Network Attack Discovery версия 12.0

Руководство администратора

Дата редакции документа: 13.03.2024

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию Positive Technologies Network Attack Discovery (далее также — PT NAD). Руководство не содержит инструкций по установке PT NAD и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим PT NAD.

Руководство предполагает наличие у читателя базовых знаний о сетевых технологиях, Unix-подобных операционных системах и синтаксисе YAML.

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 оператора — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.
- 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 кнопку **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 12).

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) 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.
- **Визуализация данных.** Отображение статистики сетевых взаимодействий в виде отчетов и графиков, а также наглядной карты сетевых взаимодействий.

PT NAD предоставляет следующие возможности:

- **Обнаружение угроз.** 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.** Встроенный несигнатурный метод обнаружения нелегитимных сканирований, флуда и DDoS-атак защищает PT NAD от переполнения базы данных и повышает стабильность захвата трафика.
- **Поддержка открытого HTTP API.** Возможность разработки сторонних приложений для работы с проанализированным трафиком.
- **Отправка информации об угрозах в системы SIEM.** Передача сведений об обнаруженных угрозах в системы SIEM, в том числе в MaxPatrol SIEM, для инвентаризации активов и проверки результативности атак. Интеграция с MaxPatrol SIEM осуществляется с помощью его API и специального агента, с другими системами SIEM — по протоколу системного журнала (syslog) или с помощью механизма webhook.
- **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.

---

1 Хранение исходной копии трафика и файлов не предусмотрено в версии PT NAD Sensor (см. раздел 2.3).

— **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 в сетевой инфраструктуре организации. Помимо регулярного запуска ретроспективного анализа (см. раздел 10.7), PT NAD повторно разбирает скопированный трафик для ретроспективного 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 и о поступлении или непоступлении в информационную инфраструктуру организации определенного трафика. Уведомления могут быть получены на электронную почту или с помощью системного журнала (см. раздел 10.10), а также могут отображаться в интерфейсе PT NAD.

— **Обнаружение DGA-доменов.** Поиск DGA-доменов при анализе доменных имен отправителя и получателя, а также при разрешении имен с помощью DNS. Поиск работает как в реальном времени, так и при ретроспективном анализе.

В этом разделе

2.1. Разбор трафика

Одной из основных функций PT NAD является разбор исходной копии трафика организации. Разбор трафика позволяет получать детальную информацию о сетевых взаимодействиях и обнаруживать атаки в сессиях. 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 общем потоке трафика отдельные соединения и реконструирует сессии. Для распознавания отдельных соединений PT NAD использует IP-адреса, порты и протоколы из сетевых пакетов. В случае разбора туннелированного трафика и трафика в сетях VLAN для корректной реконструкции сессии PT NAD также использует соответственно информацию об адресах туннелей и теги VLAN.
2. Определяет, какие протоколы были задействованы в сессиях на уровнях модели OSI от канального до прикладного.

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 в сессиях при помощи правил.

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.

2.2. Архитектура и алгоритм работы PT NAD

PT NAD имеет модульную архитектуру. Она позволяет устанавливать продукт в распределенной сети и внедрять его в организациях любого размера.

Модули продукта объединяются в следующие подсистемы:

— сенсор (см. раздел 2.2.1);

— подсистема обогащения (см. раздел 2.2.2);

— подсистема хранения (см. раздел 2.2.3);

— подсистема пользовательского интерфейса (см. раздел 2.2.4);

— подсистема мониторинга (см. раздел 2.2.5).

Как подсистемы PT NAD работают с трафиком

Сетевой трафик организации — то, с чем работает PT NAD. В этом процессе задействованы все подсистемы, кроме мониторинга. Алгоритм работы PT NAD с трафиком изображен на диаграмме ниже. Стрелки показывают направления потоков информации.

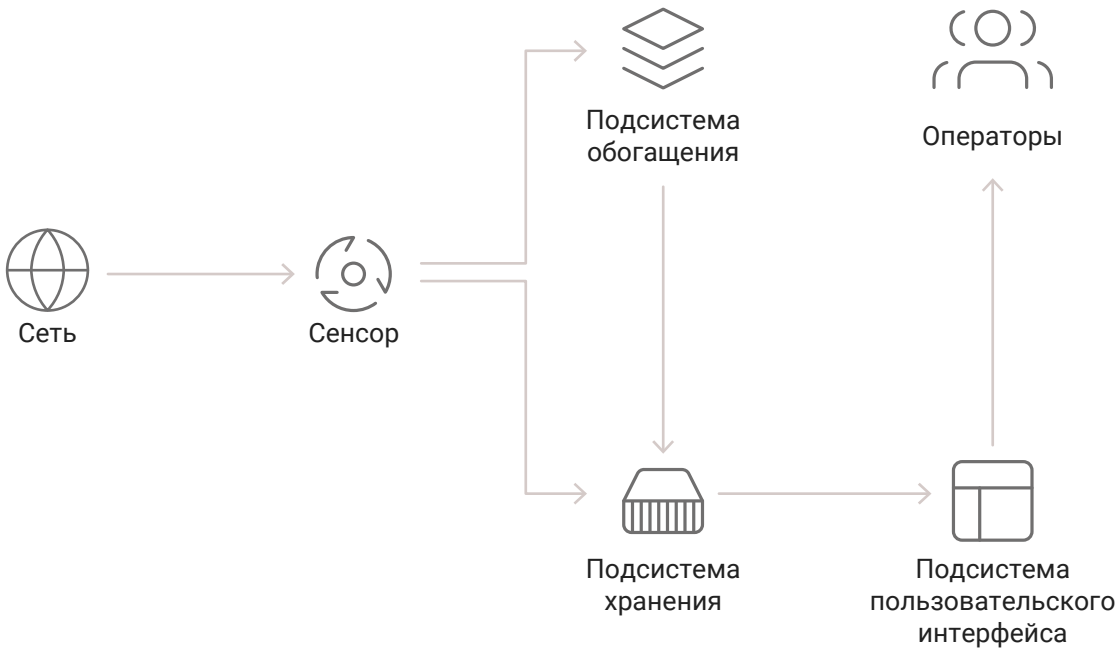

Рисунок 1. Работа PT NAD с трафиком

Работа с трафиком делится на следующие этапы:

1. Сенсоры захватывают копию сетевого трафика организации.
2. Сенсоры обрабатывают захваченную копию трафика: выполняют ее разбор (см. раздел 2.1) и одновременно с этим записывают ее в формате PCAP в подсистему хранения.
3. Сенсоры передают результаты разбора трафика, в том числе информацию об обнаруженных атаках, в виде метаданных в подсистему обогащения.
4. Подсистема обогащения дополняет метаданные трафика сессий информацией о доменных именах и странах отправителей и получателей запросов, а также индикаторами 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, 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.
5. Подсистема обогащения анализирует метаданные трафика сессий для поиска событий информационной безопасности.

