.2. Просмотр информации об IP-адресе или домене на внешних ресурсах

При обнаружении подозрительной активности вы можете просмотреть подробную информацию о внешнем IP-адресе или домене на одном или нескольких сторонних аналитических ресурсах (например, VirusTotal), чтобы расследовать причины такой активности.

Примечание. Инструкция применима только к тем IP-адресам и доменам, которые не относятся к обнаруженным узлам (см. раздел 15).

Примечание. Список ссылок на внешние ресурсы настраивается администратором PT NAD.

Из ленты активностей

- Чтобы из ленты активностей перейти к внешнему ресурсу с информацией об IP-адресе или домене:

  1. Нажмите на IP-адрес, домен или на значок справа от этого IP-адреса или домена, если этот значок есть.
  2. В открывшемся окне перейдите по ссылке на интересующий вас внешний ресурс.

     В новой вкладке браузера откроется страница внешнего ресурса с информацией об IP-адресе или домене.

С других страниц интерфейса

- Чтобы с других страниц интерфейса перейти к внешнему ресурсу с информацией об IP-адресе или домене:

  1. Нажмите справа от IP-адреса или домена.

Примечание. Если значка  нет, чтобы он появился, нужно навести курсор на IP-адрес или домен.

2. В открывшемся окне перейдите по ссылке на интересующий вас внешний ресурс.

   В новой вкладке браузера откроется страница внешнего ресурса с информацией об IP-адресе или домене.

18. Просмотр информации о файлах

Если вас заинтересовал конкретный файл, вы можете просмотреть подробную информацию о нем с той страницы интерфейса, где отображается его хеш-сумма. Этой информацией могут быть как общие свойства (размер, MIME-тип, названия), так и результаты проверки антивирусами и сведения о компрометации.

В этом разделе

18.1. Просмотр статистики по файлу на дашбордах

Для расследования инцидентов с участием конкретного файла можно на дашбордах просмотреть статистику трафика сессий, в ходе которых передавался этот файл.

Из карточки сессии или атаки

- Чтобы из карточки сессии или атаки перейти к статистике по файлу:

  1. Откройте карточку сессии (см. раздел 9.2) или карточку атаки (см. раздел 10.2), в ходе которых передавался файл.
  2. В списке файлов нажмите справа от файла.

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только по интересующему вас файлу.

Из виджета

- Чтобы из виджета перейти к статистике по файлу:

  1. Наведите курсор на хеш-сумму файла и нажмите на появившийся значок .
  2. В открывшемся окне нажмите .

     В новой вкладке браузера откроется страница **Дашборды**. На странице трафик будет отфильтрован для показа данных только по интересующему вас файлу.

18.2. Просмотр информации о вредоносном ПО во внешней аналитической системе

PT NAD может быть интегрирован с внешней аналитической системой. В качестве этой системы может выступать один из продуктов Positive Technologies: PT MultiScanner или PT Sandbox. Если администратор PT NAD настроил интеграцию, PT NAD отправляет извлеченные из трафика файлы во внешнюю аналитическую систему, которая проверяет файлы и возвращает результаты проверки в PT NAD. Краткая информация об обнаруженных угрозах ИБ (класс и тип вредоносного ПО) отображается в карточках сессий и атак. Вы можете просмотреть более подробную информацию о файле, перейдя на страницу результатов его проверки в интерфейсе внешней аналитической системы.

Примечание. Для просмотра подобной информации вам должен быть предоставлен доступ во внешнюю аналитическую систему с помощью сервиса PT MC. При необходимости вам нужно обратиться к администратору PT MC.

- Чтобы просмотреть информацию об обнаруженном вредоносном ПО во внешней аналитической системе:

1. Откройте карточку сессии (см. раздел 9.2) или карточку атаки (см. раздел 10.2), в ходе которых передавались файлы, определенные внешней аналитической системой как опасные или потенциально опасные.

   Примечание. Вы можете найти такие сессии или атаки, введя в строку фильтрации `rpt.type == "ms"` и нажав клавишу Enter. Для фильтрации по опасным файлам вы можете использовать дополнительное условие `rpt.color == "1"`, по потенциально опасным — `rpt.color == "4"`.

2. В списке файлов нажмите справа от файла.
3. В открывшемся окне выберите пункт **Перейти к результатам проверки**.

   Примечание. Файлы с опасным поведением, обнаруженным в ходе поведенческого анализа, помечаются значком . Вы можете найти сессии и атаки с такими файлами, введя в строку фильтрации `files.rpt.sandbox == true` и нажав клавишу Enter.

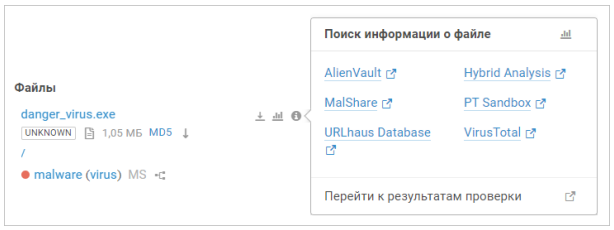


Рисунок 75. Переход во внешнюю аналитическую систему для просмотра подробной информации о файле

В новой вкладке браузера откроется страница внешней аналитической системы с подробными результатами проверки файла.

См. также

Категория виджетов Индикаторы компрометации (см. раздел A.6)

18.3. Просмотр информации о файле на внешних ресурсах

При обнаружении подозрительной активности с использованием конкретного файла можно со страницы, на которой встречается хеш-сумма этого файла, перейти к просмотру информации о нем на одном или нескольких сторонних аналитических ресурсах (например, VirusTotal), чтобы расследовать причины такой активности.

> **Примечание.** Список ссылок на внешние ресурсы настраивается администратором PT NAD.

Из карточки сессии или атаки

- Чтобы из карточки сессии или атаки перейти к просмотру информации о файле:

  1. Откройте карточку сессии (см. раздел 9.2) или карточку атаки (см. раздел 10.2), в ходе которых передавался файл.
  2. В списке файлов нажмите справа от файла.
  3. В открывшемся окне перейдите по ссылке на интересующий вас внешний ресурс.

     В новой вкладке браузера откроется страница внешнего ресурса с информацией о файле.

Из виджета

- Чтобы из виджета перейти к просмотру информации о файле:

  1. Наведите курсор на хеш-сумму файла и нажмите на появившийся значок .
  2. В открывшемся окне перейдите по ссылке на интересующий вас внешний ресурс.

     В новой вкладке браузера откроется страница внешнего ресурса с информацией о файле.

19. Регистрация инцидента в MaxPatrol 10

PT NAD может быть интегрирован с MaxPatrol 10 — системой, обеспечивающей комплексный мониторинг информационной безопасности IT-инфраструктуры предприятия. Основная цель такой интеграции — периодический обмен данными.

Если интеграция настроена, то вы можете зарегистрировать инцидент в MaxPatrol 10 на основе метаданных трафика, захваченного PT NAD.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы зарегистрировать инцидент в MaxPatrol 10:

  1. В главном меню выберите **Сессии** или **Атаки**.
  2. В таблице выберите записи сессий или атак.
  3. Нажмите **Зарегистрировать инцидент**.
  4. Укажите информацию об инциденте.
  5. Нажмите **Зарегистрировать**.

  Инцидент зарегистрирован. Вы можете просмотреть его карточку, перейдя по ссылке в появившемся уведомлении.

Кроме того, вы можете зарегистрировать инцидент из карточки сессии или атаки по кнопке **Зарегистрировать инцидент**.

20. Управление работой PT NAD

Вы можете управлять работой PT NAD при наличии у вас соответствующих привилегий. Управление осуществляется на страницах, доступных в главном меню по кнопке .

В этом разделе

20.1. Управление модулями ptdpi и фильтрами захвата трафика

PT NAD захватывает трафик с помощью модулей ptdpi подсистемы захвата. Список подключенных модулей ptdpi и фильтров захвата трафика отображается на странице **Сенсоры**, доступной из меню администрирования (кнопка в главном меню).

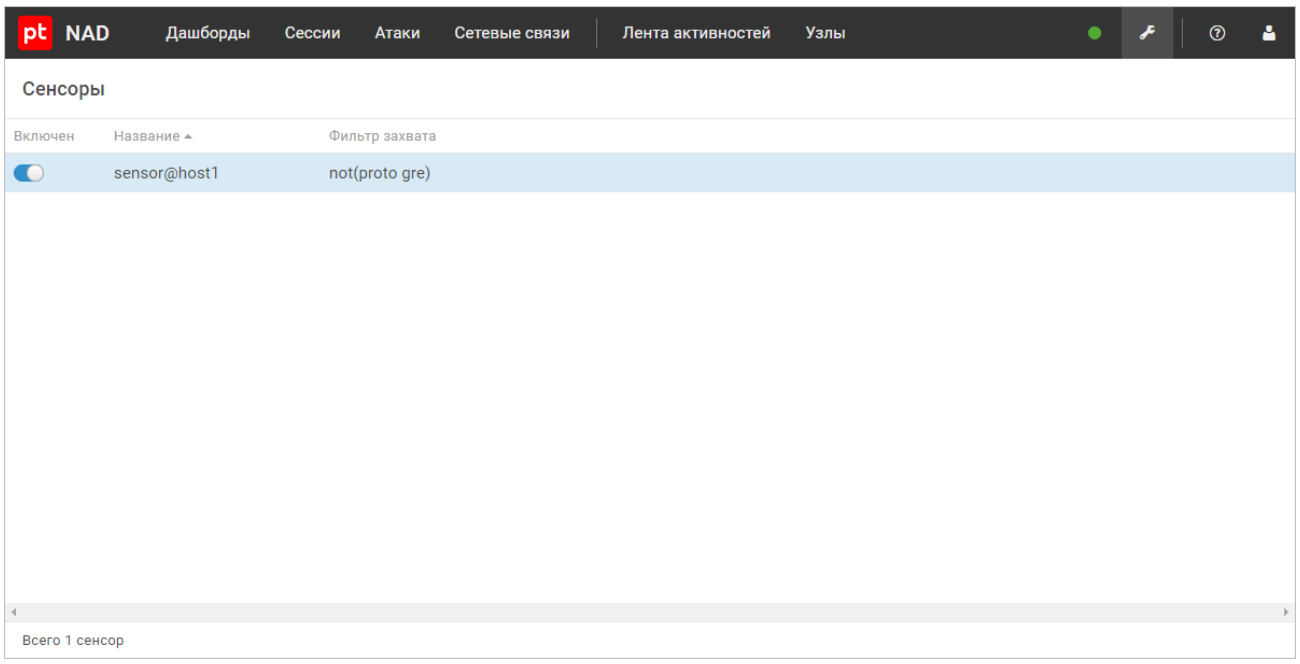


Рисунок 76. Управление модулями ptdpi и фильтрами захвата трафика

Для каждого модуля ptdpi указаны параметры:

— модуль ptdpi запущен или остановлен ;

— название;

— фильтр захвата трафика.

Вы можете настраивать фильтр захвата трафика на модулях ptdpi:

— по IP-адресу или группе IP-адресов;

— IP-подсети или группе IP-подсетей;

— сетевому порту или группе портов;

— протоколу транспортного уровня.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

20.1.1. Создание фильтра захвата трафика на модуле ptdpi

С помощью фильтра захвата трафика вы можете исключить трафик, удовлетворяющий определенным критериям, из обработки PT NAD. Например, вы можете исключить из обработки трафик, приходящий с определенного IP-адреса.

► Чтобы создать фильтр захвата трафика на модуле ptdpi:

1. В главном меню выберите → **Сенсоры**.
2. В строке с модулем ptdpi откройте поле для ввода фильтра захвата трафика по ссылке **Добавить фильтр**.

   Откроется поле фильтра захвата трафика.
3. Введите параметры фильтра захвата трафика на языке фильтрации BPF (см. раздел 20.1.6).

Внимание! Количество параметров и логических операций в выражении для фильтрации влияет на скорость обработки трафика. Чем сложнее выражение, тем больше проверок проводится и тем медленнее обрабатывается трафик. Использование длинных сложных выражений также может привести к снижению производительности PT NAD и потере данных при захвате трафика.

4. Нажмите клавишу Enter.

   Внимание! После ввода параметров продукт начнет их обработку. Не закрывайте страницу прежде, чем обработка закончится.

Фильтр захвата трафика на модуле ptdpi создан.

20.1.2. Запуск модуля ptdpi

- Чтобы запустить модуль ptdpi:

  1. В главном меню выберите → **Сенсоры**.
  2. Запустите модуль ptdpi в столбце **Включен**.

  Модуль ptdpi запущен и будет захватывать трафик в соответствии с указанным фильтром захвата трафика (см. раздел 20.1.4).

  Примечание. После запуска модуля ptdpi PT NAD первые пять минут оценивает трафик организации для настройки пороговых значений механизма, который выявляет нелегитимные сканирования, флуд и DDoS-атаки. Во время оценки трафика подобные активности не обнаруживаются.

20.1.3. Остановка модуля ptdpi

- Чтобы остановить модуль ptdpi:

  1. В главном меню выберите → **Сенсоры**.
  2. Остановите модуль ptdpi в столбце **Включен**.

  Модуль ptdpi остановлен и не будет захватывать трафик.

20.1.4. Изменение фильтра захвата трафика на модуле ptdpi

- Чтобы изменить фильтр захвата трафика на модуле ptdpi:

  1. В главном меню выберите → **Сенсоры**.
  2. В строке с модулем ptdpi нажмите на фильтр захвата трафика.

     Откроется поле фильтра захвата трафика.

3. Измените параметры фильтра захвата трафика на языке фильтрации BPF (см. раздел 20.1.6).
4. Нажмите клавишу Enter.

   Внимание! После ввода параметров продукт начнет их обработку. Не закрывайте страницу прежде, чем обработка закончится.

Фильтр захвата трафика на модуле ptdpi изменен.

20.1.5. Удаление фильтра захвата трафика на модуле ptdpi

► Чтобы удалить фильтр захвата трафика на модуле ptdpi:

1. В главном меню выберите → **Сенсоры**.
2. В строке с модулем ptdpi нажмите на фильтр захвата трафика.

   Откроется поле фильтра захвата трафика.
3. Очистите поле фильтра захвата трафика.
4. Нажмите клавишу Enter.

Фильтр захвата трафика на модуле ptdpi удален.

20.1.6. Параметры фильтрации захвата трафика

Чтобы настроить фильтрацию захвата трафика, вам нужно написать выражение на языке фильтрации Berkeley Packet Filter (BPF) и ввести его в параметрах модуля ptdpi (см. раздел 20.1.1).

Таблица 3. Примеры выражений для фильтрации захвата трафика

Фильтр	Пример выражения
По IP-адресу	`host 198.51.100.13`
По доменному имени	`host example.com`
По группе IP-адресов и доменов	`host 203.0.113.13 or host example.net or host 192.0.2.251`
По IP-подсети	`net 203.0.113.0/24`
По группе IP-подсетей	`net 203.0.113.0/24 or net 198.51.100.0/24`
По всему трафику, кроме определенных подсетей	`not(net 203.0.113.0/24 or net 198.51.100.0/24)`
По сетевому порту	`port 13090`
По диапазону портов	`portrange 100-4001`

Фильтр	Пример выражения
По протоколам транспортного уровня	`udp or tcp`
По всему трафику, кроме определенной подсети, при использовании VLAN	`not (vlan and ip and net 198.51.100.0/24)`
По всему трафику, кроме определенной подсети, при использовании VLAN или без него	`not ((ip and net 198.51.100.0/24) or (vlan and ip and net 198.51.100.0/24))`

20.2. Работа с правилами для обнаружения атак

PT NAD обнаруживает атаку или фазу ее проведения с помощью правил для атак (см. раздел 2.2).

Правила пишутся на специализированном языке (см. приложение Ж).

> **Внимание!** Для корректной работы правил вам нужно настроить группы узлов и группы портов (см. раздел 20.7).

Вы можете отмечать ложные срабатывания правил в свойствах атак (см. раздел 10.12.1).

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

20.2.1. Просмотр списка правил для обнаружения атак

- Чтобы просмотреть список правил для обнаружения атак,

  в главном меню выберите → **Правила для атак**.

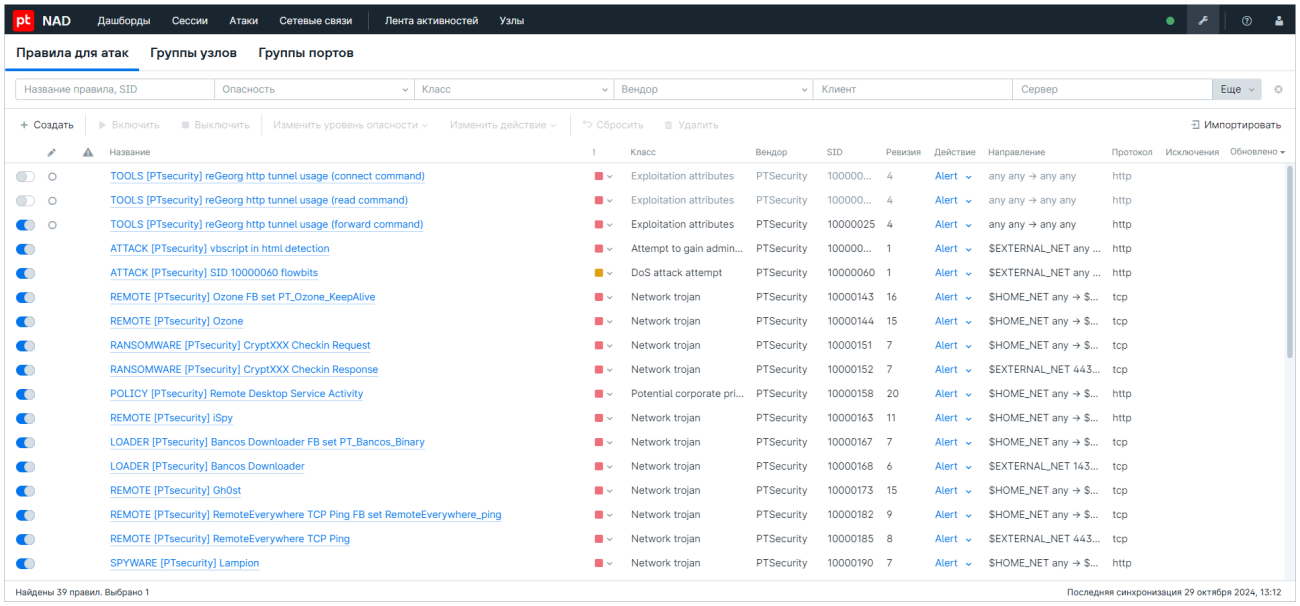


Рисунок 77. Просмотр таблицы правил для обнаружения атак

Для каждого правила указаны следующие данные:

- **Включено** — управление состоянием правила.
- **Пользовательские изменения** ( ) — наличие в строке правила значка говорит о том, что правило было изменено вами или другим пользователем PT NAD (если правило пользовательское, то значок указывает на отличие правила от его первоначальной версии).
- **Ошибки** ( ) — наличие значка в строке правила означает, что PT NAD обнаружил ошибки в правиле при его валидации (текст ошибки отображается по наведению курсора на этот значок).
- **Название** — название правила и записей об атаках, которые генерируются при срабатывании правила.
- **!** — уровень опасности атак, записи о которых генерируются при срабатывании правила.
- **Класс** — класс атак или других событий ИБ, записи о которых генерируются при срабатывании правила.
- **Вендор** — поставщик правила (у пользовательских правил вместо наименования вендора написано **<local>**).
- **SID** — идентификационный номер правила в продукте.
- **Ревизия** — версия правила (обновляется при изменении названия, класса или текста правила).
- **Действие** — реакция на срабатывание правила (**Pass** — сетевое взаимодействие безопасно, никаких действий не выполняется; **Alert** — предупреждение об атаке).

— **Направление** — адреса и сетевые порты отправителей и получателей сетевых запросов, для которых срабатывает правило, в формате `<Сети отправителей> <Порты отправителей>` → `<Сети получателей> <Порты получателей>`.

— **Протокол** — название протокола транспортного или прикладного уровня, для которого срабатывает правило.

— **Исключения** — количество исключений из правила.

— **Обновлено** — дата и время появления текущей ревизии правила (для первой ревизии — дата и время создания правила).

В списке правил для обнаружения атак вы можете:

— Включать и выключать правила для обнаружения атак. Выключенные правила не используются для анализа трафика.

— Изменять уровень опасности атаки.

— Изменять действие.

— Восстанавливать исходное значение.

— Удалять пользовательские правила.

Для ускорения работы вы можете выполнять эти действия одновременно с несколькими правилами для обнаружения атак.

> **Примечание.** Действия недоступны для правил Positive Technologies, которые используются для поиска опасных или потенциально опасных активностей.

Любые изменения в списке правил для обнаружения атак вступают в силу только после синхронизации (см. раздел 20.2.8).

20.2.2. Просмотр подробной информации о правиле для обнаружения атаки

На странице **Правила для атак** в таблице отображается краткая информация о правилах для обнаружения атак (см. раздел 10). Подробная информация о каждом правиле отображается в его карточке.

В поле **Правило** представлен текст, соответствующий синтаксису сигнатурного движка (см. приложение Ж). Вы можете частично менять текст правила.

> **Примечание.** Правила Positive Technologies, которые используются для поиска опасных или потенциально опасных активностей, не используют сигнатурный движок — такие правила не представлены в текстовом виде.

Если правило было изменено, то в поле **Исходное правило** отображается текст его исходной версии.

Если в правиле изменились название, класс или текст, то в поле **Ревизия** отображается новый номер версии правила, а в поле **Обновлено** — дата и время появления новой ревизии.

Вендор может поставлять вместе с правилом информацию об атаках, которые оно обнаруживает. Эта информация отображается в разделе **Обнаруживаемая атака** карточки правила и может включать в себя:

- описание уязвимости, эксплуатируемой злоумышленниками для совершения атаки;
- наименование ПО, используемого для совершения атаки;
- указание на методы, применяемые при совершении атаки;
- последовательность действий злоумышленников;
- рекомендации для операторов при обнаружении атаки;
- ссылки на описание атаки в базах знаний CVE, Securelist, MITRE ATT&CK и других.

Переход к карточке правила из списка правил

Вы можете просмотреть подробную информацию о правиле, открыв его карточку из списка всех правил. Такой способ просмотра может пригодиться при работе с несколькими правилами, например при их сравнении и групповом изменении.

- Чтобы перейти к карточке правила из списка правил:

  1. В главном меню выберите → **Правила для атак**.
  2. По ссылке в столбце **Название** откройте карточку правила.

Переход к карточке правила из карточки атаки

Просмотрев сведения об атаке (см. раздел 10.2), вы можете быстро перейти к изучению подробной информации о сработавшем правиле.

Примечание. PT NAD может обнаружить атаку в ходе детектирования опасной или потенциально опасной активности. В таких случаях (если атака не связана с флудом, сканированиями и ICMP-туннелями) из карточки атаки вы можете перейти к карточке правила для активности, связанной с этой атакой.

- Чтобы перейти к карточке правила из карточки атаки,

  нажмите **Перейти к правилу**.

Переход к карточке правила из карточки сессии

Просмотрев сведения о сессии (см. раздел 9.2) с атакой, вы можете быстро перейти к изучению подробной информации о сработавшем правиле.

Примечание. PT NAD может обнаружить атаку в ходе детектирования опасной или потенциально опасной активности. В таких случаях (если атака не связана с флудом, сканированиями и ICMP-туннелями) переход выполняется к карточке правила для активности, связанной с этой атакой.