6. Подсистема обогащения передает метаданные трафика, включая результаты обогащения, в подсистему хранения, а информацию об обнаруженных событиях ИБ — как в подсистему хранения, так и в базу данных подсистемы пользовательского интерфейса.
7. Подсистема пользовательского интерфейса получает из подсистемы хранения метаданные трафика и исходную копию трафика в виде файлов PCAP.

   Метаданные трафика используются подсистемой пользовательского интерфейса:

   - для автоматического регулярного поиска опасных и потенциально опасных активностей в сети организации;
   - отображения данных о трафике в веб-интерфейсе (см. раздел 7);
   - сборки отчетов.

   PCAP-файлы могут запрашиваться (экспортироваться) из подсистемы пользовательского интерфейса операторами для ретроспективного анализа в PT NAD и импорта во внешние программы.

В этом разделе

2.2.1. Сенсор

Сенсор — подсистема продукта, которая захватывает копию трафика и обрабатывает ее: фильтрует и анализирует сетевые пакеты, разбирает протоколы, извлекает файлы и приводит данные к единому формату для создания записей о сессиях.

Сенсор состоит из модулей ptdpi и nad-task-server.

Модуль ptdpi

Модуль ptdpi выполняет основные функции сенсора:

— получение копии трафика:

- ее захват с сетевого интерфейса, указанного при установке PT NAD и включенного на узле с модулем ptdpi;
- извлечение из PCAP-файлов, импортированных в PT NAD операторами;

— сохранение полученной копии трафика в формате PCAP в подсистему хранения;

— разбор трафика (см. раздел 2.1);

— выявление атак на основе правил;

— передача результатов разбора трафика в формате JSON модулю ptdpi-broker (см. раздел 2.2.2).

Модуль nad-task-server

Модуль nad-task-server — служба, которая выполняет команды управления модулем ptdpi (см. раздел 2.2.1). Команды отправляются из подсистемы пользовательского интерфейса операторами или регулярными автоматическими заданиями. Модуль nad-task-server выполняет следующие команды:

— импортировать трафик;

— экспортировать трафик;

— извлечь файлы, которые передавались в сессиях;

— включить или выключить захват трафика;

— изменить фильтр захвата трафика;

— синхронизировать базу знаний, которая включает в себя правила для обнаружения атак, правила для обнаружения активностей, репутационные списки, базы геолокации, а также списки доверенных доменов, используемых при обнаружении DGA-доменов.

2.2.2. Подсистема обогащения

Подсистема обогащения дополняет метаданные трафика сессий информацией, которая используется в дальнейшем как продуктом для поиска угроз ИБ, так и операторами для самостоятельного анализа инцидентов. Кроме того, подсистема обогащения ищет опасные и потенциально опасные активности, а также индикаторы компрометации.

Подсистема состоит из одного модуля ptdpi-broker и нескольких ptdpi-worker.

Модуль ptdpi-broker

Модуль ptdpi-broker маршрутизирует информацию между сенсором и модулями ptdpi-worker:

— принимает от модуля ptdpi (см. раздел 2.2.1) информацию о результатах анализа трафика в формате JSON;

— рассылает эту информацию модулям ptdpi-worker;

— получает от модулей ptdpi-worker результаты обогащения;

— передает данные между модулями подсистемы мониторинга (см. раздел 2.2.5).

Модули ptdpi-worker

Модули ptdpi-worker обогащают метаданные трафика. В общем случае они принимают от модуля ptdpi-broker информацию о результатах анализа трафика, обогащают ее и возвращают модулю ptdpi-broker. Каждый модуль ptdpi-worker работает с информацией определенного типа. Такое распределение позволяет регулировать нагрузку на них.

По типу обрабатываемой информации модули ptdpi-worker делятся на несколько типов.

Таблица 2. Модули ptdpi-worker

Модуль	Что получает от ptdpi-broker	Куда отправляет результат
ptdpi-worker@ad		
Ищет аномальное поведение в информационной инфраструктуре организации	Данные о сетевых соединениях	Информацию об обнаруженных активностях — модулю nad-web-server (для записи в базу данных), об атаках — модулю ptdpi-broker
ptdpi-worker@alert		
Удаляет дубликаты атак и записи об атаках, подпадающие под условия исключений из правил	Список атак	Модулю ptdpi-broker
ptdpi-worker@dns		
Выполняет следующие функции: — на основании DNS-трафика, разобранного сенсором, составляет внутренний DNS-кэш; — используя внутренний DNS-кэш, определяет по IP-адресам отправителя и получателя сессии их доменные имена; — определяет географическое положение узлов отправителя и получателя сессии, используя их IP-адреса и базу данных геолокации GeoIP;	Данные о сетевых соединениях	Модулю ptdpi-broker

Модуль	Что получает от ptdpi-broker	Куда отправляет результат
— сверяет с репутационными списками IP-адреса, доменные имена, URL и файлы, которые использовались или передавались в сессии; — обнаруживает DGA-домены среди доменных имен отправителя и получателя сессии, а также при разрешении имен с помощью DNS		
ptdpi-worker@es		
Записывает все результаты обогащения в подсистему хранения	Всю обогащенную информацию	Модулю Elasticsearch (см. раздел 2.2.3)
ptdpi-worker@hosts		
Работает с информацией об узлах[2], которые участвуют в сетевых взаимодействиях: — идентифицирует их; — помечает сессии идентификаторами узлов, которые в них участвовали; — накапливает данные о каждом узле (в частности используемые им протоколы, операционные системы, логины и баннеры); — при динамической адресации узлов анализирует сообщения DHCP-протокола и определяет, когда узел меняет IP-адрес	Данные о сетевых соединениях	Информацию об узлах — модулю nad-web-server (для записи в базу данных), об идентификаторах узлов в сессиях — модулю ptdpi-broker

2 Для включения узла в статистику его IP-адрес должен входить в группу HOME_NET.