- Чтобы перейти к карточке правила из карточки сессии,

  в блоке **Атаки** нажмите ⋮ и выберите **Перейти к правилу**.

20.2.3. Поиск правил для обнаружения атак

Вы можете искать правила для обнаружения атак с помощью панели фильтрации правил.

- Чтобы найти правила для обнаружения атак:

  1. В главном меню выберите → **Правила для атак**.
  2. Если вам нужно выполнить поиск только среди правил с ошибками (см. раздел 20.2.8), нажмите на ссылку слева от количества правил, в которых обнаружены ошибки.
  3. Если вам нужно выполнить поиск только среди правил с изменениями, которые были удалены, изменены или добавлены вами или другими пользователями PT NAD, но еще не прошли синхронизацию (см. раздел 20.2.8), нажмите на ссылку слева от количества измененных правил.

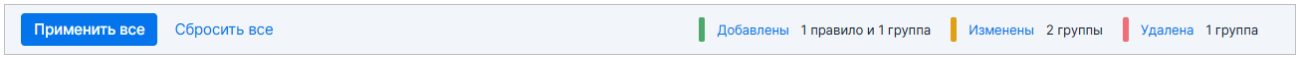


Рисунок 78. Фильтрация правил и групп с изменениями

Если выбранные изменения были не только в правилах для атак, но и в группах узлов или портов (см. раздел 20.7), то эти группы будут также отфильтрованы. Вы можете сбросить все примененные фильтры по кнопке ⊗, при переходе на другую страницу интерфейса они не сохраняются.

  4. Если вам нужно выполнить поиск по параметрам, настройте их в панели фильтрации.

     Примечание. В полях **Клиент** и **Сервер** вы можете ввести диапазоны адресов, подсети и названия групп узлов (см. раздел 20.7) в формате $<Название группы>. При поиске не учитываются отдельные IP-адреса, входящие в диапазоны, подсети или группы узлов, указанные в правилах.

     PT NAD выполнит точный поиск по полям **Откуда** (для клиентов) и **Куда** (для серверов) из карточек правил.

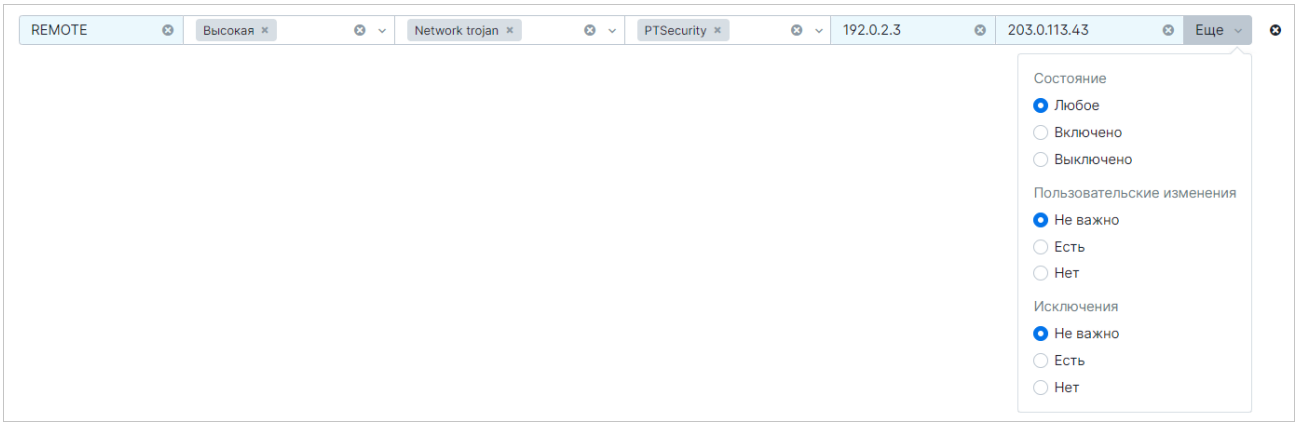


Рисунок 79. Параметры фильтрации правил

Вы можете очистить параметры фильтрации по кнопке . При переходе на другую страницу интерфейса параметры не сохраняются.

20.2.4. Импорт правил для обнаружения атак

Вы можете загружать правила для обнаружения атак в PT NAD. Правила загружаются в виде файлов .rules в архиве .tar.gz.

- Чтобы импортировать правила для обнаружения атак:

  1. В главном меню выберите → **Правила для атак**.
  2. Нажмите **Импортировать**.
  3. Выберите вендора или добавьте нового.
  4. Перетащите архив с правилами в область загрузки или добавьте его по ссылке **выберите**.
  5. Нажмите **Импортировать**.

  Продукт начнет использовать импортированные правила для анализа трафика только после их включения и синхронизации (см. раздел 20.2.8).

20.2.5. Создание правила для обнаружения атаки

- Чтобы создать правило для обнаружения атаки:

  1. В главном меню выберите → **Правила для атак**.
  2. Нажмите **Создать**.
  3. Заполните поля в карточке.

При заполнении поля **Правило** должен соблюдаться синтаксис (см. приложение Ж).

4. Нажмите **Создать**.

   Продукт начнет использовать созданное правило для анализа трафика только после синхронизации (см. раздел 20.2.8).

20.2.6. Копирование правила для обнаружения атаки

Вы можете создавать правила для обнаружения атак на основе имеющихся. Например, на основе сложного правила вендора создать пользовательское, заменив только один параметр.

Для создания правила на основе имеющегося нужно скопировать исходное правило.

> **Примечание.** Инструкция неприменима к правилам Positive Technologies, которые используются для поиска активностей, связанных с флудом, сканированиями и ICMP-туннелями.

- Чтобы скопировать правило для обнаружения атаки:

1. В главном меню выберите → **Правила для атак**.
2. По ссылке в столбце **Название** откройте карточку правила.
3. Нажмите **Создать копию**.
4. Если требуется, измените параметры правила.
5. Нажмите **Копировать**.

   > **Примечание.** При изменении правила запускается автоматическая проверка синтаксиса. Продукт не сохранит правило, пока ошибки не будут исправлены. Вы можете посмотреть исходный и измененный текст правила в окне **Копирование правила**.

Продукт начнет использовать скопированное правило для анализа трафика только после синхронизации (см. раздел 20.2.8).

20.2.7. Изменение правила для обнаружения атаки

Вы можете изменять правила для обнаружения атак. У правил вендоров вы можете изменять действие, уровень опасности и адреса отправителей и получателей сетевых запросов. У пользовательских правил вы можете изменять любые параметры, кроме идентификаторов (SID) и номеров ревизий.

> **Примечание.** Инструкция неприменима к правилам Positive Technologies, которые используются для поиска активностей, связанных с флудом, сканированиями и ICMP-туннелями.

- Чтобы изменить правило для обнаружения атаки:

  1. В главном меню выберите → **Правила для атак**.
  2. По ссылке в столбце **Название** откройте карточку правила.
  3. Нажмите **Изменить**.
  4. Измените правило.
  5. Нажмите **Сохранить**.

     Примечание. При изменении правила запускается автоматическая проверка синтаксиса. Продукт не сохранит правило, пока ошибки не будут исправлены. Вы можете посмотреть исходный и измененный текст правила в окне **Изменение правила**.

     Примечание. Если требуется вернуть исходные значения измененных полей, нажмите кнопку **Сбросить изменения** в карточке правила. Действие недоступно для пользовательских правил, у которых изменился номер ревизии (изменились название, класс или текст правила). Кроме того, в строках с такими правилами в столбце не отображается значок .

  Продукт начнет использовать измененное правило для анализа трафика только после синхронизации (см. раздел 20.2.8).

Кроме того, для каждого правила вы можете изменить уровень опасности в столбце таблицы **!** и действие — в столбце **Действие**.

20.2.8. Синхронизация правил для обнаружения атак

Изменения, внесенные в правила для обнаружения атак, не вступают в силу сразу. PT NAD запоминает их, и вы можете применить их все вместе или отклонить. Такое применение называется синхронизацией.

Все изменения отображаются под главным меню на странице **Правила для атак**. Дата последней успешной синхронизации отображается в нижней части страницы.

Изменения в правилах для обнаружения атак и в группах узлов и портов синхронизируются одновременно. Во время синхронизации PT NAD проверяет корректность изменений. Если ошибок нет, все изменения в правилах для обнаружения атак и в группах узлов и портов вступают в силу. При наличии ошибок в строках правил и групп узлов и портов, в которых обнаружены ошибки, отображается значок . При наличии критически значимых ошибок синхронизация может быть выполнена только после их исправления.

- Чтобы применить все изменения, внесенные с момента последней синхронизации,

  нажмите **Применить все**.

- Чтобы отменить все изменения, внесенные с момента последней синхронизации,

  нажмите **Сбросить все**.

20.3. Работа с правилами для обнаружения активностей

PT NAD обнаруживает опасную и потенциально опасную активность в сети организации с помощью правил для активностей (см. раздел 2.2).

Вы можете выключать и включать правила, менять уровни опасности для обнаруживаемых активностей, а также создавать, изменять и удалять пользовательские правила на основе фильтров (см. раздел 13). Правила по личным фильтрам (личные правила) работают только для вашей учетной записи, тогда как правила по общим фильтрам (общие правила) генерируют записи в ленту активностей для всех пользователей.

Кроме того, при создании пользовательских правил на основе фильтров вы можете настроить обучение правил (см. раздел 20.3.10).

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

См. также

20.3.1. Просмотр списка правил для активностей

- Чтобы просмотреть список правил для активностей,

  в главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

  Откроется страница **Правила для активностей**.

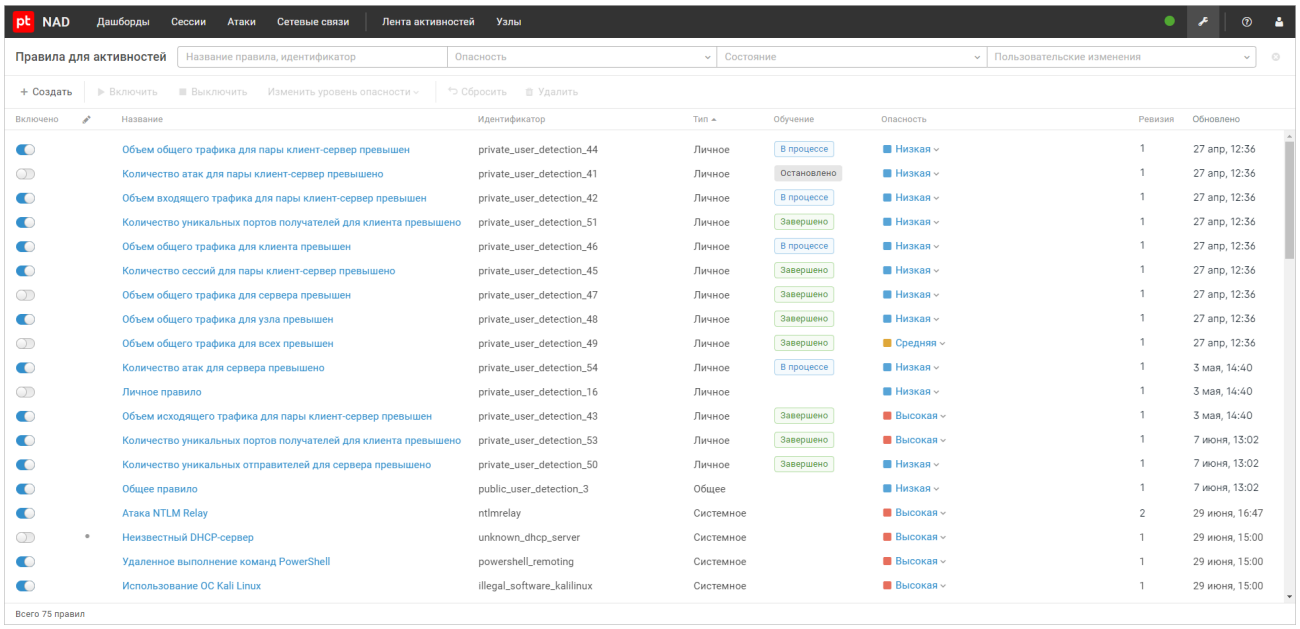


Рисунок 80. Просмотр таблицы правил для обнаружения активностей

Для каждого правила указаны следующие данные:

— **Включено** — управление состоянием правила.

— **Пользовательские изменения** ( ) — наличие в строке правила значка говорит о том, что системное правило было изменено вами или другим пользователем PT NAD. В пользовательских правилах изменения не отслеживаются.

— **Название** — название правила и записей в ленте активности, которые генерируются при срабатывании правила.

— **Идентификатор** — текстовый идентификатор правила в продукте.

— **Тип** — тип правила:

  - **Системное** — правило, поставляемое из базы знаний экспертного центра Positive Technologies;
  - **Общее** — пользовательское правило по общему фильтру;
  - **Личное** — пользовательское правило по личному фильтру.

— **Обучение** — статус обучения пользовательского правила, если обучение настроено. По нажатию на статус открывается окно с информацией об обучении.

— **Опасность** — уровень опасности активностей, записи о которых генерируются в ленте активностей при срабатывании правила.

— **Ревизия** — версия правила.

— **Обновлено** — дата и время появления текущей ревизии правила (для первой ревизии — дата и время создания правила).

20.3.2. Просмотр подробной информации о правиле для активности

На странице **Правила для активностей** в таблице отображается краткая информация о правилах для обнаружения активностей (см. раздел 14). Вы можете просмотреть подробную информацию о правиле в его карточке. Карточка правила также содержит подробную информацию об активности, обнаруживаемой этим правилом.

Из списка правил

► Чтобы перейти к карточке правила из списка правил:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.

2. По ссылке в столбце **Название** откройте карточку правила.

Из карточки активности

► Чтобы перейти к карточке правила из карточки активности, сгенерированной по срабатыванию этого правила:

1. В главном меню выберите **Лента активностей**.
2. По ссылке с названием активности откройте карточку активности.
3. По кнопке **Перейти к правилу** откройте карточку правила.

Из карточки атаки

PT NAD может обнаружить атаку в ходе детектирования опасной или потенциально опасной активности. Вы можете перейти из карточки подобной атаки к просмотру правила для активности, связанной с этой атакой.

- Чтобы перейти к карточке правила для активности из карточки атаки:

  1. В главном меню выберите **Атаки**.
  2. Откройте карточку атаки по кнопке ↙↗ в строке этой атаки.
  3. Нажмите кнопку **Перейти к правилу для активности**.

Из карточки сессии с атакой

PT NAD может обнаружить атаку в ходе детектирования опасной или потенциально опасной активности. Вы можете перейти из карточки сессии, в ходе которой была обнаружена подобная атака, к просмотру правила для активности, связанной с этой атакой.

- Чтобы перейти к карточке правила для активности из карточки сессии:

  1. В главном меню выберите **Сессии**.
  2. Откройте карточку сессии, нажав ↙↗ в строке этой сессии.
  3. В блоке атаки нажмите ⋮ и в раскрывшемся меню выберите пункт **Перейти к правилу для активности**.

20.3.3. Поиск правил для обнаружения активностей

- Чтобы найти правила для обнаружения активностей:

  1. В главном меню нажмите 🔧 и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

  2. Настройте параметры фильтрации активностей в панели фильтрации.

Рисунок 81. Параметры фильтрации правил для активностей

В таблице отобразятся только те активности, которые подходят под указанные вами параметры фильтрации. Внизу страницы будет показано количество найденных активностей.

В панели фильтрации можно настроить следующие параметры:

- **Название правила, идентификатор** — поиск правила по его идентификатору или по названию обнаруживаемой активности.
- **Опасность** — поиск правила по уровню опасности обнаруживаемой им активности.
- **Состояние** — поиск правила по его состоянию (включено или выключено).

- **Пользовательские изменения** — поиск правила по наличию в нем пользовательских изменений.

  Примечание. Вы можете очистить параметры фильтрации по кнопке ✕. При переходе на другую страницу интерфейса параметры не сохраняются.

20.3.4. Включение и выключение правила для активности

Вы можете включить или выключить правило для обнаружения активности. Выключенное правило не используется для анализа трафика.

► Чтобы включить или выключить правило для обнаружения активности:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.

2. Включите или выключите правило в столбце **Включено**.

Вы также можете включать и выключать правило в его карточке (см. раздел 20.3.2).

См. также

Включение и выключение нескольких правил для активностей (см. раздел 20.3.13.1)

20.3.5. Изменение уровня опасности активности

Вы можете настроить приоритеты для обработки записей в ленте активностей. Для этого вам нужно выбрать уровень опасности, который PT NAD будет присваивать обнаруживаемой активности при срабатывании соответствующего правила.

Примечание. Если вы измените уровень опасности в правиле, PT NAD установит новый уровень опасности в уже существующей записи в ленте активностей (см. раздел 14) только после того, как в ней будут обновлены любые данные о трафике. В остальных существующих записях уровень опасности останется прежним.

► Чтобы изменить уровень опасности активности:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.

2. В строке с правилом, с помощью которого обнаруживается активность, в столбце **Опасность** выберите новый уровень опасности.

Уровень опасности активности изменен.

Все новые активности, которые PT NAD обнаружит с помощью правила, будут иметь выбранный уровень опасности.

Вы также можете изменить уровень опасности для активности в карточке правила (см. раздел 20.3.2), с помощью которого обнаруживается эта активность.

См. также

Изменение уровня опасности нескольких активностей (см. раздел 20.3.13.2)

20.3.6. Сброс пользовательских изменений в правиле для активности

Вы можете вернуть значения по умолчанию у системного правила для активности, в котором были пользовательские изменения.

В списке всех правил для активностей

- Чтобы сбросить пользовательские изменения в правиле в списке правил:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

  2. Выберите системное правило.

     Вы можете воспользоваться поиском (см. раздел 20.3.3), чтобы найти нужное правило.

     Правила с пользовательскими изменениями помечаются значком в столбце . Уровень опасности по умолчанию будет отображаться в раскрывающемся списке **Опасность**.

  3. В панели инструментов нажмите кнопку **Сбросить** и подтвердите сброс.

  Пользовательские изменения в правиле сброшены.

В карточке правила для активности

- Чтобы сбросить пользовательские изменения в правиле в его карточке:

  1. Перейдите к карточке правила (см. раздел 20.3.2).

     Уровень опасности по умолчанию будет отображен в карточке правила в раскрывающемся списке **Опасность**.

  2. Нажмите кнопку **Сбросить изменения** и подтвердите сброс.

  Пользовательские изменения в правиле сброшены.

См. также

Сброс пользовательских изменений в нескольких правилах для активностей (см. раздел 20.3.13.3)

20.3.7. Создание правила для активности в таблице всех правил

В процессе работы с правилами для активностей вы можете создать собственное правило, не покидая страницу со списком правил.

Перед выполнением инструкции нужно убедиться в наличии фильтра (см. раздел 13), который вы будете использовать в качестве условия срабатывания правила.

► Чтобы создать правило для активности в таблице всех правил:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание правила для активности по фильтру**.

3. В поле **Название** введите название правила для активности.

   Введенное значение будет использоваться также для названия активности, генерируемой правилом.

4. Выберите тип правила и уровень опасности для активности.
5. Если требуется, настройте обучение правила (см. раздел 20.3.10).
6. В блоке **Срабатывание правила** настройте параметры срабатывания правила:
   - Выберите фильтр для трафика.
   - Настройте условие, по наступлению которого PT NAD должен уведомлять об активности.
   - Укажите, как часто PT NAD должен проверять наступление этого условия.
   - Если требуется, включите отправку уведомлений о новых активностях на вашу электронную почту (см. раздел 21.1). Эта функция действует только для личного правила.
7. Если вам нужно, чтобы запись об активности помимо общих содержала дополнительные данные отфильтрованных сессий, в блоке **Добавление данных в запись об активности**:
   - По кнопке **Добавить данные** добавьте дополнительные данные для отображения.

- Если вам нужно группировать дополнительные данные, установите флажок **Группировать по параметру** и в раскрывающемся списке выберите параметр, по которому должна производиться группировка.
- Выберите вариант представления дополнительных данных (табличный или списком).

8. Если требуется, по кнопкам **Добавить описание** и **Добавить рекомендации** добавьте описание обнаруживаемой активности и рекомендации для оператора.
9. Нажмите кнопку **Создать**.

Правило для активности создано.

См. также

Создание правил для активностей в списке фильтров (см. раздел 20.3.8)

20.3.8. Создание правил для активностей в списке фильтров

Правила для активностей можно создавать в списке фильтров (см. раздел 13). Этот способ удобен тем, что позволяет сравнивать параметры нескольких правил в одном окне. Кроме того, вы можете добавлять правила для активностей сразу после создания фильтра и видеть, по каким из фильтров правила уже существуют.

► Чтобы создать правила для активностей в списке фильтров:

1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
2. В панели фильтрации нажмите ☰.

   Откроется список сохраненных фильтров.
3. Наведите курсор на строку с фильтром и нажмите ссылку **Настройка правил**.

   Откроется окно **<Тип правил> правила для активностей по фильтру «<Название фильтра>»**, например **Личные правила для активностей по фильтру «Трафик на узел 203.0.113.13 с DGA»**.
4. Нажмите кнопку **Добавить правило**.

   Появятся параметры правила для активности.
5. В поле **Название** введите название правила для активности.

   Введенное значение будет использоваться также для названия активности, генерируемой правилом.
6. Выберите уровень опасности для активности.
7. Если требуется, настройте обучение правила (см. раздел 20.3.10).
8. В блоке **Срабатывание правила** настройте параметры срабатывания правила:

- Настройте условие, по наступлению которого PT NAD должен уведомлять об активности.
- Укажите, как часто PT NAD должен проверять наступление этого условия.
- Если требуется, включите отправку уведомлений о новых активностях на вашу электронную почту (см. раздел 21.1). Эта функция действует только для личного правила.

9. Если вам нужно, чтобы запись об активности помимо общих содержала дополнительные данные отфильтрованных сессий, в блоке **Добавление данных в запись об активности**:
   - По кнопке **Добавить данные** добавьте дополнительные данные для отображения.
   - Если вам нужно группировать дополнительные данные, установите флажок **Группировать по параметру** и в раскрывающемся списке выберите параметр, по которому должна производиться группировка.
   - Выберите вариант представления дополнительных данных (табличный или списком).
10. Если требуется, по кнопкам **Добавить описание** и **Добавить рекомендации** добавьте описание обнаруживаемой активности и рекомендации для оператора.
11. Если вам нужно добавить еще одно правило для активности по тому же фильтру, нажмите на ссылку **Добавить правило** и повторите инструкцию.
12. Нажмите кнопку **Сохранить**.

Правила для активностей по фильтру созданы.

Фильтры, по которым были настроены правила для активностей, помечаются значком .

Рисунок 82. Фильтр, по которому были созданы правила для активностей

См. также

Создание правила для активности в таблице всех правил (см. раздел 20.3.7)

20.3.9. Изменение правила для активности

Инструкция применима только для пользовательских правил. В случае с системными правилами вы можете изменять только уровень опасности активности (см. раздел 20.3.5).

Если для правила настроено обучение, вы можете изменять период обучения и уровень чувствительности правила, а также включать и выключать автоматическое переобучение правила.

- Чтобы изменить правило для активности:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.
  2. По ссылке в столбце **Название** откройте карточку правила.
  3. Нажмите **Изменить**.

     Откроется окно **Изменение правила**.
  4. Измените правило.
  5. Нажмите кнопку **Сохранить**.

  Правило для активности изменено.

20.3.10. Настройка обучения правила для активности

При создании правила для активности в таблице всех правил (см. раздел 20.3.7) или в списке фильтров (см. раздел 20.3.8) можно настроить обучение правила (см. раздел 2.2). Для правила с настроенным обучением порог срабатывания определяется автоматически на основе реальных данных о трафике.

Пользовательское правило для активности с обучением может понадобиться, например, для следующих целей:

- **Контроль объема трафика между организацией и сервисами облачного хранения.** В этом случае вам не требуется самостоятельно оценивать объем трафика и задавать порог срабатывания вручную. Правило обучится на основе данных, собранных за период обучения, и будет срабатывать на аномальные превышения объема трафика. С помощью этого правила можно вовремя обнаружить такие угрозы ИБ, как эксфильтрация данных злоумышленником или загрузка вредоносного ПО. Для создания правила вы можете использовать фильтр `app_service in ["<Название 1>","<Название 2>"]`, указав названия облачных сервисов, например `app_service in ["Yandex.disk","DropBox","MEGA"]`. Кроме того, установив высокую чувствительность для правила, вы можете отследить даже небольшие аномалии в трафике и, как следствие, обнаружить загрузку или эксфильтрацию незначительных объемов данных злоумышленником.
- **Контроль объема трафика, поступающего в сеть организации от внешних узлов.** С помощью этого правила можно обнаружить, например, туннель или подбор учетных данных. Для создания правила вы можете использовать фильтр `src.groups == EXTERNAL_NET`.

Трафик, связанный с такими корпоративными сервисами, как VPN, можно исключить из анализа при помощи фильтра `not host.ip == <IP-адрес сервиса>`, например `not host.ip == 203.0.113.3`.

— **Контроль количества сессий с ошибками аутентификации Kerberos.** В процессе обучения PT NAD отслеживает всплески количества этих сессий, которые могут быть связаны, например, с истечением срока действия паролей пользователей. Обученное правило будет считать подобные всплески легитимными и срабатывать только на аномальные превышения количества сессий. Увеличение количества сессий с неверным паролем или ненайденным пользователем может свидетельствовать об атаке методом перебора учетных данных (например, о спреинге паролей). Для создания правила вы можете использовать фильтр `kerberos.rsp.error_code == KDC_ERR_PREAUTH_FAILED` или `kerberos.rsp.error_code == KDC_ERR_C_PRINCIPAL_UNKNOWN`.

► Чтобы настроить обучение при создании правила для активности:

1. Включите обучение правила.

   В блоке **Срабатывание правила** отобразятся параметры для настройки обучения.

2. Если вы создаете правило в таблице всех правил для активностей, выберите фильтр для трафика.

3. Укажите период обучения правила.

   Минимальный период обучения правила — 7 дней. Чем больше период, тем больше данных PT NAD соберет для анализа и тем точнее определит порог срабатывания правила.

   Примечание. Вы можете изменять период обучения при изменении правила (см. раздел 20.3.9), для которого настроено обучение.

4. Если не требуется перезапускать обучение правила для активности (см. раздел 20.3.11) автоматически, выключите переобучение правила.

   Примечание. Вы можете включать и выключать переобучение при изменении правила (см. раздел 20.3.9), для которого настроено обучение.

5. Выберите объект мониторинга и параметр, о превышении порогового значения которого должен уведомлять PT NAD.

6. Выберите уровень чувствительности правила.

   Чувствительность влияет на порог срабатывания правила. Чем она выше, тем ниже порог и тем выше вероятность срабатывания. При создании правила с обучением рекомендуется оставить чувствительность по умолчанию. Вы можете изменить чувствительность, если необходимо отрегулировать количество уведомлений в ленте активностей: увеличить — если требуется уведомлять даже о незначительных превышениях параметра, или уменьшить — если правило генерирует излишнее количество срабатываний.

Примечание. Вы можете изменять уровень чувствительности при изменении правила (см. раздел 20.3.9), для которого настроено обучение.

Обучение правила для активности настроено.

PT NAD выполняет первичное обучение, если оно было настроено, сразу после создания правила для активности.

Примечание. Правило для активности, для которого выполняется обучение, не используется для анализа трафика. Продукт начнет использовать правило только после успешного завершения обучения.

20.3.11. Перезапуск обучения правила для активности

Вы можете перезапускать обучение (см. раздел 2.2) пользовательских правил для активностей вручную, если оно настроено. Кроме того, для таких правил вы можете включить автоматическое переобучение. При перезапуске вручную обучение выполняется сразу же и всего один раз. При включенном переобучении повторное обучение правила выполняется раз в сутки автоматически.

Вы можете включить переобучение правила для активности при настройке обучения (см. раздел 20.3.10) или при изменении правила (см. раздел 20.3.9). Вручную перезапускать обучение правила для активности можно в списке всех правил, в карточке правила и в панели фильтрации.

Примечание. Инструкция неприменима к правилам, которые были выключены в процессе обучения. При включении таких правил обучение перезапустится автоматически.

В списке всех правил для активностей

- Чтобы перезапустить обучение правила для активности в списке всех правил:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

  2. В строке пользовательского правила, для которого настроено обучение, нажмите на статус в столбце **Обучение**.

     Откроется окно с информацией об обучении.

  3. Нажмите кнопку **Перезапустить** и подтвердите перезапуск.

  Обучение правила для активности перезапущено.

В карточке правила для активности

- Чтобы перезапустить обучение правила для активности в его карточке:

  1. По ссылке в столбце **Название** откройте карточку правила, для которого настроено обучение.

     Примечание. В строке такого правила в столбце **Обучение** отображается статус обучения.

  2. Нажмите кнопку **Перезапустить** и подтвердите перезапуск.

  Обучение правила для активности перезапущено.

В панели фильтрации

- Чтобы перезапустить обучение правила для активности в панели фильтрации:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите ☰.

     Откроется список сохраненных фильтров.
  3. Наведите курсор на строку с фильтром и нажмите ссылку **Настройка правил**.

     Откроется окно **<Тип правил> правила для активностей по фильтру «<Название фильтра>»**, например **Личные правила для активностей по фильтру «Трафик на узел 203.0.113.13 с DGA»**.

     Примечание. Вы можете перезапускать обучение только тех правил, для которых настроено обучение. Для таких правил в поле **Обучение правила** отображается статус обучения.
  4. Нажмите на статус в поле **Обучение правила**.

     Откроется окно с информацией об обучении.
  5. Нажмите кнопку **Перезапустить** и подтвердите перезапуск.

  Обучение правила для активности перезапущено.

20.3.12. Удаление правила для активности

Вы можете удалять только пользовательские правила для активностей.

В списке всех правил для активностей

- Чтобы удалить правило для активности в списке всех правил:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

  2. Выберите пользовательское правило.

     Вы можете воспользоваться поиском (см. раздел 20.3.3), чтобы найти нужное правило.

  3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

  Правило для активности удалено.

В карточке правила для активности

- Чтобы удалить правило для активности в его карточке:

  1. Перейдите к карточке правила (см. раздел 20.3.2).
  2. Нажмите кнопку **Удалить правило** и подтвердите удаление.

  Правило для активности удалено.

В панели фильтрации

- Чтобы удалить правило для активности в панели фильтрации:

  1. В главном меню выберите **Дашборды**, **Сессии**, **Атаки** или **Сетевые связи**.
  2. В панели фильтрации нажмите .

     Откроется список сохраненных фильтров.

  3. Наведите курсор на строку с фильтром и нажмите ссылку **Настройка правил**.

     Откроется окно **<Тип правил> правила для активностей по фильтру «<Название фильтра>»**, например **Личные правила для активностей по фильтру «Трафик на узел 203.0.113.13 с DGA»**.

  4. В блоке с параметрами правила нажмите кнопку **Удалить** и подтвердите удаление.

  Правило для активности удалено.

См. также

Удаление нескольких правил для активностей (см. раздел 20.3.13.4)

20.3.13. Массовые операции с правилами для активностей

Для ускорения работы с правилами в PT NAD вы можете выполнять отдельные действия одновременно с несколькими правилами:

— включать и выключать;

— изменять уровень опасности активности;

— восстанавливать исходное значение;

— удалять пользовательские правила.

В этом разделе

Включение и выключение нескольких правил для активностей (см. раздел 20.3.13.1)

Изменение уровня опасности нескольких активностей (см. раздел 20.3.13.2)

Сброс пользовательских изменений в нескольких правилах для активностей (см. раздел 20.3.13.3)

Удаление нескольких правил для активностей (см. раздел 20.3.13.4)

20.3.13.1. Включение и выключение нескольких правил для активностей

Вы можете включать и выключать сразу несколько правил для обнаружения активностей. Выключенные правила не используются для анализа трафика.

► Чтобы включить или выключить несколько правил для обнаружения активностей:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.

2. Выберите правила в таблице.

3. В панели инструментов нажмите кнопку **Включить** или **Выключить**.

См. также

Включение и выключение правила для активности (см. раздел 20.3.4)

20.3.13.2. Изменение уровня опасности нескольких активностей

Вы можете настроить приоритеты для обработки записей в ленте активностей. Для этого вам нужно выбрать свой уровень опасности, который PT NAD будет присваивать определенным обнаруживаемым активностям при срабатывании соответствующих правил.

> **Примечание.** Если вы измените уровень опасности в правиле, PT NAD установит новый уровень опасности в уже существующей записи в ленте активностей (см. раздел 14) только после того, как в ней будут обновлены любые данные о трафике. В остальных существующих записях уровень опасности останется прежним.

- Чтобы изменить уровень опасности нескольких активностей:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

  2. Выберите правила в таблице.

  3. В панели инструментов нажмите кнопку **Изменить уровень опасности** и в раскрывшемся меню выберите новый уровень опасности.

  Уровень опасности нескольких активностей изменен.

Все новые активности, которые PT NAD обнаружит с помощью выбранных правил, будут иметь выбранный уровень опасности.

См. также

Изменение уровня опасности активности (см. раздел 20.3.5)

20.3.13.3. Сброс пользовательских изменений в нескольких правилах для активностей

Вы можете вернуть значения по умолчанию у тех системных правил для обнаружения активностей, в которых были пользовательские изменения.

- Чтобы сбросить пользовательские изменения в нескольких правилах для активностей:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Правила для активностей**.

     Откроется страница **Правила для активностей**.

Правила с пользовательскими изменениями помечаются значком ● в столбце ✎. Уровень опасности по умолчанию будет отображаться в раскрывающемся списке **Опасность**.

2. Выберите правила в таблице.
3. В панели инструментов нажмите кнопку **Сбросить** и подтвердите сброс.

Пользовательские изменения в правилах для обнаружения активностей сброшены.

См. также

Сброс пользовательских изменений в правиле для активности (см. раздел 20.3.6)

20.3.13.4. Удаление нескольких правил для активностей

Вы можете удалять только пользовательские правила для активностей.

- Чтобы удалить несколько правил для активностей:

1. В главном меню нажмите 🔧 и в раскрывшемся меню выберите пункт **Правила для активностей**.

   Откроется страница **Правила для активностей**.
2. Выберите пользовательские правила.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Правила для активностей удалены.

См. также

Удаление правила для активности (см. раздел 20.3.12)

20.4. Работа со справочниками

В этом разделе приводится описание работы с исключениями из правил для атак и с исключениями из правил для активностей.

Исключения хранятся в виде справочников на базе табличных списков. Для автоматизации работы с исключениями справочники можно составить в сторонней программе и импортировать в виде CSV-файлов в PT NAD, а также экспортировать из продукта для последующего импорта в другие экземпляры PT NAD.

Справочники исключений из правил отображаются на странице **Справочники**, доступной из меню администрирования (кнопка 🔧 в главном меню). Вы можете работать с исключениями из правил для атак и с исключениями из правил для активностей в соответствующих справочниках **Исключения для атак** и **Исключения для активностей**.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

20.4.1. Просмотр списка исключений из правил для атак

- Чтобы просмотреть список исключений из правил для атак,

  в главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

  Откроется страница **Справочники**, по умолчанию на странице отображается список исключений из правил для атак.

Для каждого исключения указаны следующие данные:

- **SID** — идентификатор правила, для которого настроено исключение. Если исключение действует для всех правил, значение отсутствует.
- **Узел отправителя** — идентификатор узла (см. раздел 15.1) отправителя.
- **IP-адрес отправителя**.
- **Домен отправителя**.
- **Группа отправителя** — группа (см. раздел 20.7), в которую входит узел отправителя.
- **Узел получателя** — идентификатор узла (см. раздел 15.1) получателя.
- **IP-адрес получателя**.
- **Домен получателя**.
- **Группа получателя** — группа (см. раздел 20.7), в которую входит узел получателя.
- **Изменено** — дата и время последнего изменения исключения.

20.4.2. Просмотр списка исключений из правил для активностей

- Чтобы просмотреть список исключений из правил для активностей:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Справочники**.

     Откроется страница **Справочники**.

  2. В панели слева выберите справочник **Исключения для активностей**.

     Отобразится список исключений из правил для активностей.

Для каждого исключения указаны следующие данные:

— **Правило для активности** — текстовый идентификатор правила для активности, к которому применяется исключение. Если исключение действует для всех правил, значение отсутствует.

— **Узел отправителя** — идентификатор узла (см. раздел 15.1) отправителя.

— **IP-адрес отправителя**.

— **Домен отправителя**.

— **Группа отправителя** — группа (см. раздел 20.7), в которую входит узел отправителя.

— **Узел получателя** — идентификатор узла (см. раздел 15.1) получателя.

— **IP-адрес получателя**.

— **Домен получателя**.

— **Группа получателя** — группа (см. раздел 20.7), в которую входит узел получателя.

— **Логин** — логин, с помощью которого была совершена попытка аутентификации.

— **Изменено** — дата и время последнего изменения исключения.

20.4.3. Добавление исключения из правила для атаки

Для повышения эффективности работы с трафиком вы можете указать, в каких случаях то или иное правило для атаки не должно срабатывать в PT NAD. Например, чтобы не тратить время на обнаружение ложных срабатываний правила, вы можете добавить IP-адреса, доменные имена, идентификаторы или группы узлов доверенных клиентов и серверов в таблицу исключений. Кроме того, внесение исключений может понадобиться, чтобы в список атак не попадали сессии, которые, по вашему мнению, не представляют интереса или реальной угрозы.

Вы можете добавить исключение из правила для обнаружения атаки:

— в карточке этого правила;

— в карточке атаки, которая была сгенерирована по срабатыванию этого правила;

— в карточке сессии с обнаруженной атакой, которая была сгенерирована по срабатыванию этого правила;

— на странице со списком всех исключений.

В этом разделе

Добавление исключения из правила в карточке атаки (см. раздел 20.4.3.1)

Добавление исключения из правила в карточке правила (см. раздел 20.4.3.2)

Добавление исключения из правила в карточке сессии (см. раздел 20.4.3.3)

Добавление исключения из правила в таблице всех исключений (см. раздел 20.4.3.4)

20.4.3.1. Добавление исключения из правила в карточке атаки

Вы можете добавить исключение из правила в карточке атаки, которая была сгенерирована по срабатыванию этого правила. Просмотрев информацию об атаке и отметив ее как ложную, вы можете в той же карточке исключить последующую генерацию аналогичных атак.

> **Примечание.** Не все атаки обнаруживаются при помощи правил для атак. Атаки могут выявляться также в ходе детектирования опасных и потенциально опасных активностей. В таких случаях (если атака не связана с флудом, сканированиями и ICMP-туннелями) нельзя добавлять исключения из правил для атак. Вместо этого вы можете добавлять исключения из правил для активностей (см. раздел 20.4.4). Для добавления исключения могут понадобиться адрес узла и идентификатор типа активности. Адрес можно найти в блоке **Атакующий узел** или **Атакуемый узел**, а идентификатор указан в скобках во всплывающем окне по кнопке рядом с кнопкой **Добавить исключение**. В этом же окне есть ссылка на таблицу исключений из правил для активностей, в которой можно добавить исключение (см. раздел 20.4.4.2).

► Чтобы добавить исключение из правила в карточке атаки:

1. В главном меню выберите **Атаки**.
2. Откройте карточку атаки по кнопке в строке этой атаки.
3. Нажмите кнопку **Добавить исключение**.

   Откроется окно для добавления исключения. Если вы или другой пользователь PT NAD ранее создавали исключения, связанные с выбранной атакой, информация о них будет приведена в блоке **Действующие исключения**.
4. Выберите тип добавляемого исключения: из правила, по которому была сгенерирована выбранная атака, или из всех правил для атак.
5. Нажмите кнопку **Добавить параметр** и в раскрывшемся меню выберите параметр атаки для создания исключения.

Появятся значения выбранного параметра, которые есть в карточке атаки. Если PT NAD обнаружит в новой сессии эти значения, то не будет регистрировать срабатывание правила.

6. Нажмите кнопку **Добавить**.

Исключение из правила добавлено.

Вы можете изменить или удалить добавленное исключение в карточке правила, открыв ее по кнопке **Перейти к правилу**, или в справочнике исключений для атак на странице **Справочники**.

20.4.3.2. Добавление исключения из правила в карточке правила

Вы можете добавить исключение из правила в карточке этого правила. Такой способ добавления пригодится, например, если вы знакомы с форматом написания исходного текста правил и можете, ознакомившись с принципами работы правила, внести нужные вам исключения.

- Чтобы добавить исключение из правила в карточке правила:

1. В главном меню выберите → **Правила для атак**.
2. В столбце **Название** по ссылке с названием правила откройте карточку правила, исключение из которого вам нужно добавить.
3. Нажмите кнопку **Добавить**.

   Откроется окно **Добавление записи**.
4. Как минимум в одном из полей введите параметры сессии, по которым PT NAD должен игнорировать выбранное правило.

   Примечание. В любом из этих полей можно указать несколько значений (с запятой в качестве разделителя). В полях **IP-адрес отправителя** и **IP-адрес получателя** допускается вводить IPv4- и IPv6-адреса, диапазоны IP-адресов (например, `198.51.100.0-198.51.100.34`), а также адреса подсетей в формате CIDR (например, `203.0.113.0/24`).
5. Нажмите кнопку **Добавить**.

Исключение из правила добавлено.

Вы можете изменить или удалить исключение в карточке правила или в справочнике исключений для атак на странице **Справочники**.

20.4.3.3. Добавление исключения из правила в карточке сессии

Вы можете добавить исключение из правила в карточке сессии с атакой, которая была обнаружена с помощью этого правила. Просмотрев информацию о сессии и отметив связанную с ней атаку как ложную, вы можете в той же карточке исключить последующую генерацию аналогичных атак.

> **Примечание.** Не все атаки обнаруживаются при помощи правил для атак. Атаки могут выявляться также в ходе детектирования опасных и потенциально опасных активностей. В таких случаях (если атака не связана с флудом, сканированиями и ICMP-туннелями) нельзя добавлять исключения из правил для атак. Вместо этого вы можете добавлять исключения из правил для активностей (см. раздел 20.4.4). Для добавления исключения могут понадобиться адрес узла и идентификатор типа активности. Адрес можно найти в блоке **Отправитель** или **Получатель**, а идентификатор указан в скобках во всплывающем окне по кнопке рядом с пунктом **Добавить исключение** контекстного меню атаки. В этом же окне есть ссылка на таблицу исключений из правил для активностей, в которой можно добавить исключение (см. раздел 20.4.4.2).

► Чтобы добавить исключение из правила в карточке сессии:

1. В главном меню выберите **Сессии**.
2. Откройте карточку сессии, нажав в строке этой сессии.
3. В блоке **Атаки** справа от записи об атаке нажмите и в раскрывшемся меню выберите пункт **Добавить исключение**.

   Откроется окно для добавления исключения. Если вы или другой пользователь PT NAD ранее создавали исключения, связанные с выбранной атакой, информация о них будет приведена в блоке **Действующие исключения**.
4. Выберите тип добавляемого исключения: из правила, по которому была сгенерирована выбранная атака, или из всех правил для атак.
5. Нажмите кнопку **Добавить параметр** и в раскрывшемся меню выберите параметр атаки для создания исключения.

   Появятся значения выбранного параметра, которые есть в карточке атаки. Если PT NAD обнаружит в новой сессии эти значения, то не будет регистрировать срабатывание правила.
6. Нажмите кнопку **Добавить**.

Исключение из правила добавлено.

Вы можете изменить или удалить исключение в карточке правила, выбрав пункт меню **Перейти к правилу** в блоке с информацией об атаке, или в справочнике исключений для атак на странице **Справочники**.

20.4.3.4. Добавление исключения из правила в таблице всех исключений

Вы можете добавить исключение из правила на странице со списком всех исключений. Такой способ может пригодиться, например, для IP-адресов, ранее добавленных в исключения из других правил.

- Чтобы добавить исключение из правила в таблице всех исключений:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

     Откроется страница **Справочники**.

  2. В панели слева выберите справочник **Исключения для атак**.

     Отобразится список исключений для атак.

  3. Нажмите .

     Откроется окно **Добавление записи**.

  4. Если вам нужно добавить исключение из конкретного правила, введите его идентификатор в поле **SID**.

     Если поле не заполнено, PT NAD применит исключение ко всем правилам для атак.

  5. Как минимум в одном из остальных полей (см. раздел 20.4.1) введите параметры сессии, по которым PT NAD должен игнорировать правило с указанным идентификатором.

     Примечание. В любом из этих полей можно указать несколько значений (с запятой в качестве разделителя). В полях **IP-адрес отправителя** и **IP-адрес получателя** допускается вводить IPv4- и IPv6-адреса, диапазоны IP-адресов (например, `198.51.100.0-198.51.100.34`), а также адреса подсетей в формате CIDR (например, `203.0.113.0/24`).

  6. Нажмите кнопку **Добавить**.

  Исключение из правила добавлено.

Вы можете изменить или удалить исключение в выбранном справочнике или в карточке правила.

20.4.4. Добавление исключения из правила для активности

Для более эффективного выявления опасных и потенциально опасных активностей вы можете указать, в каких случаях то или иное правило для активности не должно срабатывать в PT NAD. Например, чтобы не тратить время на обнаружение ложных срабатываний правила, вы можете добавить IP-адреса доверенных узлов в список исключений из этого правила.

Вы можете добавить исключение из правила для активности:

— в ленте активностей;

— списке всех исключений для активностей.

В этом разделе

Добавление исключений из правил для активностей в ленте активностей (см. раздел 20.4.4.1)

Добавление исключения из правила для активности в таблице всех исключений (см. раздел 20.4.4.2)

20.4.4.1. Добавление исключений из правил для активностей в ленте активностей

Вы можете сделать так, чтобы PT NAD не генерировал активности, схожие с теми, которые вы посчитали ложными или неинтересными. Например, просмотрев в ленте активностей информацию об активности на доверенном узле и отметив ее как ложную, вы можете заодно исключить генерацию активностей с тем же IP-адресом узла.

> **Примечание.** Вы можете добавлять исключения только из тех правил для активностей, у которых есть параметры, по которым можно настраивать исключения.

► Чтобы добавить исключение из правил для активностей в ленте активностей:

1. В главном меню выберите **Лента активностей**.
2. В блоке активности нажмите ⋮ и в раскрывшемся меню выберите пункт **Добавить исключение**.

   Откроется окно для добавления исключения. Если вы или другой пользователь PT NAD ранее создавали исключения, связанные с выбранной активностью, информация о них будет приведена в блоке **Действующие исключения**.