Модуль	Что получает от ptdpi-broker	Куда отправляет результат
ptdpi-worker@icap		
Получает информацию об опасности файлов, которые передаются в сессиях. Для этого модуль отправляет файлы на проверку во внешнюю аналитическую систему и получает от нее результаты этой проверки — тип обнаруженного вредоносного ПО и признак опасного поведения, выявленного в ходе поведенческого анализа. Для связи с внешней аналитической системой используется протокол ICAP. Модуль выступает в роли ICAP-клиента, который подключается к ICAP-серверу внешней аналитической системы	Информацию о местоположении файлов, которые сенсор извлекает из сессий и записывает на диск	Модулю ptdpi-broker
ptdpi-worker@mpx (в случае интеграции с MaxPatrol SIEM)		
Получает от MaxPatrol SIEM идентификаторы и группы активов, в которые входят узлы сетевого взаимодействия. Соотносит сработавшие правила с известными уязвимостями на узлах (прогноз результативности атаки)	Данные о сетевых соединениях, данные об атаках	Модулю ptdpi-broker
ptdpi-worker@notifier		
Рассылает в сторонние системы и продукты информацию об обнаруженных угрозах ИБ	Данные об атаках, активностях, индикаторах компрометации	В стороннюю систему следующими способами: — по протоколу syslog; — с помощью механизма webhook; — с помощью API-запросов (в текущей версии продукта отправляется информация

Модуль	Что получает от ptdpi-broker	Куда отправляет результат
		только об активностях и поддерживаются запросы только MaxPatrol SIEM)

2.2.3. Подсистема хранения

Подсистема хранения — место хранения исходной копии трафика и его метаданных. Состоит из хранилища файлов PCAP и модуля Elasticsearch.

Хранилище файлов PCAP

Хранилище файлов PCAP — каталог в файловой системе, в который модуль ptdpi записывает исходную копию трафика в формате PCAP.

Чтобы избежать переполнения дискового пространства, файлы в хранилище файлов PCAP ротируются, когда их объем начинает занимать 90% от доступного дискового пространства. Этот процент может быть изменен администратором PT NAD.

Модуль Elasticsearch

Модуль Elasticsearch — поисковая система, в базу данных которой модуль ptdpi-worker@es записывает метаданные трафика в формате JSON. Благодаря своей многопоточности и масштабируемости позволяет быстро находить и фильтровать информацию в больших массивах метаданных.

Чтобы избежать переполнения дискового пространства, метаданные трафика хранятся две недели независимо от доступного объема свободного места. Период хранения настраивается в ходе установки PT NAD и в будущем может быть изменен администратором

При установке PT NAD устанавливается Elasticsearch версии 5.6.

В модуле Elasticsearch есть механизм для балансировки нагрузки. Балансировку выполняют процессы, которые называются узлами (nodes). Они могут выполнять следующие роли:

- **Главный узел (master node).** Контролирует запуск и работу остальных узлов Elasticsearch.
- **Клиентский узел (client node).** Обрабатывает запросы к модулю Elasticsearch:
  - на запись — от модуля ptdpi-worker@es;
  - на чтение — от модулей nad-web-server, nad-task-server и ptdpistat.
- **Узел данных (data node).** Работает непосредственно с данными: записывает, индексирует, сохраняет, выполняет чтение, поиск и агрегацию.

Набор узлов Elasticsearch, имеющих между собой сетевую связь, называется кластером Elasticsearch. В кластере должно работать минимум по одному узлу каждой роли. Количество узлов данных зависит от интенсивности трафика и доступного объема оперативной памяти. Формула для расчета количества узлов данных приведена в аппаратных требованиях. Кластер также может состоять всего из одного узла. В таком случае этот узел выполняет все три роли.

Подробная информация об Elasticsearch приведена на сайте его разработчика.

См. также

Изменение ротации данных в потоковых хранилищах (см. раздел 10.9)

2.2.4. Подсистема пользовательского интерфейса

Подсистема пользовательского интерфейса состоит из следующих компонентов:

— **Веб-приложение.** Предоставляет пользовательский веб-интерфейс.

— **База данных под управлением PostgreSQL.** Хранит правила и репутационные списки, журнал аудита, фильтры захвата трафика, пользовательские данные (параметры фильтров, отчетов, уведомлений, таблиц, дашбордов и виджетов), данные об узлах, хранилищах, а также информацию об обнаруженных событиях ИБ.

— **Модуль nad-web-server.** Обеспечивает взаимодействие веб-интерфейса с остальными модулями и предоставляет API:

- для поиска по сетевым взаимодействиям и обнаруженным атакам и их анализа;
- управления репутационными списками и списками правил;
- управления подключенными сенсорами;
- импорта, экспорта трафика и извлечения файлов;
- управления учетными записями пользователей.

Модуль nad-web-server, наряду с модулем ptdpi-worker@ad подсистемы обогащения, также отвечает за поиск опасных и потенциально опасных активностей в сети организации.

— **Redis.** Хранит кэш, выполняет роль агента обмена внутренними сообщениями между модулями nad-task-server и nad-web-server.

— **Модуль nad-reporter.** Отвечает за генерацию отчетов о сетевых взаимодействиях в форматах DOCX и PDF.

2.2.5. Подсистема мониторинга

Подсистема мониторинга — набор служб, которые собирают информацию о том, как работают компоненты PT NAD, и предоставляют интерфейс для просмотра этой информации и для контроля за состоянием работы продукта в режиме реального времени.

Подсистема состоит из модулей ptdpistat и ptdpistat-server. Модули ptdpistat собирают данные мониторинга и передают их модулю ptdpistat-server. Модуль ptdpistat-server предоставляет веб-интерфейс Grafana, в котором администраторы могут просматривать графики мониторинга. За хранение данных отвечает компонент Graphite в составе модуля ptdpistat-server.