   Примечание. Вы также можете открыть это окно по кнопке **Добавить исключение** в карточке активности (см. раздел 14.2).
3. Выберите тип добавляемого исключения: из правила, по которому была сгенерирована выбранная активность, или из всех правил для активностей.
4. Нажмите кнопку **Добавить параметр** и в раскрывшемся меню выберите название параметра активности для создания исключения.

   Появятся значения выбранного параметра, которые есть в карточке активности. Если PT NAD обнаружит в новой сессии эти значения, то не будет регистрировать срабатывание правила.
5. Если исключение не должно действовать по каким-то из показанных значений, снимите флажки напротив них.

6. Если исключение должно также действовать по значениям других параметров активности, аналогичным способом добавьте эти параметры по кнопке **Добавить параметр**.
7. Нажмите кнопку **Добавить**.

   Исключение будет добавлено в справочник для активностей на странице **Справочники**.
8. Нажмите кнопку **Закрыть**.

20.4.4.2. Добавление исключения из правила для активности в таблице всех исключений

Вы можете добавить исключение из правила на странице со списком всех исключений. Такой способ может пригодиться, например, при внесении IP-адресов, ранее исключенных из других правил.

► Чтобы добавить исключение из правила для активности в таблице всех исключений:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

   Откроется страница **Справочники**.
2. В панели слева выберите справочник **Исключения для активностей**.

   Отобразится список исключений из правил для активностей.
3. Нажмите .

   Откроется окно **Добавление записи**.
4. Если вам нужно добавить исключение из конкретного правила, введите его идентификатор (см. раздел 20.3.1) в поле **Правило для активности**.

   Если поле не заполнено, PT NAD применит исключение ко всем правилам для активностей.
5. Как минимум в одном из остальных полей (см. раздел 20.4.2) введите параметры сессии, по которым PT NAD должен игнорировать правило с указанным идентификатором.

   Примечание. В каждом из этих полей можно указать только одно значение. В полях **IP-адрес отправителя** и **IP-адрес получателя** допускается вводить только IP-адреса (например, 203.0.113.0).
6. Нажмите кнопку **Добавить**.

Исключение из правила добавлено.

20.4.5. Изменение исключения из правила в справочнике

- Чтобы изменить исключение из правила в справочнике:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

     Откроется страница **Справочники**.
  2. В панели слева выберите справочник, в котором находится исключение.

     Отобразится список исключений, добавленных в выбранный справочник.
  3. В столбце **Изменено** в строке с нужным исключением нажмите .

     Откроется окно **Изменение записи**.
  4. Внесите изменения и нажмите кнопку **Сохранить**.

  Исключение из правила изменено.

20.4.6. Удаление исключений из правил в справочнике

Вы можете удалять исключения, которые были добавлены по ошибке или стали неактуальными.

- Чтобы удалить исключения из правил в справочнике:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

     Откроется страница **Справочники**.
  2. В панели слева выберите справочник, в котором находятся ненужные исключения.

     Отобразится список исключений, добавленных в выбранный справочник.
  3. Выберите исключения, которые нужно удалить.
  4. В панели инструментов нажмите и подтвердите удаление.

  Исключения из правил удалены.

20.4.7. Экспорт справочника

Вы можете экспортировать справочник с исключениями из правил.

- Чтобы экспортировать справочник:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

     Откроется страница **Справочники**.
  2. В панели слева выберите нужный справочник.

Отобразится список исключений, добавленных в выбранный справочник.

3. В панели инструментов нажмите  .

   Файл справочника будет сохранен на вашем компьютере.

Теперь вы можете импортировать полученный файл (см. раздел 20.4.8) в другой экземпляр PT NAD.

20.4.8. Импорт записей в справочник

Вы можете импортировать записи в справочник исключений. Это может понадобиться, например, если вам нужно загрузить список исключений, экспортированный (см. раздел 20.4.7) из другого экземпляра PT NAD или составленный в сторонней программе.

Импортируемый файл должен быть в формате CSV с запятой в качестве разделителя между элементами содержимого файла.

Первой должна идти строка с перечислением идентификаторов столбцов соответствующей таблицы исключений (в любом порядке):

- `rule_id` — правило для активности;
- `alert_sid` — правило для атаки;
- `src_id` — узел отправителя;
- `src_ip` — IP-адрес отправителя;
- `src_dns` — домен отправителя;
- `src_group` — группа отправителя;
- `dst_id` — узел получателя;
- `dst_ip` — IP-адрес получателя;
- `dst_dns` — домен получателя;
- `dst_group` — группа получателя;
- `login` — логин (только для правил для активностей);
- `pk` — идентификатор добавляемой записи (при импорте значение всегда отсутствует).

В каждой последующей строке с исключением должны перечисляться его параметры. Значения параметров соответствуют значениям столбцов в таблице с исключениями из правил для атак (см. раздел 20.4.1) или с исключениями из правил для активностей (см. раздел 20.4.2), порядок параметров — согласно первой строке с идентификаторами.

Пример содержимого CSV-файла с двумя записями исключений из правил для активностей:

```
rule_id,src_id,src_ip,src_dns,src_group,dst_id,dst_ip,dst_dns,dst_group,login,pk
,,203.0.113.1,,,,203.0.113.2,,,,
,,192.0.223.1,,,,192.0.249.2,,,,
```

► Чтобы импортировать записи в справочник:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Справочники**.

   Откроется страница **Справочники**.

2. В панели слева выберите нужный справочник.

   Отобразится список исключений, добавленных в выбранный справочник.

3. В панели инструментов нажмите .

   Откроется окно **Импорт записей из CSV-файла**.

4. Перетащите файл в окно или добавьте его по ссылке **выберите**.

5. Нажмите кнопку **Импортировать**.

Записи импортированы в справочник.

20.5. Управление репутационными списками

В PT NAD для анализа трафика используются репутационные списки, основанные на индикаторах компрометации. Репутационные списки указывают на потенциально опасные или заведомо безопасные узлы, файлы и ссылки.

Вы можете создавать репутационные списки самостоятельно или использовать репутационные списки Positive Technologies.

PT NAD получает обновления репутационных списков Positive Technologies автоматически:

— из базы знаний экспертного центра Positive Technologies;

— с помощью PT Cybsi Provider (если интеграция с этим компонентом MaxPatrol 10 была настроена администратором PT NAD).

Вы не можете изменять или удалять репутационные списки Positive Technologies, равно как просматривать их содержимое.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

Ретроспективный анализ сессий

Для обнаружения новейших угроз ИБ в информационной инфраструктуре организации PT NAD периодически анализирует ранее завершенные сессии в потоковом хранилище с использованием новых и измененных репутационных списков. Такой анализ называется ретроспективным.

По умолчанию ретроспективный анализ запускается ежечасно. Период запуска может быть изменен администратором PT NAD.

Вы также можете настроить уведомления (см. раздел 14.14) об обновлении репутации сессий по результатам ретроспективного анализа.

В этом разделе

20.5.1. Просмотр репутационных списков

- Чтобы просмотреть перечень репутационных списков,

  в главном меню выберите → **Репутационные списки**.

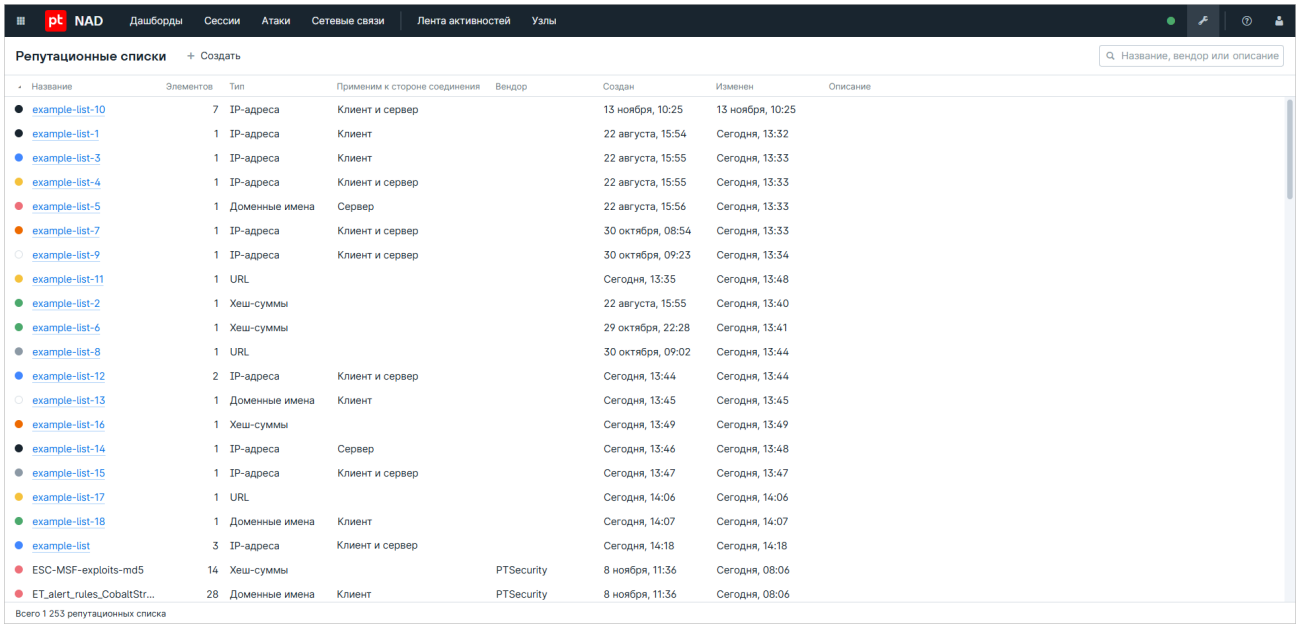


Рисунок 83. Просмотр репутационных списков

Для каждого репутационного списка указаны следующие данные:

- **Цвет** — цвет маркера, который на страницах **Сессии** и **Атаки** указывает на связь сессий и атак с репутационным списком.
- **Название** — название репутационного списка. У пользовательских репутационных списков название является ссылкой, по нажатию на которую можно перейти к карточке репутационного списка.
- **Элементов** — количество элементов в репутационном списке.
- **Тип** — тип элементов репутационного списка.

— **Применим к стороне соединения** — сторона соединения (клиент, сервер или клиент и сервер), к которой применяется репутационный список. Значение можно задать только для репутационных списков IP-адресов и доменных имен.

— **Вендор** — поставщик репутационного списка. У пользовательских репутационных списков значение отсутствует.

— **Создан** — дата создания репутационного списка.

— **Изменен** — дата последнего изменения репутационного списка.

— **Описание** — текстовое описание пользовательского репутационного списка. Вы можете добавить и изменить описание по ссылке, которая появляется при наведении курсора на строку репутационного списка в этом столбце.

Вы можете найти репутационный список по его названию, вендору или описанию, используя поле поиска.

20.5.2. Просмотр элементов репутационного списка

Если репутационный список был создан вами или другим пользователем PT NAD, вы можете просмотреть элементы этого списка в его карточке. Вы не можете просматривать элементы репутационных списков Positive Technologies.

► Чтобы просмотреть элементы репутационного списка:

1. В главном меню выберите → **Репутационные списки**.
2. По ссылке в столбце **Название** откройте карточку репутационного списка.

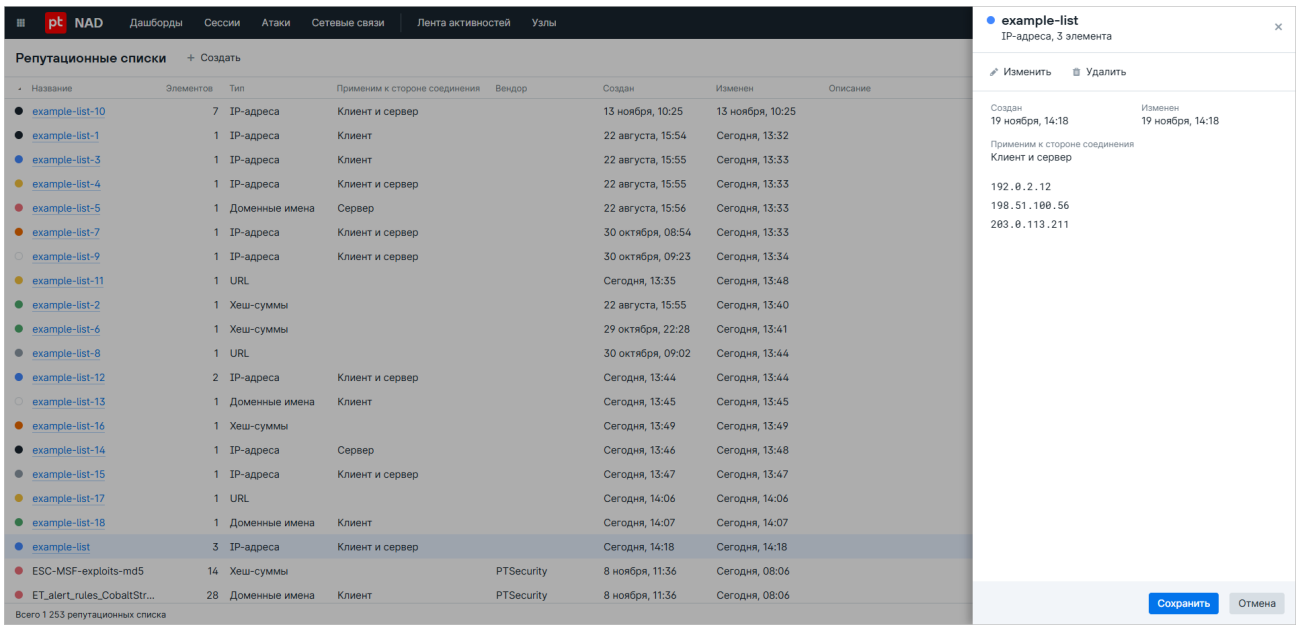


Рисунок 84. Просмотр карточки репутационного списка

Вы можете удалить выбранный репутационный список или внести в него изменения. Действия доступны только для тех репутационных списков, которые были созданы пользователями через веб-интерфейс или сторонними приложениями через API без указания параметра `external_key`.

20.5.3. Создание репутационного списка

Вы можете создавать репутационные списки:

- IP-адресов;
- доменных имен;
- URL;
- хеш-сумм файлов, вычисленных по алгоритму MD5.

► Чтобы создать репутационный список:

1. В главном меню выберите → **Репутационные списки**.
2. Нажмите **Создать**.
3. Выберите тип элементов списка.
4. Выберите цвет маркера, который на страницах **Сессии** и **Атаки** будет указывать на связь сессий и атак с репутационным списком.
5. Если вы создаете репутационный список IP-адресов или доменных имен, то выберите сторону соединения, к которой должен применяться список.
6. Введите уникальное название репутационного списка.

   Примечание. Название должно состоять из латинских букв, цифр, знаков подчеркивания и дефисов. Максимальная длина — 30 символов.
7. Введите элементы списка соответствующего типа.
8. Нажмите **Создать**.

   Если ошибок нет, список будет сохранен. В противном случае PT NAD выделит ошибочные элементы красным цветом. Вы можете удалить их по ссылке **Удалить элементы с ошибками** и повторить попытку сохранения.

20.6. Составление списка исключений из DGA-доменов

Вы можете составить список доверенных доменных имен, которые не нужно проверять на использование DGA (см. раздел 2.3). Доменные имена более низкого уровня будут также исключены из проверки. Например, имя nsdfggp.com в списке означает, что имена support.nsdfggp.com и privacy.nsdfggp.com также не будут проверяться.

Примечание. Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

- Чтобы составить список исключений из DGA-доменов:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **DGA-домены**.

   Откроется страница **DGA-домены**.

2. В поле **Доверенные домены** введите список доменных имен, которые должны быть исключены из проверки на использование DGA.

   Каждое доменное имя нужно вводить на новой строке.

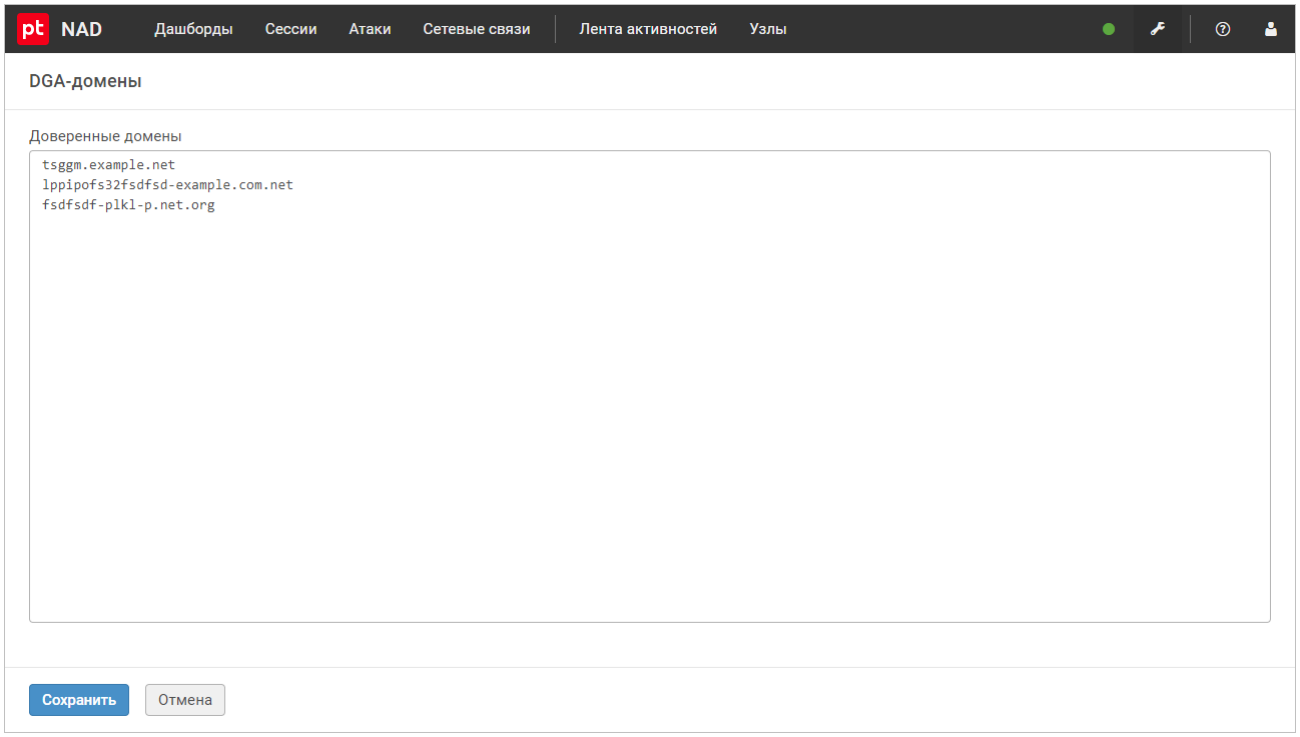


Рисунок 85. Составление списка исключений из DGA-доменов

3. Нажмите кнопку **Сохранить**.

Список исключений из DGA-доменов составлен.

20.7. Управление группами узлов и портов

PT NAD позволяет объединять узлы или порты в группы по какому-либо признаку. Группы используются:

— для настройки правил для обнаружения атак (см. раздел 20.2) и для обнаружения активностей (см. раздел 20.3);

— настройки других групп;

— сбора информации об узлах, участвующих в сессиях (см. раздел 15);

— фильтрации сессий (см. раздел 9.6).

Группы могут быть трех типов:

— **Системные группы.** Предусмотрены в продукте по умолчанию.

— **Пользовательские группы.** Создаются пользователями.

— **Группы правил.** Создаются автоматически, когда правила загружаются в продукт.

Информация о группах узлов и группах портов отображается в рабочей области страницы **Правила для атак и группы**, доступной из меню администрирования (кнопка в главном меню).

Информация о группах узлов и о группах портов находится на разных вкладках. Для обеих вкладок действует общий поиск. Вы можете искать группы по названиям, узлам, портам и комментариям, используя поле поиска. Кроме того, вы можете выполнить поиск только по группам с ошибками (см. раздел 20.7.2) или по группам с изменениями, нажав на ссылку слева от количества нужных групп.

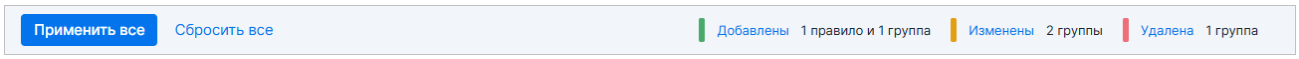


Рисунок 86. Фильтрация правил и групп с изменениями

Вы можете создавать пользовательские группы узлов и группы портов. Кроме того, вы можете изменять состав групп узлов и групп портов, а также удалять группы. При удалении группы PT NAD проверяет, используется ли она в правилах или других группах. До синхронизации вы можете восстановить помеченную к удалению группу узлов или портов.

Для удобства администрирования групп вы можете к каждой из них добавлять описания в столбце **Комментарий**.

Любые изменения групп узлов и групп портов вступают в силу только после синхронизации (см. раздел 20.7.2).

> **Примечание.** Если экземпляры PT NAD объединены в иерархию, то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли (см. раздел 2.4).

В этом разделе

20.7.1. Создание группы узлов или портов

- Чтобы создать пользовательскую группу узлов или группу портов:

  1. В главном меню выберите → **Правила для атак и группы**.
  2. Выберите вкладку **Группы узлов** или **Группы портов**.
  3. Нажмите **Создать**.
  4. Введите название группы и добавьте в нее элементы.

     Примечание. После создания группы вы не сможете изменить ее название.

     Название группы должно быть уникальным и состоять из латинских букв, цифр, знаков подчеркивания. Максимальная длина — 63 символа.

     Количество элементов группы не ограничено. При добавлении элементов в группу вы можете использовать спецсимволы, перечисленные в таблице ниже.

  Продукт начнет использовать созданную группу только после синхронизации (см. раздел 20.7.2).

Таблица 4. Спецсимволы для элементов группы

Спецсимвол	Назначение	Пример использования
`!`	Исключение элемента	`!80`
`,`	Разделение элементов	`192.0.2.3,192.0.2.6`
`[ ]`	Объединение элементов	`[21,25,110,80]`
`$<Название группы>`	Ссылка на другую группу элементов такого же типа (в группе узлов можно ссылаться только на группы узлов, в группе портов — на группы портов)	`$DNS_SERVERS`
`:`	Диапазон портов	`80:84`
`-`	Диапазон IP-адресов узлов	`192.0.2.3-192.0.2.11`
`/`	IP-адрес подсети узлов	`203.0.113.0/24`

20.7.2. Синхронизация групп узлов и портов

Изменения, внесенные в группы узлов и портов, не вступают в силу сразу. PT NAD запоминает их, и вы можете применить их все вместе или отклонить. Такое применение называется синхронизацией.

Все изменения отображаются под главным меню на странице **Правила для атак и группы**. Дата последней успешной синхронизации отображается в нижней части страницы.

Изменения в правилах для обнаружения атак и в группах узлов и портов синхронизируются одновременно. Во время синхронизации PT NAD проверяет корректность изменений. Если ошибок нет, все изменения в правилах для обнаружения атак и в группах узлов и портов вступают в силу. При наличии ошибок в строках правил и групп узлов и портов, в которых обнаружены ошибки, отображается значок ⚠. При наличии критически значимых ошибок синхронизация может быть выполнена только после их исправления.

- Чтобы применить все изменения, внесенные с момента последней синхронизации, нажмите **Применить все**.
- Чтобы отменить все изменения, внесенные с момента последней синхронизации, нажмите **Сбросить все**.