> **Примечание.** При необходимости администратор PT NAD может настроить отправку данных мониторинга во внешнюю систему. В качестве такой системы может выступать Zabbix и (или) Graphite. При подключении внешнего Graphite модуль ptdpistat-server становится недоступным.

На диаграмме ниже показано, как подсистема мониторинга взаимодействует с другими компонентами продукта (подсвеченные блоки обозначают компоненты подсистемы мониторинга).

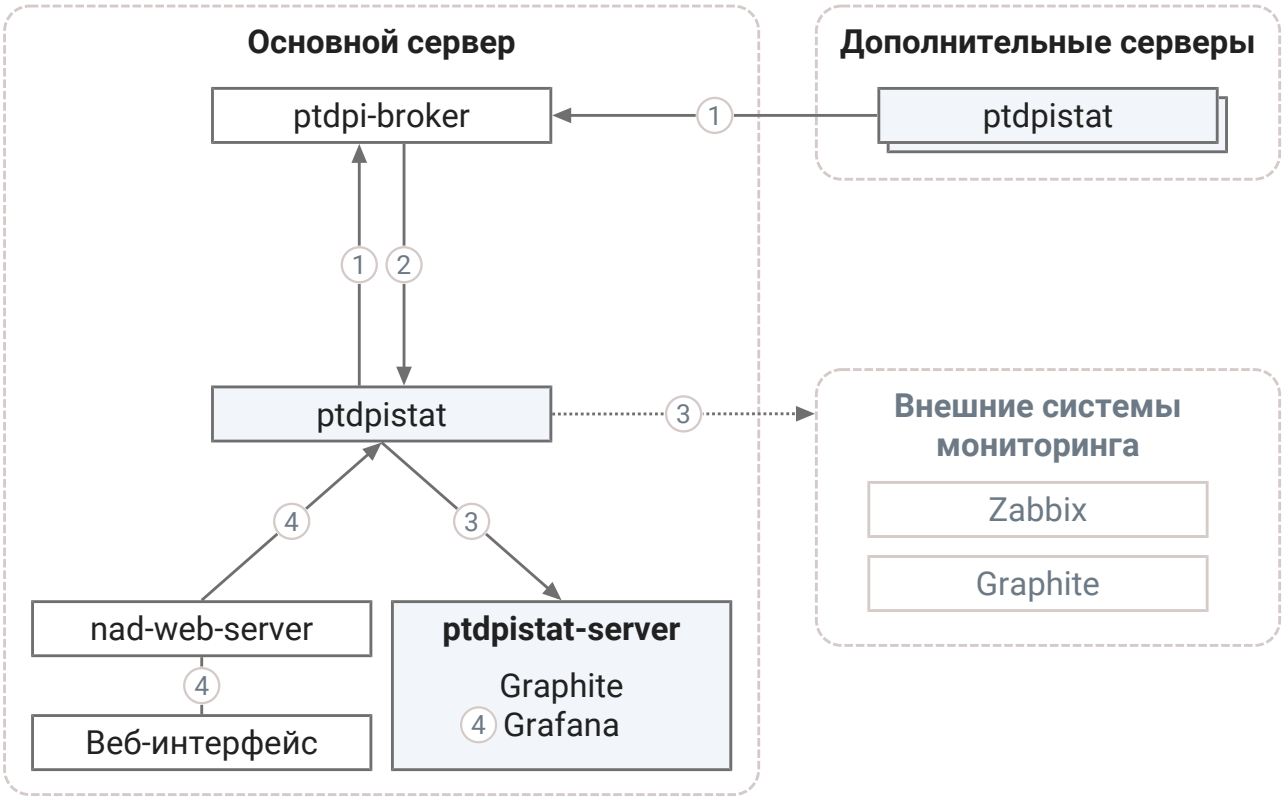

Рисунок 2. Взаимодействие подсистемы мониторинга с другими модулями PT NAD

Работа подсистемы мониторинга делится на следующие этапы:

1. Модуль ptdpistat собирает информацию о работе компонентов PT NAD на том сервере, на котором он запущен. Модуль также следит за состоянием операционной системы, в которой он работает. Собранную информацию модуль ptdpistat передает модулю ptdpi-broker.
2. Модуль ptdpi-broker перенаправляет собранную информацию основному модулю ptdpistat (в многосерверной конфигурации — тому, который работает на основном сервере).
3. Основной модуль ptdpistat передает статистику, собранную им и модулями ptdpistat на дополнительных серверах:
   - модулю ptdpistat-server;
   - в системы внешнего мониторинга Zabbix и (или) Graphite (если интеграция с этими системами была настроена).
4. Подсистема мониторинга показывает данные мониторинга пользователю:
   - В главном меню интерфейса PT NAD (состояние работы продукта и ошибки в работе конкретных модулей).

Для отображения данных мониторинга в интерфейсе PT NAD модуль nad-web-server обращается к основному модулю ptdpistat.

- В интерфейсе Grafana модуля ptdpistat-server.

2.2.6. Безопасность хранения и передачи данных

При работе с интерфейсом все передаваемые данные защищаются при помощи HTTPS с использованием SSL-сертификата Positive Technologies. Запросы, адресованные порту 80 (HTTP), автоматически перенаправляются на порт 443 (HTTPS).

Примечание. Вы можете заменить стандартный SSL-сертификат самоподписанным или выданным официальным центром сертификации (см. раздел 5.7.1).

Безопасность хранения данных обеспечивается с помощью проверки целостности продукта (см. раздел 5.8).

Для предотвращения несанкционированного доступа к продукту PT NAD уведомляет администратора о неуспешных попытках входа (см. раздел 10.5).

2.3. PT NAD Sensor

Для интеграции с MaxPatrol SIEM 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 SIEM:

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

— полученные в ходе обработки трафика метаданные трафика хранятся не больше одного дня;

— скорость захвата трафика ограничена 1 Гбит/с.

3. Что нового в версии 12.0

Ниже приводится список новых возможностей и улучшений, которые появились в PT NAD версии 12.0.