21. Настройка интерфейса и учетной записи пользователя

При работе с интерфейсом PT NAD каждый пользователь использует собственную учетную запись. Вы можете настроить свою учетную запись: сменить пароль, а также изменить личные данные и контакты. Настройка учетной записи осуществляется в личном кабинете. В личном кабинете вы можете также настроить интерфейс: сменить язык, часовой пояс и тему оформления. Эти параметры привязаны к вашей учетной записи.

Личный кабинет пользователя доступен в главном меню по кнопке .

В этом разделе

21.1. Изменение личных данных и контактов

Администратор создает учетные записи пользователей. Пользователь может добавлять, изменять и удалять свои личные данные и контакты в учетной записи в личном кабинете.

> **Примечание.** Если вход в PT NAD осуществляется с помощью PT MC, личные данные и контакты можно изменять только в PT MC. В таком случае в личном кабинете на вкладке **Личные данные** отображается информация из вашего профиля в PT MC.
>
> **Примечание.** Вы не можете изменить логин вашей учетной записи.

- Чтобы изменить личные данные и контакты:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Личные данные**.

     Откроется страница **Личные данные**.

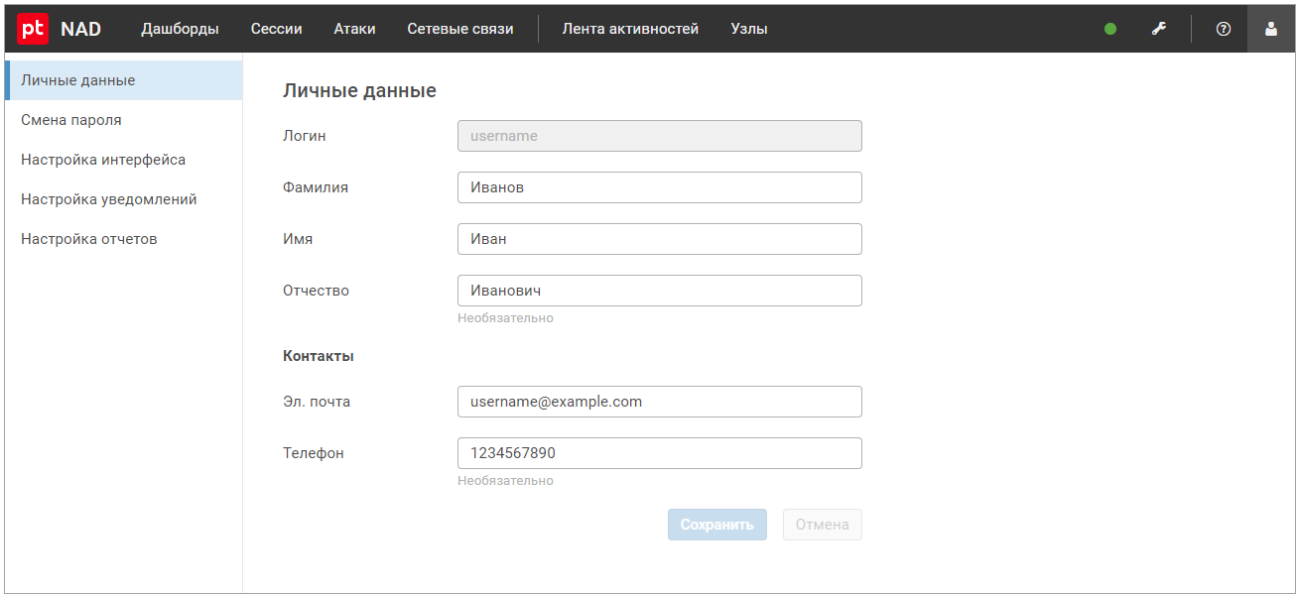


Рисунок 87. Изменение данных и контактов в учетной записи

2. Внесите изменения в поля **Фамилия**, **Имя**, **Отчество**, **Эл. почта**, **Телефон**.
3. Нажмите кнопку **Сохранить**.

Ваши личные данные и контакты изменены.

21.2. Смена пароля учетной записи

В целях безопасности вы можете сменить пароль вашей учетной записи.

Примечание. Если вход в PT NAD осуществляется с помощью PT MC, смена пароля производится тоже в PT MC. В таком случае в личном кабинете нет вкладки **Смена пароля**.

- Чтобы сменить пароль вашей учетной записи:

1. В главном меню выберите → **Смена пароля**.
2. Введите старый пароль.
3. Дважды введите новый пароль.
4. Нажмите кнопку **Сохранить**.

Пароль вашей учетной записи изменен.

21.3. Смена языка интерфейса

Интерфейс PT NAD доступен на русском и английском языках. По умолчанию язык интерфейса соответствует языку браузера, с помощью которого вы впервые вошли в продукт.

Примечание. Вместе с языком интерфейса также меняется язык ваших почтовых уведомлений, отчетов, справочного центра и скачиваемой документации.

- Чтобы сменить язык интерфейса:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. Выберите язык интерфейса.
  3. Нажмите кнопку **Сохранить**.

  Язык интерфейса изменен.

21.4. Смена темы оформления интерфейса

Интерфейс PT NAD доступен в двух темах: светлой и темной. По умолчанию выбрана тема, соответствующая оформлению интерфейса операционной системы.

- Чтобы сменить тему интерфейса:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. Выберите тему оформления интерфейса.
  3. Нажмите кнопку **Сохранить**.

  Тема интерфейса сменена.

21.5. Смена часового пояса

По умолчанию PT NAD отображает любое время в интерфейсе в часовом поясе компьютера, с которого вы впервые вошли в интерфейс. Выбранный часовой пояс также влияет на время в ваших почтовых уведомлениях и создаваемых вами отчетах.

- Чтобы сменить часовой пояс:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. В раскрывающемся списке **Часовой пояс** выберите новый часовой пояс.

     Вы можете найти нужный часовой пояс с помощью поля поиска.
  3. Нажмите кнопку **Сохранить**.

  Часовой пояс изменен.

21.6. Включение автоматического выхода из PT NAD по бездействию

Для защиты учетной записи от несанкционированного использования вы можете сделать так, чтобы ваша сессия в PT NAD автоматически завершалась по истечении определенного администратором времени бездействия.

Примечание. Для использования функция должна быть настроена администратором PT NAD.

- Чтобы включить автоматический выход из продукта по бездействию:

  1. В главном меню выберите → **Настройка интерфейса**.
  2. Установите флажок **Автоматически выходить из системы через <Количество минут, определенное администратором> минут бездействия**.
  3. Нажмите кнопку **Сохранить**.

  Автоматический выход из продукта по бездействию включен.

22. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на продукты Positive Technologies в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продуктов

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продуктов в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продуктов.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продуктов в рамках выпуска обновленных версий продукта

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 5. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

— предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);

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

— заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение A. Системные виджеты в PT NAD

В этом разделе описываются поставляемые с продуктом системные виджеты, с которыми вы можете работать (см. раздел 11).

Виджеты могут представлять собой столбчатые и круговые диаграммы, диаграммы с областями, гистограммы, карты, таблицы, сводки и тепловые карты.

Количество информации, показываемой на виджете, зависит от формы отображения данных:

— На горизонтальных столбчатых диаграммах, горизонтальных гистограммах и в таблицах по умолчанию отображается не более 50 записей — столбцов, линий и строк соответственно. Вы можете изменять максимальное количество записей (см. раздел 11.6) в этих виджетах.

— На вертикальных столбчатых диаграммах и вертикальных гистограммах отображается не более 20 столбцов и линий соответственно.

— На круговых диаграммах отображается не более 10 секторов.

Вы можете сортировать строки в таблицах по нажатию на заголовок столбца. PT NAD заново запросит из хранилища все данные, соответствующие характеру виджета, примененному фильтру и периоду, выбранному на диаграмме интенсивности трафика (см. раздел 6.3). Полученные данные будут отсортированы по выбранному вами значению и отображены в таблице.

В этом разделе

A.1. Категория виджетов Трафик

В категорию **Трафик** входят виджеты, которые показывают статистику захваченного PT NAD трафика по его атрибутам (IP-адресам, портам, доменам, количеству сессий, времени, странам, протоколам, объему переданных данных).

Доменные имена по числу сессий

Виджет **Доменные имена по числу сессий** отображает список доменных имен серверов с указанием количества сессий.

При наведении курсора на линию отображаются имя сервера и количество запросов. По нажатию на имя сервера или соответствующую ему линию в строку фильтрации добавляется параметр с этим именем (например, `dst.dns == "server.example.org"`).

Интенсивность трафика

Виджет **Интенсивность трафика** показывает количество сессий за выбранную единицу времени.

При наведении курсора на столбец отображаются время и количество сессий, зарегистрированных в это время. Когда вы выделяете период на виджете, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

Клиенты по сессиям и трафику

Виджет **Клиенты по сессиям и трафику** представляет собой таблицу. Таблица содержит список клиентов с указанием числа сессий и объема переданного и полученного трафика. На дашборде **Трафик** виджет отображается по умолчанию.

По нажатию на IP-адрес в строку фильтрации добавляется параметр с IP-адресом источника взаимодействия (например, `src.ip == 198.51.100.0`), а по нажатию на доменное имя — параметр с доменом источника взаимодействия (например, `src.dns == "client.example.org"`).

Клиенты по странам

Виджет **Клиенты по странам** представляет собой карту мира. На карте показаны те страны, в которых расположены источники сетевых запросов. На дашборде **Трафик** виджет отображается по умолчанию.

Чем насыщеннее оттенок цветовой индикации страны, тем больше взаимодействий с узлами из этой страны было зарегистрировано. При наведении курсора на страну отображаются ее название и двухбуквенный код, количество сессий, объем отправленных и полученных данных. По нажатию на страну в строку фильтрации добавляется параметр с кодом страны источника взаимодействия (например, `src.geo.country == "PL"`).

Примечание. Код страны определяется ISO 3166-1.

Объем трафика

Виджет **Объем трафика** представляет собой диаграмму с областями. Диаграмма показывает изменение объемов отправленного и полученного трафика с течением времени. На дашборде **Трафик** виджет отображается по умолчанию.

Примечание. На странице **Сессии** аналогичную функцию выполняет диаграмма объемов отправленного и полученного трафика (см. раздел 9.4).

При наведении курсора на диаграмму отображаются дата, время, скорость отправки и получения трафика. Вы можете скрыть информацию об отправленном или полученном трафике, выбрав внизу виджета **Отправлено** или **Получено** соответственно. Когда вы выделяете период на виджете, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

Пары «клиент — сервер» по сессиям и трафику

Виджет **Пары «клиент — сервер» по сессиям и трафику** представляет собой таблицу. Таблица содержит список пар «клиент — сервер» с указанием числа сессий и объема отправленного и полученного трафика. На дашборде **Трафик** виджет отображается по умолчанию.

В таблице отображаются IP-адреса или доменные имена клиента и сервера. По нажатию на IP-адрес в строку фильтрации добавляется параметр с этим IP-адресом (например, `src.ip == 198.51.100.0`), а по нажатию на доменное имя — параметр с этим именем (например, `dst.dns == "server.example.org"`).

Прикладные протоколы

Виджет **Прикладные протоколы** представляет собой круговую диаграмму. Диаграмма показывает долю каждого из прикладных протоколов (см. приложение В) в общем объеме трафика. На дашборде **Трафик** виджет отображается по умолчанию.

При наведении курсора на сектор круга отображаются имя протокола и объем переданного и полученного трафика. По нажатию на сектор круга в строку фильтрации добавляется параметр с названием протокола (например, `app_proto == "tls"`). Вы можете убрать протокол с диаграммы, выбрав его в списке под диаграммой.

Приложения по числу сессий

Виджет **Приложения по числу сессий** отображает список приложений (см. приложение Д) с указанием количества сессий, в которых эти приложения были задействованы.

При наведении курсора на линию отображаются название приложения и количество сессий, в которых был зафиксирован трафик этого приложения. По нажатию на название или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `app_service == "YouTube"`).

Порты серверов

Виджет **Порты серверов** отображает список портов серверов с указанием количества сессий.

При наведении курсора на линию отображаются номер сетевого порта и количество сессий, установленных с использованием этого порта. По нажатию на номер порта или соответствующую ему линию в строку фильтрации добавляется параметр с этим портом (например, `dst.port == 10050`).

Серверы и клиенты по времени

Виджет **Серверы и клиенты по времени** показывает, сколько серверов и клиентов было обнаружено за выбранную единицу времени.

При наведении курсора на столбец отображаются тип узлов (клиенты или серверы), их количество и время. Вы можете скрыть информацию о клиентах или серверах, выбрав внизу виджета **Клиенты** или **Серверы** соответственно. Когда вы выделяете период на виджете, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

Серверы по сессиям и трафику

Виджет **Серверы по сессиям и трафику** представляет собой таблицу. Таблица показывает список серверов с указанием числа сессий и объема отправленного и полученного трафика. На дашборде **Трафик** виджет отображается по умолчанию.

По нажатию на IP-адрес в строку фильтрации добавляется параметр с IP-адресом получателя взаимодействия (например, `dst.ip == 198.51.100.11`), а по нажатию на доменное имя — параметр с доменом получателя взаимодействия (например, `dst.dns == "server.example.org"`).

Серверы по странам

Виджет **Серверы по странам** представляет собой карту мира. На карте показаны те страны, в которых расположены получатели сетевых запросов. На дашборде **Трафик** виджет отображается по умолчанию.

Чем насыщеннее оттенок цветовой индикации страны, тем больше взаимодействий с серверами из этой страны было зарегистрировано. При наведении курсора на страну отображаются ее название и двухбуквенный код, количество сессий, объем отправленных и полученных данных. По нажатию на страну в строку фильтрации добавляется параметр с кодом страны получателя взаимодействия (например, `dst.geo.country == "DE"`).

Примечание. Код страны определяется ISO 3166-1.

Транспортные протоколы

Виджет **Транспортные протоколы** представляет собой круговую диаграмму. Диаграмма показывает долю каждого из транспортных протоколов в общем объеме трафика. На дашборде **Трафик** виджет отображается по умолчанию.

При наведении курсора на сектор круга отображаются название транспортного протокола и объем трафика, переданного и полученного с использованием этого протокола. По нажатию на сектор круга в строку фильтрации добавляется параметр с названием транспортного протокола (например, `proto == "TCP"`). Вы можете убрать протокол с диаграммы, выбрав его в списке под диаграммой.

A.2. Категория виджетов Атаки

В категорию **Атаки** входят виджеты со статистикой атак, зарегистрированных PT NAD.

Атаки по времени

Виджет **Атаки по времени** показывает, сколько атак было обнаружено за выбранную единицу времени.

При наведении курсора на цветной отрезок столбца отображаются время и количество зарегистрированных в это время атак с соответствующим этому цвету уровнем опасности. По нажатию на отрезок столбца одного цвета в строку фильтрации добавляется параметр с соответствующим этому цвету уровнем опасности атак (например, `alert.pr == 1`). Вы можете скрыть информацию об атаках определенного уровня опасности, выбрав его в списке внизу виджета. Когда вы выделяете период на виджете, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

Атакующие узлы

Виджет **Атакующие узлы** отображает список атакующих узлов с указанием количества атак, зарегистрированных PT NAD.

При наведении курсора на цветной отрезок линии отображаются IP-адрес атакующего узла, уровень опасности атаки и количество атак с этим уровнем. По нажатию на IP-адрес атакующего узла в строку фильтрации добавляется параметр с этим IP-адресом (например, `alert.attacker.ip == 198.51.100.11`), по нажатию на доменное имя — параметр с этим именем (например, `alert.attacker.dns == "example.org"`), по нажатию на отрезок линии — параметр с уровнем опасности атаки (например, `alert.pr == 1`).

Атаки по классам

Виджет **Атаки по классам** отображает список классов атак с указанием количества обнаружений PT NAD.

При наведении курсора на цветной отрезок линии отображаются название класса атаки, количество атак и уровень опасности атаки с этим классом. По нажатию на класс атаки в строку фильтрации добавляется параметр с названием этого класса (например, `alert.cls == "A System Call was Detected"`), по нажатию на отрезок линии — параметр с уровнем опасности атаки (например, `alert.pr == 1`).

Атаки по количеству

Виджет **Атаки по количеству** отображает список атак с указанием количества обнаружений продуктом. На дашборде **Атаки** виджет отображается по умолчанию.

При наведении курсора на цветной отрезок линии отображаются название атаки, количество атак с этим названием и уровень опасности атаки. По нажатию на название атаки в строку фильтрации добавляется параметр с этим именем (например, `alert.msg == "PROTOCOL-ICMP Echo Reply"`), по нажатию на отрезок линии — параметр с уровнем опасности атаки (например, `alert.pr == 1`).

Атаки по странам источников

Виджет **Атаки по странам источников** представляет собой карту мира. На карте мира показаны те страны, в которых расположены атакующие узлы. На дашборде **Атаки** виджет отображается по умолчанию.

Чем насыщеннее оттенок цветовой индикации страны, тем больше атак с узлов этой страны было зарегистрировано. При наведении курсора на страну отображаются ее название и двухбуквенный код, а также количество атак. По нажатию на страну в строку фильтрации добавляется параметр с кодом страны — источника атаки (например, `alert.attacker.geo.country == "FR"`).

Примечание. Код страны определяется ISO 3166-1.

Атаки по странам целей

Виджет **Атаки по странам целей** представляет собой карту мира. На карте показаны те страны, в которых расположены атакуемые узлы.

Чем насыщеннее оттенок цветовой индикации страны, тем больше атак на узлы из этой страны было зарегистрировано. При наведении курсора на страну отображаются ее название и двухбуквенный код, а также количество атак. По нажатию на страну в строку фильтрации добавляется параметр с кодом страны — цели атаки (например, `alert.victim.geo.country == "FR"`).

Примечание. Код страны определяется ISO 3166-1.

Атаки по уровням опасности

Виджет **Атаки по уровням опасности** представляет собой круговую диаграмму. Диаграмма показывает доли атак различных уровней опасности.

При наведении курсора на сектор круга отображаются уровень опасности атак и количество атак этого уровня. По нажатию на сектор круга в строку фильтрации добавляется параметр с уровнем опасности (например, `alert.pr == 1`). Вы можете убрать уровень опасности с диаграммы, выбрав его в списке под диаграммой.

Атакуемые узлы

Виджет **Атакуемые узлы** показывает список атакуемых узлов с указанием количества атак, зарегистрированных PT NAD. На дашборде **Атаки** виджет отображается по умолчанию.

При наведении курсора на цветной отрезок линии отображаются IP-адрес атакуемого узла, уровень опасности атаки и количество атак с этим уровнем. По нажатию на IP-адрес атакуемого узла в строку фильтрации добавляется параметр с этим IP-адресом (например, `alert.victim.ip == 203.0.113.1`), по нажатию на доменное имя — параметр с этим именем (например, `alert.victim.dns == "example.org"`), по нажатию на отрезок линии — параметр с уровнем опасности атаки (например, `alert.pr == 1`).

Сводка по атакам

Виджет **Сводка по атакам** показывает основные данные об атаках в цифрах. На дашборде **Атаки** виджет отображается по умолчанию.

По нажатию на название уровня опасности атак в строку фильтрации добавляется соответствующий параметр (например, `alert.pr == 1`). По нажатию на число всех атак или на число уникальных атак в строку фильтрации добавляется параметр `alert` для отображения сессий с атаками.

События

Виджет **События** показывает список событий ИБ с указанием количества обнаружений продуктом. Событиями ИБ считаются срабатывания правил, которые не указывают на атаки.

При наведении курсора на линию отображаются название события и количество обнаружений этого события. По нажатию на название события в строку фильтрации добавляется параметр с этим названием (например, `alert.msg == "INFO [PTsecurity] LDAP enumeration by OS"`), по нажатию на линию — условие `alert.pr == 4` для поиска событий.

Тактики ATT&CK

Виджет **Тактики ATT&CK** представляет собой тепловую карту. Карта показывает тактики MITRE ATT&CK: чем больше атак, выполненных при помощи отдельной тактики, тем ярче цвет, которым она показана.

При наведении курсора на прямоугольник с названием тактики во всплывающем окне отображаются ссылка и количество зарегистрированных продуктом атак, в ходе которых была использована эта тактика. Если нажать на эту ссылку, в строку фильтрации добавится параметр с идентификатором тактики в базе знаний MITRE ATT&CK (например, `alert.att_ck='TA0006'`). Если нажать на прямоугольник с названием тактики, на виджете отобразится список техник, связанных с этой тактикой.

При наведении курсора на цветной отрезок линии отображаются название техники, уровень опасности и количество атак с этим уровнем, в ходе которых была использована техника. По нажатию на название техники в строку фильтрации добавляется параметр с

идентификаторами тактики и техники в базе знаний MITRE ATT&CK (например, `alert.att_ck='TA0006-T1187'`), по нажатию на отрезок линии — параметр с уровнем опасности атаки (например, `alert.pr == 1`).

См. также

Работа с атаками (см. раздел 10)

A.3. Категория виджетов ПО

В категорию **ПО** входят виджеты со статистикой программного обеспечения отправителей и получателей сетевых запросов.

Баннеры клиентов по числу сессий

Виджет **Баннеры клиентов по числу сессий** отображает список баннеров клиентов с указанием количества сессий. На дашборде **Обнаруженное ПО** виджет отображается по умолчанию.

При наведении курсора на линию отображаются название баннера и количество сессий. По нажатию на название баннера или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `banner.client == "Java/1.8.0_111"`).

Баннеры серверов по числу сессий

Виджет **Баннеры серверов по числу сессий** отображает список баннеров серверов с указанием количества сессий. На дашборде **Обнаруженное ПО** виджет отображается по умолчанию.

При наведении курсора на линию гистограммы отображаются название баннера и количество сессий. По нажатию на название баннера или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `banner.server == "nginx"`).

Баннеры клиентов по числу узлов

Виджет **Баннеры клиентов по числу узлов** отображает список баннеров клиентов с указанием количества узлов.

При наведении курсора на линию отображаются название баннера и количество узлов. По нажатию на название баннера или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `banner.client == "Java/1.8.0_111"`).

Баннеры серверов по числу узлов

Виджет **Баннеры серверов по числу узлов** отображает список баннеров серверов с указанием количества узлов.

При наведении курсора на линию отображаются название баннера и количество узлов. По нажатию на название баннера или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `banner.server == "nginx"`).

Операционные системы клиентов

Виджет **Операционные системы клиентов** отображает список операционных систем клиентов с указанием количества сессий. На дашборде **Обнаруженное ПО** виджет отображается по умолчанию.

При наведении курсора на линию отображаются название операционной системы и количество сессий. По нажатию на название ОС или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `os.client == "Windows: XP"`).

Операционные системы серверов

Виджет **Операционные системы серверов** отображает список операционных систем серверов с указанием количества сессий. На дашборде **Обнаруженное ПО** виджет отображается по умолчанию.

При наведении курсора на линию отображаются название операционной системы и количество сессий. По нажатию на название ОС или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `os.server == "Linux: 3.x"`).

A.4. Категория виджетов HTTP

В категорию **HTTP** входят виджеты со статистикой захваченного PT NAD трафика, относящейся к HTTP.

HTTP-клиенты по числу запросов

Виджет **HTTP-клиенты по числу запросов** отображает список HTTP-клиентов с указанием количества запросов.

При наведении курсора на линию отображаются название HTTP-клиента и количество запросов. По нажатию на название HTTP-клиента или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `http.rqs.User-Agent == "Mozilla/5.0"`).