Настройка PT NAD в интерфейсе

Начиная с версии 12.0 настройка PT NAD выполняется в интерфейсе, а не в конфигурационных файлах. Для этого в центр управления добавлены вкладки **Общие параметры**, **Обновление баз знаний**, **Интеграция с продуктами Positive Technologies** и **Средства интеграции**.

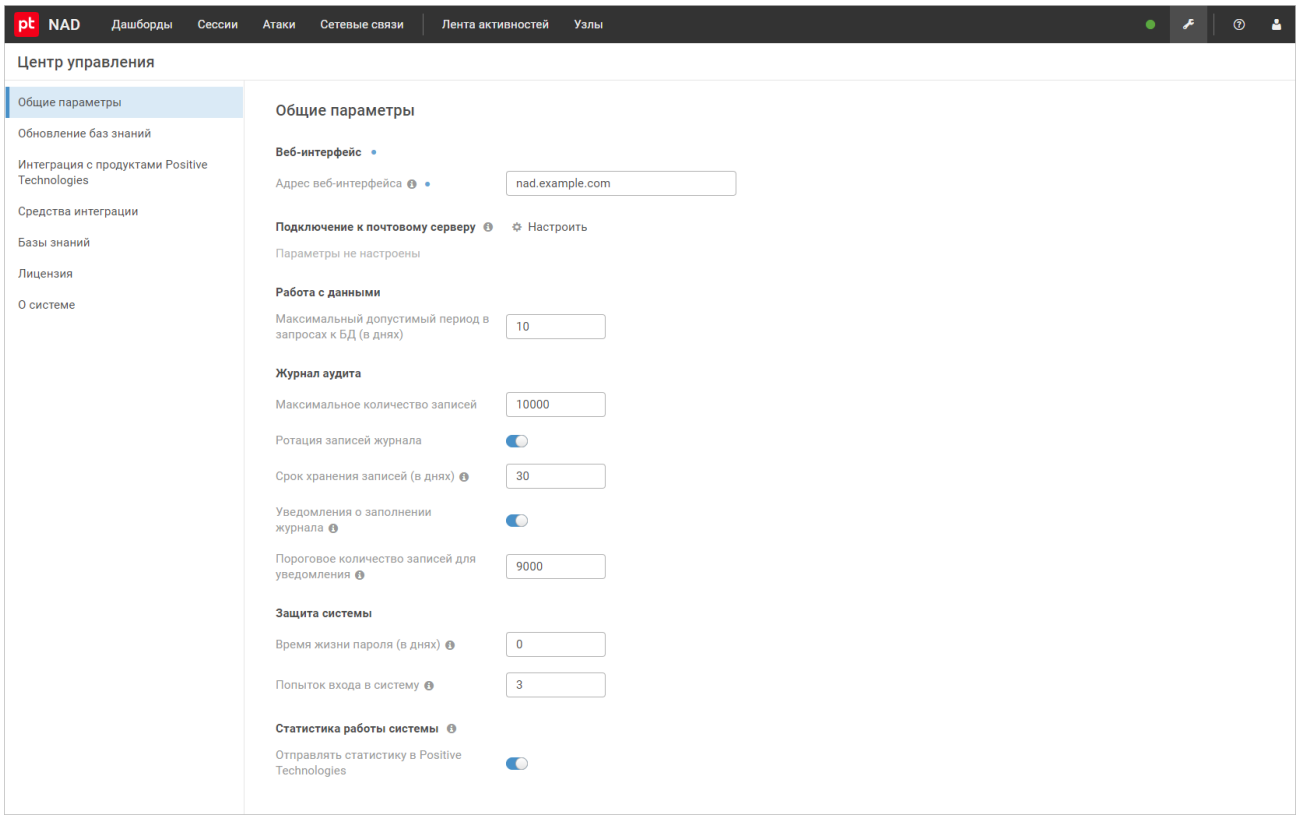

Рисунок 3. Настройка PT NAD в интерфейсе

Чтобы начать использовать новую возможность, после установки PT NAD версии 12.0 или обновления до этой версии вам нужно перенести параметры продукта из конфигурационных файлов в базу данных (см. раздел 5.3).

Журналирование IP-адресов пользователей

Теперь администраторы могут просматривать IP-адреса, с которых пользователи заходят в PT NAD. Для этого в таблицу **Пользователи** добавлен столбец **Последний IP-адрес** (см. рисунок ниже). Такая информация позволяет своевременно обнаруживать несанкционированный доступ к продукту.

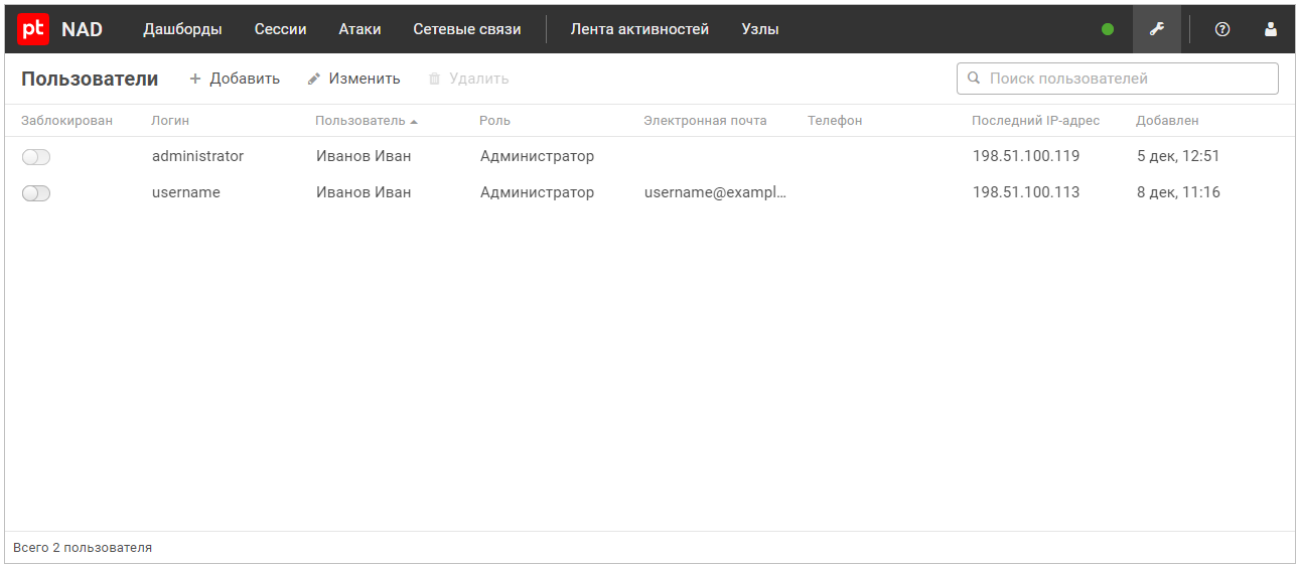

Рисунок 4. Пользователи и последние IP-адреса, с которых они заходили в продукт

Кроме того, администраторы могут отслеживать IP-адреса, с которых осуществлялись успешные и неуспешные попытки аутентификации. Для этого в столбец **Детали** в журнале аудита (см. раздел 10.4) для записей с действием **login** PT NAD теперь записывает IP-адреса. Во всплывающей подсказке, которая открывается по нажатию на логин в столбце **Пользователь**, отображается последний IP-адрес пользователя.

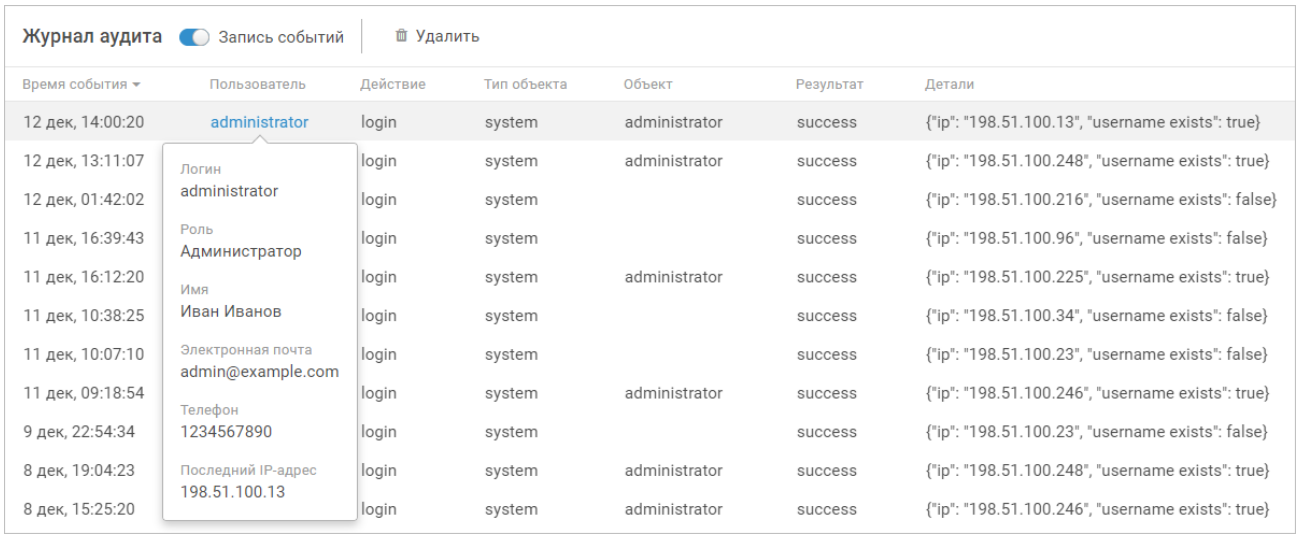

Рисунок 5. Просмотр IP-адресов пользователей в журнале аудита

4. Лицензирование

Для работы PT NAD, его защиты от нелегального использования и получения обновлений из базы знаний экспертного центра Positive Technologies нужна лицензия.

При заказе лицензии устанавливается срок ее действия. По истечении этого срока PT NAD перестает получать обновления из базы знаний экспертного центра Positive Technologies.

Одна лицензия может быть активирована только в одном экземпляре PT NAD. В одном экземпляре PT NAD одновременно может действовать только одна лицензия.

См. также

Активация лицензии (см. раздел 5.2)

Просмотр информации о лицензии PT NAD (см. раздел 8)

Замена лицензии PT NAD (см. раздел 9)

5. Первоначальная настройка PT NAD

После установки или обновления PT NAD вам нужно выполнить его первоначальную настройку.

В этом разделе

5.1. Настройка аутентификации

После установки или обновления PT NAD вам нужно настроить аутентификацию пользователей в продукте.

В этом разделе

5.1.1. Смена стандартного пароля администратора

В целях безопасности сразу после установки PT NAD вам нужно сменить стандартный пароль для учетной записи администратора.

- Чтобы сменить стандартный пароль администратора:

  1. В адресной строке браузера введите IP-адрес или доменное имя узла с установленным веб-сервером nginx.

Откроется страница входа в PT NAD.

2. В поле **Логин** введите `administrator`.
3. В поле **Пароль** введите `Administr@t0r`.
4. Нажмите кнопку **Войти**.

   Откроется страница **Дашборды**.

5. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Смена пароля**.

   Откроется страница **Смена пароля**.