HTTP-серверы по числу запросов

Виджет **HTTP-серверы по числу запросов** отображает список HTTP-серверов с указанием количества запросов.

При наведении курсора на линию отображаются название HTTP-сервера и количество запросов. По нажатию на название HTTP-сервера или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `http.rsp.Server == "nginx"`).

Сводка по HTTP

Виджет **Сводка по HTTP** отражает основные показатели HTTP-трафика в цифрах: количество HTTP-запросов, HTTP-серверов, HTTP-клиентов и HTTP-узлов.

HTTP-методы

Виджет **HTTP-методы** представляет собой круговую диаграмму. Диаграмма показывает долю каждого из HTTP-методов в общем количестве запросов.

При наведении курсора на сектор круга отображаются название HTTP-метода и количество запросов, выполненных с использованием этого метода. По нажатию на сектор круга в строку фильтрации добавляется параметр с названием HTTP-метода (например, `http.rqs.method == "GET"`). Вы можете убрать HTTP-метод с диаграммы, выбрав его в списке под диаграммой.

Узлы по числу запросов

Виджет **Узлы по числу запросов** отображает список узлов с указанием количества HTTP-запросов на подключение к этим узлам.

При наведении курсора на линию отображаются название узла и количество запросов. По нажатию на название узла или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `http.rqs.Host == "example.org"`).

URL по числу запросов

Виджет **URL по числу запросов** представляет собой таблицу. Таблица содержит список URL с указанием количества HTTP-запросов.

По нажатию на URL в строку фильтрации добавляется параметр с этим URL (например, `http.rqs.url == "/dists/updates/Release"`).

A.5. Категория виджетов DNS

В категорию **DNS** входят виджеты со статистикой запросов к DNS-серверам.

DNS-записи по числу запросов

Виджет **DNS-записи по числу запросов** отображает список DNS-записей с указанием количества запросов к DNS-серверу.

При наведении курсора на линию отображаются DNS-запись и количество запросов. По нажатию на DNS-запись или соответствующую ей линию в строку фильтрации добавляется параметр с этой DNS-записью (например, `dns.query.rrname == "example.org"`).

DNS-записи по типам

Виджет **DNS-записи по типам** представляет собой круговую диаграмму. Диаграмма отражает долю каждого типа DNS-записей в общем количестве запросов к DNS-серверу.

При наведении курсора на сектор круга отображаются тип DNS-записей и количество запросов к DNS-серверу. По нажатию на сектор круга в строку фильтрации добавляется параметр с типом DNS-запроса (например, `dns.query.rrtype == "A"`). Вы можете убрать тип DNS-записей с диаграммы, выбрав его в списке под диаграммой.

A.6. Категория виджетов Индикаторы компрометации

В категорию **Индикаторы компрометации** (IOC) входят виджеты со статистикой обнаружения индикаторов компрометации в трафике.

IP-адреса клиентов (из реп. списков)

Виджет **IP-адреса клиентов (из реп. списков)** показывает, какие IP-адреса клиентов из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются IP-адрес клиента и то количество раз, которое он встретился в трафике. По нажатию на IP-адрес или соответствующую ему линию в строку фильтрации добавляется параметр с этим IP-адресом (например, `src.ip == 203.0.113.113`).

IP-адреса серверов (из реп. списков)

Виджет **IP-адреса серверов (из реп. списков)** показывает, какие IP-адреса серверов из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются IP-адрес сервера и то количество раз, которое он встретился в трафике. По нажатию на IP-адрес или соответствующую ему линию в строку фильтрации добавляется параметр с этим IP-адресом (например, `dst.ip == 203.0.113.1`).

URL из реп. списков

Виджет **URL из реп. списков** показывает, какие URL из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются URL и то количество раз, которое он встретился в трафике. По нажатию на URL или соответствующую ему линию в строку фильтрации добавляется параметр с этим URL (например, `http.rqs.url == "https://example.net/about"`).

Доменные имена из реп. списков в DNS-записях

Виджет **Доменные имена из реп. списков в DNS-записях** показывает, какие доменные имена из репутационных списков встречались в DNS-записях чаще всего.

При наведении курсора на линию отображаются доменное имя и то количество раз, которое оно встретилось в DNS-записях. По нажатию на доменное имя или соответствующую ему линию в строку фильтрации добавляется параметр с этим доменным именем (например, `dns.query.rrname == "example.com"`).

Доменные имена клиентов (из реп. списков)

Виджет **Доменные имена клиентов (из реп. списков)** показывает, какие доменные имена клиентов из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются доменное имя клиента и то количество раз, которое оно встретилось в трафике. По нажатию на доменное имя или соответствующую ему линию в строку фильтрации добавляется параметр с этим доменным именем (например, `src.dns == "example.com"`).

Доменные имена серверов (из реп. списков)

Виджет **Доменные имена серверов (из реп. списков)** показывает, какие доменные имена серверов из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются доменное имя сервера то количество раз, которое оно встретилось в трафике. По нажатию на доменное имя или соответствующую ему линию в строку фильтрации добавляется параметр с этим доменным именем (например, `dst.dns == "example.org"`).

Индикаторы компрометации по времени

Виджет **Индикаторы компрометации по времени** показывает, сколько раз за выбранную единицу времени PT NAD обнаруживал индикаторы компрометации.

При наведении курсора на цветной отрезок столбца отображаются время и количество обнаружений индикаторов компрометации этого цвета. По нажатию на цветной отрезок столбца в строку фильтрации добавляется параметр с соответствующим этому цвету значением (например, `rpt.color == 1`). Вы можете скрыть информацию об обнаружениях индикаторов компрометации определенного цвета, выбрав его в списке под диаграммой. Когда вы выделяете период на виджете, аналогичный период выбирается на диаграмме интенсивности трафика (см. раздел 6.3).

Проверка во внешней системе (ВПО)

Виджет **Проверка во внешней системе (ВПО)** показывает, какие типы вредоносного и потенциально опасного ПО обнаруживались чаще всего внешней аналитической системой (при настроенной интеграции PT NAD с PT MultiScanner или PT Sandbox).

При наведении курсора на линию отображаются результат проверки (тип ПО) и количество обнаружений этого типа ПО в трафике. По нажатию на результат проверки или соответствующую ему линию в строку фильтрации добавляется параметр с этим результатом (например, `rpt.verdict == "virus"`).

Реп. списки по числу срабатываний

Виджет **Реп. списки по числу срабатываний** показывает репутационные списки, которые срабатывали чаще других.

При наведении курсора на линию отображаются название репутационного списка и количество его срабатываний. По нажатию на название репутационного списка или соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `rpt.cat == "list_1"`).

Файлы из реп. списков

Виджет **Файлы из реп. списков** показывает, какие файлы из репутационных списков встречались в трафике чаще всего.

При наведении курсора на линию отображаются самое часто встречающееся название файла с указанной хеш-суммой MD5 и то количество раз, которое этот файл встретился в трафике. По нажатию на название файла или на линию в строку фильтрации добавляется параметр с названием файла (например, `files.filename == "win32.exe"`), по нажатию на хеш-сумму — параметр с хеш-суммой (например, `files.md5 == "340cf64a0fbf...49b63"`).

Проверка во внешней системе (файлы)

Виджет **Проверка во внешней системе (файлы)** показывает, какие опасные и потенциально опасные файлы чаще всего обнаруживались внешней аналитической системой (при настроенной интеграции PT NAD с PT MultiScanner или PT Sandbox).

При наведении курсора на линию отображаются самое часто встречающееся название файла с указанной хеш-суммой MD5 и то количество раз, которое этот файл встретился в трафике. По нажатию на название файла или на линию в строку фильтрации добавляется параметр с названием файла (например, `files.filename == "win32.exe"`), по нажатию на хеш-сумму — параметр с хеш-суммой (например, `files.md5 == "340cf64a0fbf...49b63"`).

См. также

Составление списка исключений из DGA-доменов (см. раздел 20.6)

Просмотр информации о вредоносном ПО во внешней аналитической системе (см. раздел 18.2)

A.7. Категория виджетов Учетные данные

В категорию **Учетные данные** входят виджеты со статистикой использования пар «логин — пароль», извлеченных из трафика.

Успешная аутентификация

Виджет **Успешная аутентификация** отображает список логинов с указанием количества сессий с успешными попытками аутентификации.

При наведении курсора на линию отображаются логин и количество сессий, в которых были успешные попытки аутентификации с использованием этого логина. По нажатию на логин или соответствующую ему линию в строку фильтрации добавляются параметры с этим логином и признаком успешной аутентификации (например, `credentials.login == "admin" && credentials.valid == "true"`).

Неуспешная аутентификация

Виджет **Неуспешная аутентификация** отображает список логинов с указанием количества сессий с неуспешными попытками аутентификации.

При наведении курсора на линию отображаются логин и количество сессий, в которых были неуспешные попытки аутентификации с использованием этого логина. По нажатию на логин или соответствующую ему линию в строку фильтрации добавляются параметры с этим логином и признаком неуспешной аутентификации (например, `credentials.login == "admin" && credentials.valid == "false"`).

Пары «логин — пароль» по числу сессий

Виджет **Пары «логин — пароль» по числу сессий** отображает список пар «логин — пароль» с указанием количества сессий с успешными попытками аутентификации.

При наведении курсора на линию отображаются логин и количество сессий с этим логином и паролем. По нажатию на логин в строку фильтрации добавляется параметр с логином (например, `credentials.login == "admin"`), по нажатию на пароль или соответствующую ему линию — параметр с паролем (например, `credentials.password == 1526423068`).

A.8. Категория виджетов Электронная почта

В категорию **Электронная почта** входят виджеты со статистикой сообщений электронной почты.

Почтовые адреса отправителей

Виджет **Почтовые адреса отправителей** отображает список адресов электронной почты с указанием количества отправленных писем.

При наведении курсора на линию отображаются адрес электронной почты и количество отправленных с него писем. По нажатию на адрес электронной почты или соответствующую ему линию в строку фильтрации добавляется параметр с этим адресом (например, `mail.from == "username@example.org"`).

Почтовые адреса получателей

Виджет **Почтовые адреса получателей** отображает список адресов электронной почты с указанием количества полученных писем. Получателями считаются адреса из полей `To`, `Cc` и `Bcc` в заголовках сообщений электронной почты.

При наведении курсора на линию отображаются адрес электронной почты и количество полученных на него писем. По нажатию на адрес электронной почты или соответствующую ему линию в строку фильтрации добавляется параметр с этим адресом (например, `mail.recipient == "username@example.com"`).

Темы писем

Виджет **Темы писем** представляет собой таблицу. Таблица содержит список тем, которые часто встречаются в электронных письмах.

По нажатию на тему в строку фильтрации добавляется параметр с этой темой (например, `mail.subject == "Информация по вашему заказу"`).

A.9. Категория виджетов Файлы

В категорию **Файлы** входят виджеты со статистикой файлов, извлеченных из захваченного трафика.

Названия файлов

Виджет **Названия файлов** показывает список встречающихся в трафике названий файлов.

При наведении курсора на линию отображаются название и количество файлов с этим названием. По нажатию на название файла или на соответствующую ему линию в строку фильтрации добавляется параметр с этим названием (например, `files.filename == "form.php"`).

MIME-типы

Виджет **MIME-типы** отображает список MIME-типов с указанием количества файлов.

При наведении курсора на линию отображаются MIME-тип и количество файлов с этим типом. По нажатию на MIME-тип или на соответствующую ему линию в строку фильтрации добавляется параметр с этим типом (например, `files.mime == "text/plain"`).

Файлы (хеш-суммы)

Виджет **Файлы (хеш-суммы)** показывает список встречающихся в трафике файлов.

При наведении курсора на линию отображаются MD5-хеш-сумма и количество файлов с этой хеш-суммой. По нажатию на MD5-хеш-сумму или на соответствующую ей линию в строку фильтрации добавляется параметр с этой хеш-суммой (например, `files.md5 == "6adf97f83acf6453d4a6a4b1070f3754"`).

Файлы по размерам

Виджет **Файлы по размерам** представляет собой круговую диаграмму. Диаграмма отражает распределение файлов по размерам.

При наведении курсора на сектор круга отображаются диапазон размеров и количество файлов, размеры которых входят в этот диапазон. По нажатию на сектор круга в строку фильтрации добавляется параметр с минимальным и (или) максимальным размерами файлов (например, `files.size > 10000000 && files.size <= 100000000`). Вы можете убрать диапазон с диаграммы, выбрав его в списке под диаграммой.

См. также

Скачивание файлов, переданных в сессиях (см. раздел 9.12)

Скачивание файлов, переданных во время атак (см. раздел 10.11)

Приложение Б. Фильтры и полнотекстовый поиск

В этом приложении приводится справочная информация о языке фильтрации данных продукта.

В этом разделе

См. также

Управление фильтрами (см. раздел 13)

Б.1. Операторы в фильтрах

При составлении фильтров вы можете использовать операторы сравнения, логические операторы, оператор диапазона и оператор множества.

Таблица 6. Операторы в фильтрах

Оператор	Значение	Пример фильтра
Операторы сравнения		
`>`	больше	`pkts.sent > 1000`
`<`	меньше	`alert.pr < 2`
`>=`	больше или равно (не меньше)	`files.size >= 15000`
`<=`	меньше или равно (не больше)	`pkts.total <= 500`
`=`	полнотекстовый поиск по строковым полям (см. раздел Б.3)	`smtp.rqs.mail.subject = 'софт'`
`==`	равно (точное совпадение)	`src.ip == 10.0.0.24`
`<>` `!=`	не равно (не совпадает)	`proto != "TCP"`
`~`	соответствует шаблону	`files.filename ~ '*.exe'`
Логические операторы		
`&&` `and`	и	`src.port == 23518 && dst.port == 445`

Оператор	Значение	Пример фильтра
`||` `or`	или	`dst.dns == "example.com" or src.dns == "example.com"`
`!` `not`	не (отрицание)	`not http.rqs.user-agent ~ "*Windows NT*"`
Прочие операторы		
`in [x,y,z]` `in (x,y,z)`	равно (точное совпадение) одному из перечисленных в скобках значений	`app_proto in [tls,ssh,dns]`
`in [n..m]`	входит в указанный промежуток (от `n` до `m`), где `n` и `m` — целые числа	`bytes.total in [150000..250000]`

Б.2. Параметры фильтрации

Таблица 7. Параметры фильтрации и их значения

Параметр	Значение
`alert`	Сессии с атаками
`alert.att_ck`	Идентификаторы тактик и техник в базе знаний MITRE ATT&CK
`alert.attacker.dns`	Домен атакующего узла
`alert.attacker.geo.asn`	Уникальный номер автономной системы (autonomous system number), присвоенный атакующему узлу
`alert.attacker.geo.city`	Город атакующего узла
`alert.attacker.geo.country`	Двухбуквенный код страны атакующего узла согласно ISO 3166-1
`alert.attacker.geo.org`	Организация атакующего узла
`alert.attacker.groups`	Сессии, в которых адреса атакующих узлов входят в группы узлов (см. раздел 20.7). При настроенной интеграции с MaxPatrol 10 в фильтрации также участвуют группы активов, полученные от этой системы
`alert.attacker.host_id`	Идентификатор атакующего узла (см. раздел 15)
`alert.attacker.hostname`	Название атакующего узла (см. раздел 15.6)
`alert.attacker.ip`	IP-адрес атакующего узла
`alert.cls`	Название класса атаки

Параметр	Значение
alert.false_positive	Сессии с отметками о ложных срабатываниях правил (см. раздел 10.12)
alert.false_positive.author	Логины пользователей, добавивших отметки о ложных срабатываниях правил (см. раздел 10.12.1)
alert.false_positive.date	Дата и время в UTC±0, когда были добавлены отметки о ложных срабатываниях правил (см. раздел 10.12.1), в формате гггг-ММ-ддТчч:мм:сс (например, 2018-08-30T12:49:15)
alert.msg	Название атаки
alert.pr	Уровень опасности атаки
alert.success	Сессии с успешными атаками. Атака является успешной, если для узла обнаружена уязвимость, применимая к такой атаке (по информации из MaxPatrol 10, если была настроена интеграция с этим продуктом)
alert.victim.dns	Домен атакуемого узла
alert.victim.geo.asn	Уникальный номер автономной системы (autonomous system number), присвоенный атакуемому узлу
alert.victim.geo.city	Город атакуемого узла
alert.victim.geo.country	Двухбуквенный код страны атакуемого узла согласно ISO 3166-1
alert.victim.geo.org	Организация атакуемого узла
alert.victim.groups	Сессии, в которых адреса атакуемых узлов входят в группы узлов (см. раздел 20.7). При настроенной интеграции с MaxPatrol 10 в фильтрации также участвуют группы активов, полученные от этой системы
alert.victim.host_id	Идентификатор атакуемого узла (см. раздел 15)
alert.victim.hostname	Название атакуемого узла (см. раздел 15.6)
alert.victim.ip	IP-адрес атакуемого узла
app_proto	Основной прикладной протокол сессии
app_protos	Все прикладные протоколы, задействованные в сессии
app_service	Название приложения (см. приложение Д), которое было задействовано при передаче трафика между клиентом и сервером (Spotify, YouTube и т. п.)
banner.client	Баннер клиента
banner.server	Баннер сервера
bytes.recv	Объем полученных данных в байтах

Параметр	Значение
bytes.sent	Объем отправленных данных в байтах
bytes.total	Весь объем данных в байтах
credentials.login	Фильтрация по логину, выявленному в сессии
credentials.password	Пароль, выявленный в сессии
credentials.valid	Корректная учетная запись
dns	Сессии с протоколом DNS
dns.query.rrname	DNS-запись
dns.query.rrtype	Тип DNS-записи
dst.dns	Домен получателя
dst.geo.asn	Уникальный номер автономной системы (autonomous system number), присвоенный узлу-получателю
dst.geo.city	Город получателя
dst.geo.country	Двухбуквенный код страны получателя согласно ISO 3166-1
dst.geo.org	Организация получателя
dst.groups	Сессии, в которых адреса получателей запросов входят в группы узлов (см. раздел 20.7). При настроенной интеграции с MaxPatrol 10 в фильтрации также участвуют группы активов, полученные от этой системы
dst.host_id	Идентификатор узла получателя (см. раздел 15)
dst.hostname	Название узла получателя (см. раздел 15.6)
dst.ip	IP-адрес получателя
dst.mac	MAC-адрес получателя
dst.port	Порт получателя
errors	Сессии, при сборке которых были обнаружены ошибки (см. приложение E), например отсутствующие или поврежденные пакеты, нехватка ресурсов. При наличии ошибок сессии они отображаются в ее карточке (см. раздел 9.2)
files	Сессии, в которых есть файлы
files.filename	Имя файла
files.md5	MD5-хеш-сумма файла
files.mime	MIME-тип файла

Параметр	Значение
files.rpt.sandbox	Опасное поведение файла, обнаруженное в ходе поведенческого анализа (при настроенной интеграции с PT MultiScanner версии ниже 3.0 или с PT Sandbox): — true — выявлено опасное поведение файла. Такие файлы помечаются значком в карточках сессии и атаки. — false — опасное поведение не выявлено или поведенческий анализ не проводился
files.rpt.verdict	Семейство вредоносного ПО, обнаруженного среди файлов сессии (при настроенной интеграции с PT MultiScanner)
files.size	Размер файла в байтах
flags	Сессии с флагами (см. приложение E) — сообщениями об особенностях сборки сессий. Флаги передают дополнительную информацию о достижении лимитов, появлении неопасного события ИБ или получении сообщений ICMP. При наличии флагов сессии они отображаются в ее карточке (см. раздел 9.2)
ftp	Сессии с FTP
host.dns	Сессии по DNS-имени узла
host.groups	Сессии, в которых адреса узлов входят в группы узлов (см. раздел 20.7). При настроенной интеграции с MaxPatrol 10 в фильтрации также участвуют группы активов, полученные от этой системы
host.host_id	Идентификатор узла (см. раздел 15)
host.hostname	Название узла (см. раздел 15.6)
host.ip	IP-адрес узла
host.port	TCP- или UDP-порт узла
http	Сессии с HTTP
http.rqs.host	Имя узла в HTTP-запросе
http.rqs.url	URL запроса
http.rqs.user-agent	Название баннера HTTP-клиента
icmp	Сессии с ICMP
imap	Сессии с IMAP
ntp	Сессии с NTP

Параметр	Значение
`os.client`	Операционная система отправителя
`os.server`	Операционная система получателя
`pipes`	Сессии, в которых есть именованные каналы
`pipes.bytes.recv`	Объем данных, принятых по именованному каналу, в байтах
`pipes.bytes.sent`	Объем данных, переданных по именованному каналу, в байтах
`pipes.name`	Название именованного канала
`pipes.path`	Путь именованного канала
`pkts.recv`	Количество полученных пакетов
`pkts.sent`	Количество отправленных пакетов
`pkts.total`	Общее количество пакетов
`pop3`	Сессии с POP3
`proto`	Сессии, данные в которых передавались с использованием транспортного протокола (например, `proto == tcp`)
`rpt`	Сессии с обнаруженными индикаторами компрометации (см. раздел А.6)
`rpt.cat`	Название репутационного списка, сработавшего в сессии, или тип вредоносного ПО, обнаруженного PT MultiScanner или PT Sandbox в файлах сессии (при настроенной интеграции с внешней аналитической системой для проверки файлов)
`rpt.color`	Цвет индикатора компрометации, обнаруженного в сессии. Если индикатор компрометации был обнаружен при срабатывании репутационного списка, цвет индикатора компрометации будет соответствовать цвету этого репутационного списка. Возможные значения, соответствующие цветам репутационных списков: — `0` — белый; — `1` — красный; — `2` — черный; — `3` — серый; — `4` — желтый;

Параметр	Значение
	— `5` — синий; — `6` — зеленый; — `7` — оранжевый. Если индикатор компрометации был обнаружен при помощи механизма выявления DGA-доменов, значение `rpt.color` будет `8`. При настроенной интеграции с PT MultiScanner значение `1` используется также для поиска файлов, определенных этим продуктом как опасные, `4` — как потенциально опасные
`rpt.type`	Способ обнаружения индикаторов компрометации: — `"ip"` — сработал репутационный список IP-адресов; — `"dga"` — в атрибутах сессии найден DGA-домен; — `"host"` — сработал репутационный список доменных имен; — `"url"` — сработал репутационный список URL; — `"md5"` — сработал репутационный список хеш-сумм файлов; — `"ms"` — PT MultiScanner определил файл, переданный в ходе сессии, как опасный (при настроенной интеграции с этим продуктом)
`rpt.verdict`	Название вредоносного ПО, которое использует или генерирует DGA-домены (см. раздел 20.6)
`rpt.where`	Место обнаружения в трафике индикатора компрометации: — `"flow.dst"` — среди IP-адресов или доменных имен получателя; — `"flow.src"` — среди IP-адресов или доменных имен отправителя; — `"files"` — в файлах сессии; — `"dns"` — в сообщениях протокола DNS; — `"http"` — в сообщениях протокола HTTP; — `"http.x-f-for"` — в поле X-Forwarded-For в заголовках HTTP-сообщений;

Параметр	Значение
	— `"tls.sni"` — в поле Server Name Indication (SNI) в сообщениях протокола TLS; — `"quic.sni"` — среди доменных имен серверов в сообщениях протокола QUIC
`sip`	Сессии с SIP
`smtp`	Сессии с SMTP
`snmp`	Сессии с SNMP
`src.dns`	Доменное имя источника сетевого взаимодействия
`src.geo.asn`	Уникальный номер автономной системы (autonomous system number), присвоенный узлу-источнику
`src.geo.city`	Город источника
`src.geo.country`	Двухбуквенный код страны источника согласно ISO 3166-1
`src.geo.org`	Организация источника
`src.groups`	Сессии, в которых адреса отправителей запросов входят в группы узлов (см. раздел 20.7). При настроенной интеграции с MaxPatrol 10 в фильтрации также участвуют группы активов, полученные от этой системы
`src.host_id`	Идентификатор узла источника (см. раздел 15)
`src.hostname`	Название узла источника (см. раздел 15.6)
`src.ip`	IP-адрес источника
`src.mac`	MAC-адрес источника
`src.port`	Порт источника
`ssh`	Сессии с протоколом SSH
`state`	Состояние сессии. Возможные значения: `ESTABLISHED` (сессия успешно установлена) и `FINISHED` (сессия успешно закрыта)
`telnet`	Сессии с протоколом Telnet
`tftp`	Сессии с TFTP
`tls`	Сессии с протоколом TLS

Б.3. Полнотекстовый поиск

Некоторые параметры фильтрации доступны для полнотекстового поиска.

Таблица 8. Параметры для полнотекстового поиска

Параметр	Где выполняется полнотекстовый поиск
alert.any	В информации об атаках
alert.false_positive.comment	В комментариях к отметкам о ложных срабатываниях правил (см. раздел 10.12)
any	В информации о сессиях
dns.answer.txt	В TXT-записях протокола DNS, полученных от кэширующего DNS-сервера
dns.authority.txt	В TXT-записях протокола DNS, полученных от DNS-сервера владельца ресурса
dns.any	В полях, относящихся к протоколу DNS
files.any	В информации о файлах
ftp.any	В полях, относящихся к FTP
ftp.rsp.answers	В ответных сообщениях от FTP-сервера
http.any	В полях, относящихся к HTTP
imap.any	В полях, относящихся к IMAP
imap.rsp.args	В ответных сообщениях от IMAP-сервера
mail.subject	В темах сообщений электронной почты
pop3.any	В полях, относящихся к POP3
pop3.rsp.args	В ответных сообщениях от POP3-сервера
sip.any	В полях, относящихся к SIP
smtp.any	В полях, относящихся к SMTP
snmp.any	В полях, относящихся к SNMP
ssh.any	В полях, относящихся к протоколу SSH
telnet.any	В полях, относящихся к протоколу TELNET
telnet.rqs	В запросах протокола TELNET
telnet.rsp	В ответных сообщениях протокола TELNET
tftp.any	В полях, относящихся к TFTP
tls.any	В полях, относящихся к протоколу TLS

Б.4. Примеры фильтров

В таблице ниже приведены примеры фильтров.

Таблица 9. Примеры фильтров

Фильтр	Описание
`!files`	Сессии без файлов
`dst.ip == 213.180.204.3`	Сессии с IP-адресом получателя 213.180.204.3
`alert.pr <= 2`	Сессии с уровнем опасности атаки не меньше 2 (то есть со средним или высоким уровнем опасности атаки)
`dst.dns ~ "ptsec*"`	Сессии, в которых домен получателя соответствует шаблону `ptsec*`
`files.filename ~ '*.jpg'`	Сессии с файлами, имеющими расширение .jpg
`http(rqs.method == POST and rsp.status == OK)`	Сессии с HTTP-запросом методом POST и ответом 200 OK
`src.ip == 198.51.100.31 and not http.rqs.user-agent ~ "*Windows NT*"`	Сессии с IP-адресом источника 198.51.100.31 и таким названием баннера HTTP-клиента, которое не совпадает с шаблоном `*Windows NT*`
`dst.dns == "example.org" && http`	Сессии с доменом получателя example.org, включающие HTTP-запросы и ответы
`!errors && !flags`	Сессии без ошибок обработки и флагов

Приложение В. Прикладные протоколы, обнаруживаемые PT NAD

В этом разделе перечислены протоколы прикладного уровня, которые PT NAD может обнаруживать в трафике. Для каждого протокола в таблице указано, может ли PT NAD разбирать сообщения этого протокола и извлекать файлы из трафика.

Таблица 10. Обнаруживаемые прикладные протоколы

Обозначение	Протокол	Разбор	Извлечение файлов
amqp	Advanced Message Queuing Protocol (amqp.org)	—	—
bgp	Border Gateway Protocol (RFC4271)	—	—
bitcoin	Протокол Bitcoin (en.bitcoin.it)	—	—
bittorrent	Протокол BitTorrent (bittorrent.org)	—	—
canon-bjnp	Протокол обнаружения сервиса LAN, используемый в принтерах и сканерах Canon (canon.com)	—	—
clickhouse	Протокол системы управления базами данных ClickHouse (clickhouse.com)	—	—
db2-drda	DB2 Distributed Relational Database Architecture (ibm.com)	—	—
dcerpc	Distributed Computing Environment / Remote Procedure Call	✔	—
dhcp	Dynamic Host Configuration Protocol (RFC 2131)	✔	—
dhcpv6	Dynamic Host Configuration Protocol for IPv6 (RFC 3315)	—	—
dns	Domain Name System (RFC 1034)	✔	—
drweb	Протокол продукта Dr.Web Enterprise Security Suite (drweb.ru)	—	—
dtls	Datagram Transport Layer Security (RFC 6347)	✔	—

Обозначение	Протокол	Разбор	Извлечение файлов
elasticsearch	Протокол системы Elasticsearch (elastic.co)	—	—
encrypted	Неизвестный зашифрованный протокол	—	—
facebook	Протокол сети Facebook (developers.facebook.com)[3]	—	—
falcongaze	Протокол продукта Falcongaze SecureTower Agent (falcongaze.com)	—	—
fb-zero	Протокол сети Facebook Zero (0.facebook.com)[3]	—	—
ftp	File Transfer Protocol (RFC 959)	✔	✔
guardant	Протокол продукта Guardant Net (guardant.ru)	—	—
http	Hypertext Transfer Protocol	✔	✔
http2	Hypertext Transfer Protocol version 2 (http2.github.io)	✔	✔
icap	Internet Content Adaptation Protocol (RFC 3507)	—	—
imap	Internet Message Access Protocol (RFC 3501)	✔	✔
infowatch	Протокол продукта InfoWatch Device Monitor (infowatch.ru)	—	—
isakmp	Internet Security Association and Key Management Protocol (RFC 2408)	—	—
jrmi	Java Remote Method Invocation Protocol (oracle.com)	—	—
kafka	Протокол платформы Apache Kafka (kafka.apache.org)	—	—
kerberos	Протокол аутентификации Kerberos (RFC 4120)	✔	—

3 Facebook, Instagram и WhatsApp — продукты компании Meta, которая, в соответствии с законодательством Российской Федерации, признана экстремистской организацией и запрещена в России.

Обозначение	Протокол	Разбор	Извлечение файлов
ksn	Протокол сети Kaspersky Security Network (kaspersky.ru/ksn)	—	—
ldap	Lightweight Directory Access Protocol (RFC 4510)	✔	—
llmnr	Link-Local Multicast Name Resolution (RFC 4795)	—	—
lotus	Протокол платформы HCL Notes (ранее IBM Notes и Lotus Notes)	—	—
mc-nmf	Net.TCP Port Sharing (docs.microsoft.com)	✔	—
mdns	Multicast DNS (RFC 6762)	—	—
memcache	Протокол системы Memcached (memcached.org)	—	—
mongodb	Протокол системы управления базами данных MongoDB (docs.mongodb.com)	—	—
ms-scom	Протокол программы System Center Operations Manager (docs.microsoft.com)	—	—
ms-update	Протокол утилиты Windows Update Delivery Optimization (docs.microsoft.com)	—	—
mysql	Протокол системы управления базами данных MySQL (dev.mysql.com)	✔	—
nat-t	NAT Traversal	—	—
nbns	NetBIOS Name Server (RFC 1001)	—	—
nfs	Network File System (RFC 1094)	✔	✔
ntlm	NT LAN Manager (docs.microsoft.com)	✔	—
ntp	Network Time Protocol (ntp.org)	✔	—
openvpn	Протокол технологии OpenVPN (openvpn.net)	—	—

Обозначение	Протокол	Разбор	Извлечение файлов
oracle-tns	Oracle TNS (Transparent Network Substrate, протокол компании Oracle)	✔	—
p2p-dc	Протокол Direct Connect	—	—
pop3	Post Office Protocol 3 (RFC 1081)	✔	✔
postgresql	Протокол системы управления базами данных PostgreSQL (postgresql.org)	✔	—
pptp	Point-to-Point Tunneling Protocol (RFC 2637)	—	—
printer-pjl	Протокол Printer Job Language (hp.com)	—	—
printer-ps	Протокол печати PostScript (adobe.com)	—	—
quic	A UDP-Based Multiplexed and Secure Transport, экспериментальный протокол Google (tools.ietf.org/html/draft-ietf-quic-transport-27)	✔	—
radius	Remote Authentication Dial In User Service (RFC 2865)	—	—
rdp	Remote Desktop Protocol (docs.microsoft.com)	✔	—
redis	Протокол системы управления базами данных Redis (redis.io)	—	—
rexec	Протокол приложения REXEC (ibm.com)	—	—
rfb	Remote Framebuffer (RFC 6143)	—	—
rlogin	BSD Rlogin (RFC 1282)	—	—
rsync	Протокол утилиты rsync (rsync.samba.org)	—	—
rtcp	Real-Time Transport Protocol (RFC 3550)	—	—
rtsp	Real-Time Streaming Protocol (RFC 7826)	—	—

Обозначение	Протокол	Разбор	Извлечение файлов
sap	Session Announcement Protocol (RFC 2974)	—	—
sip	Session Initiation Protocol (RFC 3261)	✔	—
skinny-voip	Skinny Client Control Protocol (cisco.com)	—	—
skype	Протокол программы Skype (skype.com)	—	—
smb	Server Message Block (docs.microsoft.com)	✔	✔
smb-mailslot	Server Message Block Mailslot (docs.microsoft.com)	—	—
smtp	Simple Mail Transfer Protocol (RFC 5321)	✔	✔
snmp	Simple Network Management Protocol	✔	—
socks5	SOCKS 5 (RFC 1928)	✔	—
splunk	Протокол платформы Splunk (splunk.com)	—	—
ssdp	Simple Service Discovery Protocol	—	—
ssh	Secure Shell (RFC 4251)	✔	—
stakhanovets	Протокол DLP-системы компании «Стахановец» (stakhanovets.ru/dlp)	—	—
stratum	Протокол майнинга Stratum (reference.cash/mining/stratum-protocol)	—	—
stun	Session Traversal Utilities for NAT (RFC 3489)	—	—
stun-apple			
stun-classic			
syslog	Протокол системного журнала (RFC 5424)	—	—
tds	Tabular Data Stream (docs.microsoft.com)	✔	—

Обозначение	Протокол	Разбор	Извлечение файлов
teamviewer	Протокол программы TeamViewer (teamviewer.com)	—	—
telnet	Telnet (RFC 854)	✔	—
tftp	Trivial File Transfer Protocol (RFC 1350)	✔	✔
thrift	Протокол фреймворка Apache Thrift (thrift.apache.org)	—	—
tls	Transport Layer Security (RFC 8446)	✔	—
trueconf	Протокол системы TrueConf (trueconf.ru)	—	—
umeye-app	Протокол приложения UMEye (umeye.com)	—	—
viber	Протокол приложения Viber (viber.com)	—	—
vipaks-data	Протокол передачи видео компании «Випакс» (vipaks.ru)	—	—
vipnet	Протоколы системы ViPNet VPN (infotecs.ru)	—	—
vipnet-mftp			
vipnet-sync			
vpn_kontinent	Протокол комплекса шифрования «Континент» (securitycode.ru)	—	—
vmware	Протокол компании VMware (vmware.com)	—	—
whatsapp	Протокол приложения WhatsApp (whatsapp.com)[3]	—	—
wireguard	WireGuard (wireguard.com)	—	—
ws-discovery	Web Services Dynamic Discovery (specs.xmlsoap.org)	—	—
xmpp	Extensible Messaging and Presence Protocol (xmpp.org)	—	—
zabbix	Протокол системы Zabbix (zabbix.com)	—	—

Обозначение	Протокол	Разбор	Извлечение файлов
`zmtp`	ZeroMQ Message Transport Protocol (zeromq.org)	—	—
`zmtp_v2`			

Приложение Г. Протоколы туннелирования, обнаруживаемые PT NAD

PT NAD может распознавать трафик, инкапсулируемый в пакеты протоколов туннелирования (см. таблицу ниже). Распознавание работает также и в том случае, когда туннели вложены один в другой (максимально допустимый уровень вложенности — 256).

Таблица 11. Протоколы туннелирования, обнаруживаемые PT NAD

Протокол	**Описание**
802.1Q (VLAN)	ieee802.org/1/pages/802.1Q-2014.html
ERSPAN (Type I, Type II, Type III)	datatracker.ietf.org/doc/html/draft-foschiano-erspan-03
Geneve	RFC 8926
GRE	RFC 1701
IP in IP	RFC 1853
MPLS	RFC 5332
PPP	RFC 1661
PPPoE	RFC 2516
QinQ	ieee802.org/1/pages/802.1ad.html
Teredo	RFC 4380
TZSP	en.wikipedia.org/wiki/TZSP
VNTag	ieee802.org/1/files/public/docs2009/new-pelissier-vntag-seminar-0508.pdf
VXLAN	RFC 7348

Приложение Д. Приложения, обнаруживаемые PT NAD

PT NAD может идентифицировать приложения, в том числе веб-приложения, а также сайты и служебные сервисы, которые использовались при передаче трафика. Такие приложения перечислены в таблице ниже.

Таблица 12. Обнаруживаемые приложения

Категория или компания-производитель	**Обозначение**	**Приложение**
Банкинг	`Sber.online`	СберБанк Онлайн
Безопасность	`Kaspersky-agent`	Kaspersky Endpoint Agent
Видео и стриминг	`1kxun`	1kxun
	`AmazonVideo`	Amazon Prime Video
	`Hulu`	Hulu
	`IFLIX`	iflix
	`iQIYI`	iQIYI
	`NetFlix`	Netflix
	`OCS`	OCS
	`PPStream`	PPStream
	`QuickPlay`	Quickplay
	`RapidVideo`	Rapid Video
	`Rutube`	Rutube
	`Showmax`	Showmax
	`Vevo`	Vevo
	`VidTO`	Vidto
	`Vkontakte.live`	VK Play Live
	`Vkontakte.video`	VK Видео
	`Yandex.video`	Яндекс Видео
	`YouTube`	YouTube
	`YouTubeUpload`	YouTube Upload
Игры	`Nintendo`	Nintendo
	`Playstation`	PlayStation

Категория или компания-производитель	Обозначение	Приложение
	Steam	Steam
	WorldOfWarcraft	World of Warcraft
Интернет-сервисы	Cloudflare	Cloudflare
	DNScrypt	DNSCrypt
	DoH_DoT	DNS over HTTPS и DNS over TLS
	Ntop	Ntop
	Ookla	Ookla
	OpenDNS	OpenDNS
	UbuntuONE	Ubuntu One
Карты	2gis	2ГИС
	GoogleMaps	Google Maps
	Waze	Waze
	Yandex.maps	Яндекс Карты
Маркетплейсы	Amazon	Amazon
	eBay	eBay
	Ozon	Ozon
	Wildberries	Wildberries
Медиа	CNN	CNN
	Wikipedia	Wikipedia
Мессенджеры	Discord	Discord
	ICQ	ICQ
	Imo	imo
	KakaoTalk	KakaoTalk
	Ktalk	Контур.Толк
	Line	Line
	Mattermost	Mattermost
	QQ	QQ
	Signal	Signal
	Skype	Skype
	Slack	Slack

Категория или компания-производитель	Обозначение	Приложение
	Teams	Microsoft Teams
	Telegram	Telegram
	Viber	Viber
	Webex	Webex
	WeChat	WeChat
	WhatsApp	WhatsApp[4]
	WhatsAppFiles	WhatsAppFiles[4]
	Zoom	Zoom
Музыка	Deezer	Deezer
	LastFM	Last.fm
	Musical.ly	Musical.ly
	Pandora	Pandora
	SoundCloud	SoundCloud
	Spotify	Spotify
	Vevo	Vevo
	Vkontakte.audio	VK Музыка
	Yandex.music	Яндекс Музыка
Обмен файлами	Anonfiles	AnonFile
	BitTorrent	BitTorrent
	Box	Box
	Catbox.moe	Catbox
	DropBox	Dropbox
	Dropmefiles	DropMeFiles
	Dropsend	DropSend
	Fastupload.io	Fastupload.io
	File.io	File.io
	FileMail	Filemail
	Files.fm	Files.fm

4 Facebook, Instagram и WhatsApp — продукты компании Meta, которая, в соответствии с законодательством Российской Федерации, признана экстремистской организацией и запрещена в России.

Категория или компания-производитель	Обозначение	Приложение
	Filesend.io	FileSend.IO
	Filetransfer.io	FileTransfer.io
	Gitflic	GitFlic
	Github	GitHub
	Gitlab	GitLab
	GoogleDrive	Google Drive
	Internxt	Internxt
	IPFS	IPFS
	Jumpshare	Jumpshare
	Justbeamit	JustBeamIt
	Karelia	Disk Karelia
	Mail.ru Cloud	Облако Mail.ru
	Mediafire	MediaFire
	MEGA	Mega
	MS_OneDrive	OneDrive
	Onehub	Onehub
	Pastebin	Pastebin
	Pcloud	pCloud
	Pixeldrain	Pixeldrain
	Rediafile	Rediafile
	Send-Anywhere	Send Anywhere
	Sendspace	Sendspace
	Storj	Storj
	SugarSync	SugarSync
	Tresorit	Tresorit
	Ufile.io	Ufile.io
	Vis.ee	ffsend
	Wdfiles	WDfiles
	Wetransfer	WeTransfer
	Yandex.disk	Яндекс Диск

Категория или компания-производитель	Обозначение	Приложение
Социальные сети	Baidu	Baidu
	Douyin	Douyin
	Facebook	Facebook[4]
	Instagram	Instagram[4]
	Kuaishou	Kuaishou
	Likee	Likee
	LinkedIn	LinkedIn
	Livejournal	LiveJournal
	Messenger	Facebook Messenger[4]
	Odnoklassniki	Одноклассники
	Quora	Quora
	Reddit	Reddit
	Sina(Weibo)	Sina Weibo
	Snapchat	Snapchat
	TikTok	TikTok
	Tinder	Tinder
	Tuenti	Tuenti
	Twitch	Twitch
	Twitter	X (Twitter)
	Vkontakte	ВКонтакте
Удаленный доступ	Aeroadmin	AeroAdmin
	AmmyyAdmin	Ammyy Admin
	Anydesk	AnyDesk
	LiteManager	LiteManager
	Myassistance	Ассистент
	Radmin	Radmin
	RemoteAdmin	RemoteAdmin
	RMS	Remote Manipulator System
	Teamviewer	TeamViewer
Электронная почта	GMail	Gmail

Категория или компания-производитель	Обозначение	Приложение
	Hotmail	Hotmail
	Mail.ru	Mail.ru
	MSN	MSN
	ProtonMail	Proton Mail
	Sina	Sina
	Yahoo	Yahoo
	Yandex.mail	Яндекс Почта
Яндекс	Yandex	Яндекс
	Yandex.disk	Яндекс Диск
	Yandex.mail	Яндекс Почта
	Yandex.maps	Яндекс Карты
	Yandex.music	Яндекс Музыка
	Yandex.video	Яндекс Видео
Apple	AppleiCloud	iCloud
	AppleiTunes	iTunes
	ApplePush	Служба push-уведомлений Apple
	AppleStore	App Store
Google	DataSaver	Data Saver
	GMail	Gmail
	Google	Google
	GoogleDocs	Google Docs
	GoogleDrive	Google Drive
	GoogleHangout	Google Hangout
	GoogleMaps	Google Maps
	GooglePlus	Google Plus
	GoogleServices	Google Services Framework
	PlayStore	Google Play
Microsoft	Hotmail	Hotmail
	Microsoft	Microsoft
	MS_OneDrive	OneDrive

Категория или компания-производитель	Обозначение	Приложение
	MSN	MSN
	Office365	Microsoft 365
	Teams	Microsoft Teams
	WindowsUpdate	Windows Update
VK	Vkontakte	ВКонтакте
	Vkontakte.audio	VK Музыка
	Vkontakte.live	VK Play Live
	Vkontakte.pay	VK Pay
	Vkontakte.video	VK Видео
VPN	Cyberghost-vpn	CyberGhost VPN
	HotspotShield	Hotspot Shield
	Opera-vpn	Opera VPN
	Steganos-vpn	Steganos VPN Online Shield

Приложение E. Флаги и ошибки обработки сессий

При анализе соединения и сборке сессии PT NAD может добавлять в свойства сессии дополнительную информацию об анализе пакетов сессии, сборке сессии и записи трафика в хранилище. PT NAD показывает эту информацию в виде флагов и ошибок в карточках сессий и атак. Флаги и ошибки могут быть полезными при диагностике неполадок сетевого оборудования и при исправлении неправильной сетевой конфигурации, а также могут понадобиться при обращении в службу технической поддержки.

Ошибки обработки сессий указывают на потери данных при захвате трафика, отсутствие нужных сегментов в захваченном трафике, проблемы с распознаванием данных или их записью в хранилище. Вы можете найти сессии с ошибками, введя в строку фильтрации `errors` или `errors == "<Название ошибки>"` (например, `errors == "ASYNC"`) и нажав клавишу Enter.