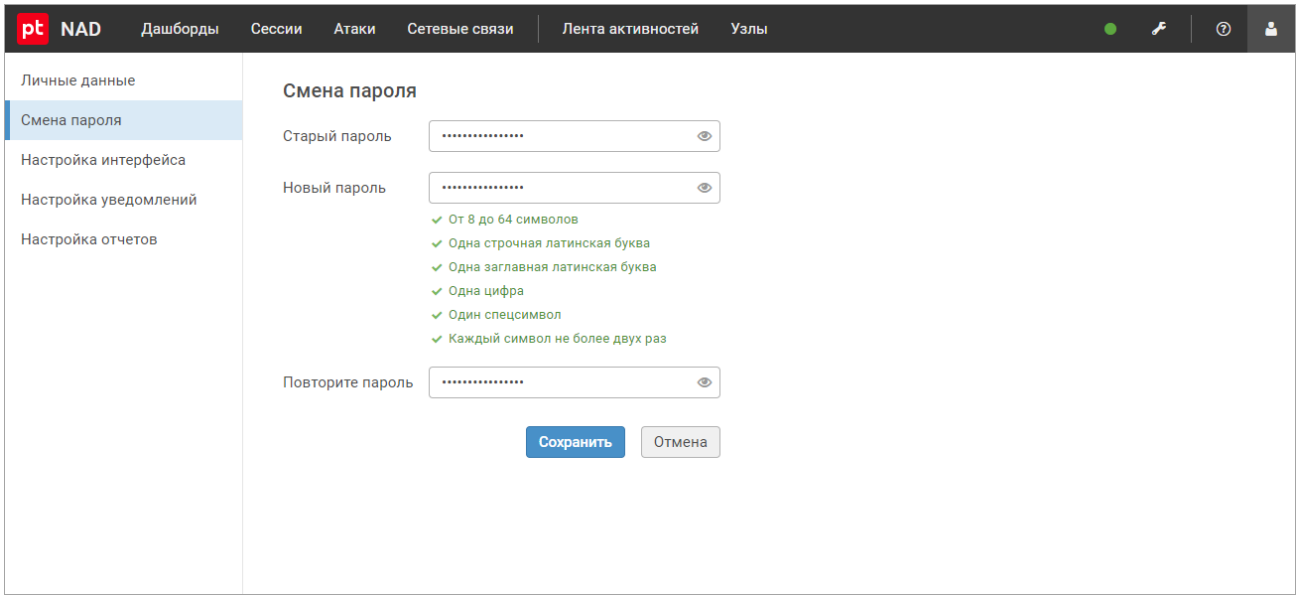

Рисунок 6. Смена стандартного пароля администратора

6. В поле **Старый пароль** введите `Administr@t0r`.
7. Дважды введите новый пароль.

   Примечание. Пароль должен быть не короче 8 символов и содержать как минимум одну строчную и одну прописную латинскую букву, одну цифру и один спецсимвол. Каждый символ не должен повторяться более двух раз.

8. Нажмите кнопку **Сохранить**.

Стандартный пароль администратора изменен.

5.1.2. Настройка срока действия паролей учетных записей

По умолчанию пароли пользовательских учетных записей в PT NAD действуют бессрочно. Вы можете установить срок действия паролей согласно политике устаревания паролей вашей организации.

Примечание. Описанная в этом разделе функция недоступна, если в процессе установки PT NAD была настроена аутентификация с помощью сервиса единого входа PT MC.

- Чтобы настроить срок действия паролей:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. В блоке параметров **Защита системы** в поле **Время жизни пароля (в днях)** укажите срок действия пароля.

     Примечание. Для возврата бессрочного действия паролей нужно ввести 0.

  3. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

  Срок действия паролей настроен.

При попытке войти в PT NAD с устаревшим паролем пользователь не сможет продолжить работу с продуктом, пока не сменит пароль на новый. PT NAD также отправит уведомление об истекшем сроке действия пароля на адрес электронной почты, указанный в личном кабинете пользователя. Пользователи могут узнать, сколько дней осталось до смены их паролей, в личном кабинете на вкладке **Смена пароля**.

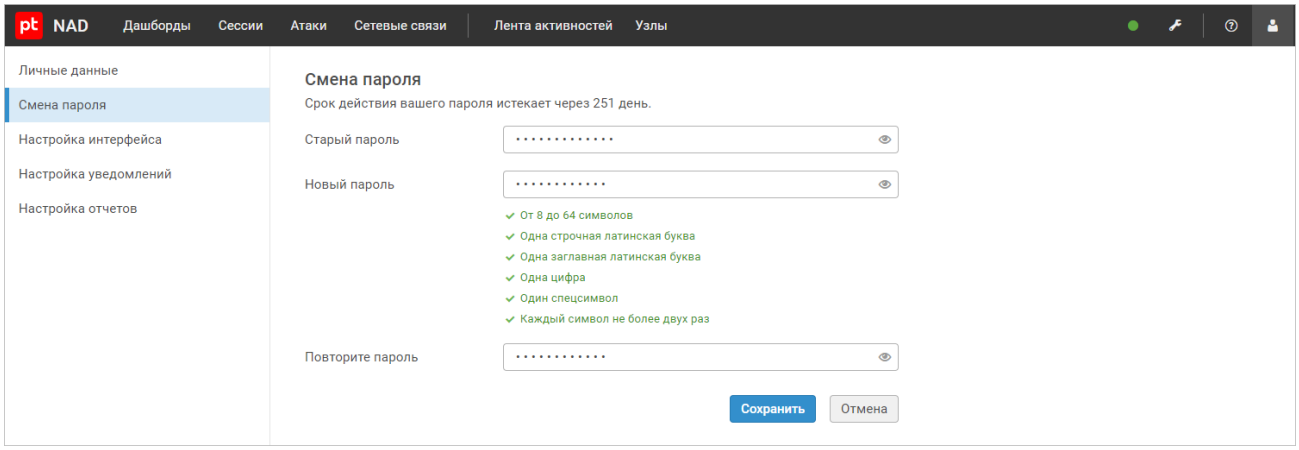

Рисунок 7. Просмотр информации о сроке действия пароля

5.1.3. Настройка аутентификации через PT MC

Если в вашей организации установлен MaxPatrol SIEM версии 21 или выше, вы можете настроить аутентификацию пользователей PT NAD с помощью компонента PT Management and Configuration (PT MC), который обеспечивает единый вход для всех продуктов Positive Technologies.

Примечание. Подробная информация о PT MC представлена по адресу help.ptsecurity.com/projects/mc/latest/ru-RU/help.

Учетные записи пользователей, созданные в PT NAD, не переносятся в PT MC автоматически. Но после настройки аутентификации через PT MC вы можете создать учетные записи в PT MC с теми же логинами и набором прав, что и в PT NAD. В этом случае владельцы учетных записей сохранят свои пользовательские параметры (правила уведомлений, параметры отчетов, сохраненные фильтры и дашборды).

Перед выполнением инструкции нужно указать адрес веб-интерфейса (см. раздел 5.4) и включить доверие сертификата организации (см. раздел 5.10), которым подписан сертификат сервера PT MC.