Таблица 13. Ошибки обработки сессий

Название ошибки	Текст ошибки	Примечание
APP_LAYER_DISABLED	Не удалось завершить анализ трафика, переданного по протоколу прикладного уровня. Возникли потери данных или данные не были распознаны	Если анализ трафика был остановлен по причине потери данных, APP_LAYER_DISABLED будет сопровождаться ошибкой GAP_DETECT
ASYNC	Не удалось проанализировать часть трафика сессии. Не обнаружена передача данных одной из сторон TCP-соединения	Может возникнуть: — из-за особенностей записи VLAN-тегов в организации; — некорректной настройки зеркалирования трафика; — неправильной настройки захвата (см. раздел 20.1.4) туннелированного трафика в PT NAD
BAD_CHECKSUM	В трафике сессии есть поврежденные пакеты. Нарушение их целостности обнаружено при проверке контрольных сумм	В текущей версии PT NAD проверяет контрольные суммы только у сегментов TCP. Поврежденные пакеты не анализируются. В нормальной ситуации получатель отклоняет поврежденный пакет, и отправитель пересылает его повторно. Если этого не произошло, поврежденный пакет может повлиять на анализ соединения и сборку сессии в PT NAD. В некоторых случаях из-за особенно-

Название ошибки	Текст ошибки	Примечание
		стей настройки сетевого оборудования может потребоваться отключить проверку контрольных сумм в PT NAD. Для этого вам нужно обратиться к администратору
GAP_DETECT	Не удалось полностью проанализировать TCP-соединение. Возникли потери данных	При захвате трафика был потерян один или несколько TCP-сегментов с данными. При этом, если задействованный в соединении протокол прикладного уровня поддерживает синхронизацию после обрыва связи, PT NAD попытается продолжить анализ TCP-соединения (см. описание флага APP_SYNCED). TCP-сегменты могут быть потеряны при зеркалировании трафика из-за ошибок в коммутаторах или проблем при захвате трафика PT NAD
L4_DIR_TOGGLED	Не удалось вовремя определить корректное направление передачи данных. Направление было определено после создания записи сессии и не соответствует протоколу транспортного уровня	Аналогична ошибке PARSE_TOGGLED, но относится к протоколу транспортного уровня (L4)
MISSED_END	Не удалось обнаружить закрытие TCP-соединения. Не найден сегмент с флагом FIN или RST	Аналогична ошибке GAP_DETECT, но потери сегментов с флагом FIN или RST возникли в конце TCP-соединения
MISSED_START	Не удалось получить информацию о согласовании TCP-соединения (three-way handshake). Не найдены сегменты с флагами SYN и SYN, ACK	Может повлиять на корректное определение: — направления передачи данных; — прикладного протокола; — количества переданных байтов и пакетов

Название ошибки	Текст ошибки	Примечание
OUT_OF_WINDOW	Не удалось завершить анализ TCP-соединения. Потери данных превысили лимит	Лимит определяется конфигурацией PT NAD и по умолчанию равен 10 КБ. До закрытия TCP-соединения он может быть переопределен параметрами самого соединения, но это значение не может быть меньше указанного в конфигурации. Для изменения лимита вам нужно обратиться к администратору
PARSE_TOGGLED	Не удалось вовремя определить корректное направление передачи данных. Направление было определено после создания записи сессии и не соответствует протоколу прикладного уровня	Аналогична ошибке L4_DIR_TOGGLED, но относится к протоколу прикладного уровня (L7)
PCAP_DROPS	Не удалось записать часть сессии в хранилище файлов PCAP. Скорость передачи данных превысила скорость их записи на диск	Не влияет на анализ соединения
REASM_BROKEN	Не удалось завершить сборку сессии. Возникла рассинхронизация потоков данных TCP-соединения	При появлении большого количества записей сессий с этой ошибкой нужно обратиться в службу технической поддержки (см. раздел 22)
REASM_LIMIT	Не удалось завершить сборку сессии. Количество пакетов, переданных в TCP-соединении без подтверждения, достигло установленного лимита	Лимит определяется конфигурацией PT NAD и по умолчанию равен 1000. Для изменения лимита вам нужно обратиться к администратору
RES_LIMIT	Не удалось проанализировать часть трафика сессии. Недостаточно памяти	Возникает в том случае, когда PT NAD исчерпывает объем памяти, выделенный для анализа TCP-соединения. При появлении большого количества записей сессий с этой ошибкой рекомендуется обратиться к администратору

Название ошибки	Текст ошибки	Примечание
SSN_BROKEN	Не удалось проанализировать TCP-соединение. Переданы некорректные или нераспознанные данные	При появлении большого количества записей сессий с этой ошибкой нужно обратиться в службу технической поддержки (см. раздел 22)

Флаги сессий — это сообщения об особенностях сборки сессий. В отличие от ошибок сессий, флаги не указывают на проблемы, а передают информацию о достижении лимитов, появлении неопасного события ИБ или получении сообщений ICMP. Вы можете найти сессии с флагами, введя в строку фильтрации `flags` или `flags == "<Название флага>"` (например, `flags == "MIDSTREAM"`) и нажав клавишу Enter.

Таблица 14. Флаги сессий

Название флага	Текст флага	Примечание
APP_SERVICE_ML	Приложение определено при помощи алгоритма машинного обучения	PT NAD определяет приложение, которое было задействовано при передаче трафика между клиентом и сервером (записывается в поле `app_service`). Флаг указывает на то, что в ходе этого определения было применено машинное обучение
APP_SYNCED	Анализ TCP-соединения возобновлен после появления ошибки GAP_DETECT	Не все прикладные протоколы, обнаруживаемые PT NAD, поддерживают синхронизацию сообщений между отправителем и получателем после обрыва связи. Если в соединении синхронизация сообщений между отправителем и получателем была успешно выполнена хотя бы один раз, PT NAD помечает такое соединение флагом APP_SYNCED
BREAK	Не удалось завершить анализ TCP-соединения. Потери данных превысили лимит	Возникает при создании записи о сессии для соединения, при анализе которого возникла ошибка OUT_OF_WINDOW
FORCED_CLOSED	Некорректные данные о закрытии соединения. При передаче данных из модуля ptdpi в БД возникли потери	Может возникнуть из-за аварийного завершения работы модуля ptdpi во время сессии. В атрибутах этой сессии время завершения сессии будет фактически со-

Название флага	Текст флага	Примечание
		ответствовать времени последнего обновления информации о соединении. Для соединений короче 30 секунд время завершения сессии будет тем же, что и время ее начала
ICMP_DST_UNREACH	Получено сообщение ICMP «Destination Unreachable»	См. RFC 792
ICMP_TIMEEXCD	Получено сообщение ICMP «Time Exceed»	См. RFC 792
MIDSTREAM	Не удалось проанализировать TCP-соединение. Возникли потери данных или модуль ptdpi был запущен после открытия TCP-соединения	Флаг всегда сопровождается ошибкой MISSED_START в той же записи сессии
MULTI_FLOW	Сессии объединены на основании общих признаков	Возникает при обнаружении флуд-атаки (отправка множества схожих запросов разными отправителями на один IP-адрес) или сеанса сканирования (отправка множества схожих запросов разным получателям с одного IP-адреса)
MULTI_TUNNELS	Несколько разных туннелей в одном соединении	Пакеты одного соединения, идущие в разных направлениях, имеют разные теги VLAN или помещены в разные туннели
PARSE_LIMIT	Анализ трафика приостановлен. Объем данных, переданных в сессии, достиг установленного для протокола лимита	Для получения информации о настроенных лимитах и их изменения вам нужно обратиться к администратору
PCAP_LIMIT	Запись PCAP приостановлена. Объем данных, переданных в сессии, достиг установленного для протокола лимита	Для получения информации о настроенных лимитах и их изменения вам нужно обратиться к администратору
RULES_DETECT_LIMIT	Выявление атак приостановлено. Объем данных, переданных в сессии, достиг установленного для протокола лимита	Для получения информации о настроенных лимитах и их изменения вам нужно обратиться к администратору

Название флага	Текст флага	Примечание
SPLIT	Показана информация только о части сессии	Информация о сессии, которая началась в один день и завершилась в другой, разделяется на части и представлена в интерфейсе несколькими записями сессий, каждая из которых будет помечена флагом SPLIT. При работе с сессиями с флагом SPLIT могут возникать проблемы со скачиванием извлеченных файлов и PCAP-файлов

См. также

Включение экспертного режима просмотра флагов и ошибок обработки сессий (см. раздел 9.7)

Приложение Ж. Синтаксис правил для обнаружения атак

PT NAD использует сигнатурный движок, частично совместимый с Suricata 5. Подробное описание синтаксиса, используемого для написания правил в Suricata 5, доступно на сайте его разработчика. В этом разделе перечислены отличительные особенности синтаксиса правил PT NAD.

В этом разделе

См. также

Правила в PT NAD (см. раздел 2.2)

Работа с правилами для обнаружения атак (см. раздел 20.2)

Ж.1. Поддерживаемые ключевые слова Suricata 5

PT NAD поддерживает все ключевые слова Suricata 5, за исключением:

- ключевых слов SSH;
- ключевых слов Transformations;
- bypass;
- filesha1;
- filesha256;
- http.start;
- ja3s.hash;
- ja3s.string;
- prefilter;
- ssl_state;
- tls.certs;
- tls.issuerdn;
- tls.store;
- tls.subject.

В контексте ключевого слова http.header_names не поддерживаются ключевые слова byte_extract и pcre.

Ж.2. Ключевые слова для записи протоколов и приложений

В дополнение к ключевым словам Suricata 5 в PT NAD можно использовать ключевые слова `set_app_proto` и `set_app_service`. Они позволяют через правила для обнаружения атак записывать в метаданные трафика сессии соответственно прикладной протокол и приложение, которые были задействованы при передаче трафика, но не были обнаружены стандартными средствами PT NAD.

> **Внимание!** Протоколы и приложения, записанные таким образом, не могут в дальнейшем использоваться для активации других правил для обнаружения атак. Помимо того, модуль ptdpi не разбирает сообщения прикладного протокола, если он был записан при помощи ключевого слова `set_app_proto`.

Пример правила с использованием ключевого слова `set_app_proto`:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (sid: 123456789; rev:3; msg:"APP
[PTsecurity] Telegram"; set_app_proto: "telegram"; classtype:misc-activity; flow:
established, to_server; stream_size: client, <, 267; stream_size: server, <, 2;
dsize: 265; content: "|07|"; depth: 1; metadata: id_824245; metadata: created_at
2019_02_02, updated_at 2019_07_25;)
```

Пример правила с использованием ключевого слова `set_app_service`:

```
alert http $EXTERNAL_NET any -> $HOME_NET any (sid:987654321; rev:2; msg:"APP
[PTsecurity] Telegram Messenger v3 HTTP"; set_app_service: "telegram";
classtype:misc-activity; flow: established, to_client; content:"200"; http_stat_code;
file_data; content: "|00000000000000001|"; depth:9; content: "|00000063241605|";
distance:8; within:7; fast_pattern; content: "|08|"; distance:32; within:1; content:
"|00000015c4b51c|"; distance:8; within:7; content: "|000000|"; distance:1; within:3;
metadata: autosign, id_681439; metadata: created_at 2018_09_13, updated_at
2019_07_25;)
```

Ж.3. Расширение ptrule для обращения к полям в транзакциях протоколов

С помощью ключевых слов DNS и HTTP из Suricata 5 в правилах для обнаружения атак можно обращаться к полям в транзакциях соответствующих протоколов. Кроме этих ключевых слов, в PT NAD можно также сопоставлять значения полей (см. раздел Ж.3.4) в транзакциях следующих протоколов:

- DCE/RPC;
- FTP;
- POP3;
- QUIC;

— SMB (первая и вторая версии);

— TLS.

Сопоставление выполняется при помощи расширения ptrule сигнатурного движка PT NAD. Расширение использует собственный синтаксис, который позволяет создавать гибкие правила внутри правил для обнаружения атак.

Для использования расширения нужно написать ключевое слово `ptrule`, двоеточие и вложенное правило (далее — правило ptrule). Например:

```
alert ftp any any -> any any (sid:19000030;priority:1;rev:2;msg:"Successful anonymous
FTP login";classtype:unknown; ptrule: ftp.rqs.code == "USER" && ftp.rqs.args ==
"anonymous" && ftp.rsp.code == 230;)
```

Ключевое слово `ptrule` можно комбинировать с другими ключевыми словами.

В этом разделе

Допустимые структуры в правилах ptrule (см. раздел Ж.3.1)

Операторы для полей в правилах ptrule (см. раздел Ж.3.2)

Типы данных в правилах ptrule (см. раздел Ж.3.3)

Поля протоколов, доступные в правилах ptrule (см. раздел Ж.3.4)

Ж.3.1. Допустимые структуры в правилах ptrule

В правиле ptrule допускается использование любого количества и любых комбинаций булевых структур, приведенных в таблице ниже.

Таблица 15. Допустимые структуры в правиле ptrule

Структура	Пояснение	Пример
`<Поле> <Оператор> <Значение>`	Оператор зависит от типа данных поля, с которым он используется (см. раздел Ж.3.2). **Примечание.** Вы не можете сравнивать одно поле с другим	`pop3.rsp.status == "RSP status"`
`<Булево поле>`	То же, что `<Поле> == true` или `<Поле> != false`	`tls.client_cert.valid`
`!<Булево поле>`	То же, что `<Поле> == false` или `<Поле> != true`	`!tls.client_cert.valid`
`<Структура 1> && <Структура 2>`	Правило срабатывает, если обе структуры имеют значение `true`	`ftp.rqs.code == "USER" && ftp.rqs.args == "anonymous"`

Структура	Пояснение	Пример
`<Структура 1> || <Структура 2>`	Правило срабатывает, если хотя бы одна из структур имеет значение `true`	`smb.v2.status == 104 || smb.v2.command == 12`
`!<Структура>`	Правило срабатывает, если структура имеет значение `false`	`!(tls.version == "1.2" && tls.tls_resumed)`

Структуры имеют одинаковый приоритет и читаются слева направо. Для группировки и приоритизации нескольких выражений в одном правиле нужно использовать скобки, например:

```
!((ftp.rsp.code >= 110) && (ftp.rsp.code <= 633))
```

См. также

Поля протоколов, доступные в правилах ptrule (см. раздел Ж.3.4)

Ж.3.2. Операторы для полей в правилах ptrule

Для сопоставления значений полей (см. раздел Ж.3.4) используются операторы сравнения и логические операторы.

Таблица 16. Операторы для полей

Оператор	Значение	Используется с типами данных	Пример
`==`	Равно (точное совпадение). При использовании с типом данных Array of strings результат сравнения `true`, если значение совпадает с хотя бы одной из строк массива	Любыми	`smb.v2.command == 14`
`!=`	Не равно (не совпадает). При использовании с типом данных Array of strings результат сравнения `true`, если значение не совпадает ни с одной из строк массива	Любыми	`ftp.rsp.code != 230`
`>`	Больше	UInt64 и DateTime	`dcerpc.rqs.opnum > 50`

Оператор	Значение	Используется с типами данных	Пример
`>=`	Больше или равно (не меньше)	UInt64 и DateTime	`tls.server_cert.valid.not_before >= "2021-03-01"`
`<`	Меньше	UInt64 и DateTime	`ftp.rsp.code < 500`
`<=`	Меньше или равно (не больше)	UInt64 и DateTime	`tls.server_cert.valid.not_before <= "2022-01-01"`
`~`	Соответствует шаблону (регулярному выражению). Для использования жадного квантификатора в конец нужно добавить `/g`, например `tls.server_cert.serial ~ h"29000016763492 33DA2BCEDBDF000100001676"/g`. При использовании с типом данных Array of strings результат сравнения `true`, если значение совпадает с хотя бы одной из строк массива	String, Array of strings и UUID	`smb.v1.server.native_os ~ "Windows (8|9|10)"`
`&&`	И	Boolean	`tls.client_cert.self_signed && tls.client_cert.valid`
`||`	Или	Boolean	`tls.client_cert.self_signed || tls.client_cert.valid`
`!`	Не (отрицание)	Boolean	`!ftp.rsp.sub_resp`

См. также

Типы данных в правилах ptrule (см. раздел Ж.3.3)

Ж.3.3. Типы данных в правилах ptrule

Расширение ptrule использует строгую типизацию данных — преобразований типов не делается. От типа данных зависит, какой оператор может использоваться (см. раздел Ж.3.2).

Таблица 17. Типы данных

Тип данных	Описание	Примеры значений
UInt	Целое беззнаковое число	`0`, `123`, `0xcde124`, `3399731`
Boolean	Логический тип	`false`, `true`
String	Строковый тип. Можно добавлять в строку отдельные символы в виде HEX-кода в формате `\x<HEX-код>`. Например, слово Überlingen можно записать как `"\xdcberlingen"`. Если строка состоит только из HEX-кода, ее можно записать в формате `h"<HEX-код>"`. Например, строку `"\xa1\xb2\xc3\xd4"` можно записать как `h"a1b2c3d4"`. Для экранирования кавычек (`"`) и HEX-кода нужно добавить перед ними символ обратной косой черты (`\`). Для сравнения строк без учета регистра в конец значения нужно добавить `/i`, например `"example.com"/i`	`"abcd"`, `h"a1b2c3d4"`, `"\xa1\xb2\xc3\xd4"`, `"Hex code \"\\xa1\""`
Array of strings	Массив строк. Для сравнения строк без учета регистра в конец значения нужно добавить `/i`, например `"example.com"/i`	—
DateTime	Дата и время в формате `гггг-ММ-дд чч:мм:сс`. Время может быть опущено. Время указывается в UTC	`"2022-07-15"`, `"2018-10-04 10:53:19"`
UUID	Универсально уникальный идентификатор	`"aabb4567-e89b-12d3-a456-426655440000"`, `"6cb71c2c-"`
MD5	Хеш-сумма файла, вычисленная по алгоритму MD5	`"8c13d614aa018ed5bc6c78b545ece530"`
FtpCmdCode	Строка с кодом FTP-команды. Список допустимых кодов можно посмотреть в стандарте RFC 959	`"USER"`, `"PASS"`, `"RETR"`

См. также

Поля протоколов, доступные в правилах ptrule (см. раздел Ж.3.4)

Ж.3.4. Поля протоколов, доступные в правилах ptrule

Все поля, упоминаемые в одном правиле ptrule, должны принадлежать к одной транзакции. В таблице ниже перечислены поля в транзакциях протоколов, которые могут использоваться в правилах ptrule. Тип данных (см. раздел Ж.3.3) влияет на то, какой оператор может использоваться при сопоставлении значений поля.

Таблица 18. Поля протоколов, доступные в ptrule

Поле	Тип данных
dcerpc.rqs.data	String
dcerpc.rqs.msg_type	UInt
dcerpc.rqs.opnum	UInt
dcerpc.rqs.uuid	UUID
dcerpc.rsp.data	String
dcerpc.rsp.msg_type	UInt
dcerpc.version	UInt
ftp.rqs.args	Array of strings
ftp.rqs.code	FtpCmdCode
ftp.rsp.answers	Array of strings
ftp.rsp.code	UInt
ftp.rsp.sub_resp	Boolean
pop3.rqs.cmd.args	String
pop3.rqs.cmd.name	String
pop3.rsp.args	String
pop3.rsp.data	Array of strings
pop3.rsp.status	String
quic.server_name	String
smb.v1.command	UInt
smb.v1.error_class	UInt
smb.v1.error_code	UInt
smb.v1.status	UInt
smb.v2.command	UInt
smb.v2.status	UInt
tls.client_cert.fingerprint	String

Поле	Тип данных
tls.client_cert.issuer.c	String
tls.client_cert.issuer.cn	String
tls.client_cert.issuer.l	String
tls.client_cert.issuer.o	String
tls.client_cert.issuer.ou	String
tls.client_cert.issuer.st	String
tls.client_cert.self_signed	Boolean
tls.client_cert.serial	String
tls.client_cert.subject.c	String
tls.client_cert.subject.cn	String
tls.client_cert.subject.l	String
tls.client_cert.subject.o	String
tls.client_cert.subject.ou	String
tls.client_cert.subject.st	String
tls.client_cert.valid	Boolean
tls.client_cert.valid.not_after	DateTime
tls.client_cert.valid.not_before	DateTime
tls.client_next_protocol	Array of strings
tls.client_ver	String
tls.ja3_md5	MD5
tls.ja3_string	String
tls.next_protocol	Array of strings
tls.server_cert.fingerprint	String
tls.server_cert.issuer	String
tls.server_cert.issuer.c	String
tls.server_cert.issuer.cn	String
tls.server_cert.issuer.l	String
tls.server_cert.issuer.o	String
tls.server_cert.issuer.ou	String
tls.server_cert.issuer.st	String
tls.server_cert.self_signed	Boolean

Поле	Тип данных
tls.server_cert.serial	String
tls.server_cert.subject	String
tls.server_cert.subject.c	String
tls.server_cert.subject.cn	String
tls.server_cert.subject.l	String
tls.server_cert.subject.o	String
tls.server_cert.subject.ou	String
tls.server_cert.subject.st	String
tls.server_cert.valid	Boolean
tls.server_cert.valid.not_after	DateTime
tls.server_cert.valid.not_before	DateTime
tls.server_name	Array of strings
tls.tls_resumed	Boolean
tls.version	String

Глоссарий

PT NAD Sensor

Упрощенная версия PT NAD, которая используется для интеграции с MaxPatrol 10. Позволяет снизить требования к аппаратным ресурсам за счет отключения или ограничения функций, не имеющих значения для работы в MaxPatrol 10.

актив

Информация, ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие), процессы, выпускаемая продукция, услуги или оборудование, имеющие ценность для организации и подлежащие защите от киберугроз.

атака

То же, что и кибератака.

вредоносное программное обеспечение

Программное обеспечение, которое разрабатывается для получения несанкционированного доступа к вычислительным ресурсам и данным, а также для нанесения ущерба путем копирования, искажения, удаления или подмены данных.

выделенное хранилище

Хранилище, выделенное оператором для удобства работы с определенным трафиком (например, связанным с инцидентом ИБ или поступившим от конкретного сервера за определенный период) или для долгосрочного хранения трафика.

инвентаризация IT-активов

Сбор сведений об IT-активах для получения представления об IT-инфраструктуре организации.

инцидент ИБ

Событие (группа событий) информационной безопасности, которое может привести к нарушению функционирования IT-инфраструктуры или возникновению угроз безопасности обрабатываемой в ней информации.

исходная копия трафика

Сетевые данные, которые были захвачены модулем ptdpi и сохранены в хранилище файлов PCAP. Исходную копию трафика можно экспортировать в формате PCAP для ретроспективного анализа в PT NAD и импорта во внешние программы.

кибератака

Целенаправленное воздействие программных и (или) программно-аппаратных средств на IT-инфраструктуру и ее компоненты с целью нарушения (прекращения) ее функционирования или создания угрозы безопасности обрабатываемой в ней информации. Целями кибератаки могут быть, например, несанкционированный перевод денежных средств, нарушение или блокировка работы системы, получение несанкционированного доступа к инфраструктуре или хищение персональных данных.

метаданные трафика

Сведения о сессии — о задействованных в ней протоколах и приложениях, доменных именах, переданных файлах, обнаруженных индикаторах компрометации, о геолокации отправителя и получателя, объеме переданных и полученных данных. Продукт получает метаданные трафика в два этапа: при разборе захваченного трафика и при обогащении уже разобранного трафика. Метаданные можно экспортировать в форматах JSON и CSV для ретроспективного анализа в других продуктах или самостоятельного изучения.

модуль ptdpi

Часть подсистемы захвата, которая отвечает за захват и анализ сетевого трафика, а также выявление атак на основе правил и репутационных списков.

потоковое хранилище

Тип хранилища, которое создается при развертывании продукта и в которое поступает поток трафика с сенсора. Каждый сенсор записывает исходную копию трафика и метаданные трафика в свое потоковое хранилище. Трафик в потоковом хранилище ротируется согласно конфигурации продукта.

репутационный список

Список IP-адресов, доменов, URL или файлов, использование или передача которых в ходе сетевого взаимодействия между двумя узлами свидетельствует о конкретной угрозе ИБ или иным образом маркирует это сетевое взаимодействие.

ретроспективный анализ

Анализ данных с учетом изменения во времени, начиная от текущего момента времени к какому-либо прошедшему, для выявления закономерностей и построения гипотез.

сессия

Сеанс обмена сетевыми пакетами между двумя узлами — клиентом и сервером.

событие ИБ

Любое зафиксированное явление в системе или сети (например, подключение пользователя к файловому серверу, обработка веб-запроса сервером, отправка email-сообщения, блокирование объекта межсетевым экраном сетевого соединения).

угроза ИБ

Возможность нарушения информационной безопасности, в результате которого может быть нанесен ущерб организации или пользователю.

узел

Любое устройство в сети TCP/IP, которое отправляет и получает данные и имеет свой IP-адрес.

фильтр захвата трафика

Условие или набор условий на языке фильтрации Berkeley Packet Filter (BPF), по которым сенсор выбирает трафик для обработки.

хранилище

Логическая область для хранения исходной копии трафика и метаданных трафика. Предусмотрены потоковые и выделенные хранилища.