Примечание. Если вы настраивали интеграцию с PT MC по устаревшей инструкции (с помощью команд консоли) уже после обновления PT NAD до версии 12.0, вам нужно перенести параметры интеграции из конфигурационных файлов в базу данных с помощью команды `sudo /opt/ptsecurity/nad/bin/manage settings migrate --iam-cookie /opt/ptsecurity/etc/iam_cookie.json`, после чего выполнить команду `sudo /opt/ptsecurity/nad/bin/manage settings sync`. В противном случае интеграция работать не будет.

- Чтобы настроить аутентификацию пользователей PT NAD с помощью PT MC:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. Выберите вкладку **Интеграция с продуктами Positive Technologies**.
3. В блоке параметров **Интеграция с PT MC** по кнопке **Настроить** откройте окно **Настройка интеграции с PT MC**.
4. В поле **Адрес сервера PT MC** укажите IP-адрес или доменное имя сервера PT MC, например `ptmc.example.com`.
5. В поле **Идентификатор экземпляра PT NAD** укажите идентификатор экземпляра PT NAD.

   Внимание! При регистрации нескольких экземпляров PT NAD в одном экземпляре PT MC идентификаторы должны быть уникальными.

   Примечание. Допустимые символы в идентификаторе — буквы латинского алфавита в нижнем регистре, цифры, точка, знак подчеркивания и дефис.

6. Если в PT MC регистрируется несколько экземпляров PT NAD, в поле **Название экземпляра PT NAD** смените название экземпляра, чтобы оно было уникальным.
7. Если вам не нужно, чтобы PT NAD проверял сертификат PT MC, отключите проверку сертификата.

8. Нажмите кнопку **Сохранить**.
9. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Аутентификация пользователей PT NAD с помощью PT MC настроена. Чтобы начать использовать возможности интеграции с PT MC, пользователям понадобится перезайти под своей учетной записью с помощью этого сервиса.

Теперь вы можете использовать роли и привилегии PT NAD при настройке аутентификации в PT MC. Например, вы можете назначать роли PT NAD учетным записям, которые уже были созданы в PT MC для аутентификации пользователей в MaxPatrol SIEM.

5.2. Активация лицензии

После установки PT NAD нужно активировать лицензию, приобретенную вашей организацией. Для этого нужно загрузить файл лицензии `license-access-token.key` в продукт. Вы можете найти этот файл на установочном диске из комплекта поставки или в электронном письме, поступившем на адрес, указанный при заказе лицензии.

Для проверки лицензии PT NAD обращается к серверу update.ptsecurity.com. Если в вашей организации используется ПО, ограничивающее сетевой доступ, перед активацией лицензии нужно убедиться, что с узлов с установленным модулем nad-task-server разрешен доступ по HTTPS к update.ptsecurity.com. Это можно сделать, например, при помощи команды `wget -Sq -O /dev/null https://update.ptsecurity.com/test`. Если доступ есть, результат выполнения этой команды начинается со строки `HTTP/1.1 200 OK`.

► Чтобы активировать лицензию:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**.
2. Выберите вкладку **Лицензия**.
3. Нажмите кнопку **Добавить**.

   Откроется окно **Добавление лицензии**.

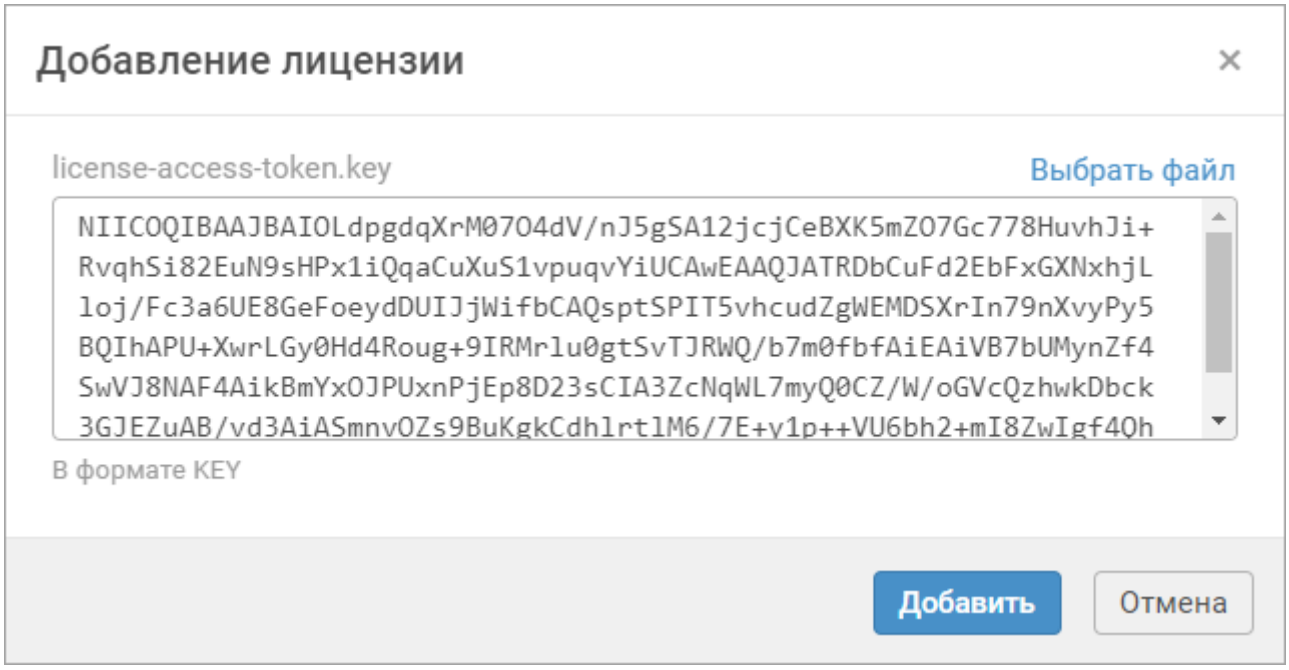

Рисунок 8. Добавление лицензии

4. По ссылке **Выбрать файл** выберите файл лицензии на своем компьютере.

   В поле появится содержимое файла лицензии.

5. Нажмите кнопку **Добавить**.

   На странице отобразится информация об активированной лицензии.

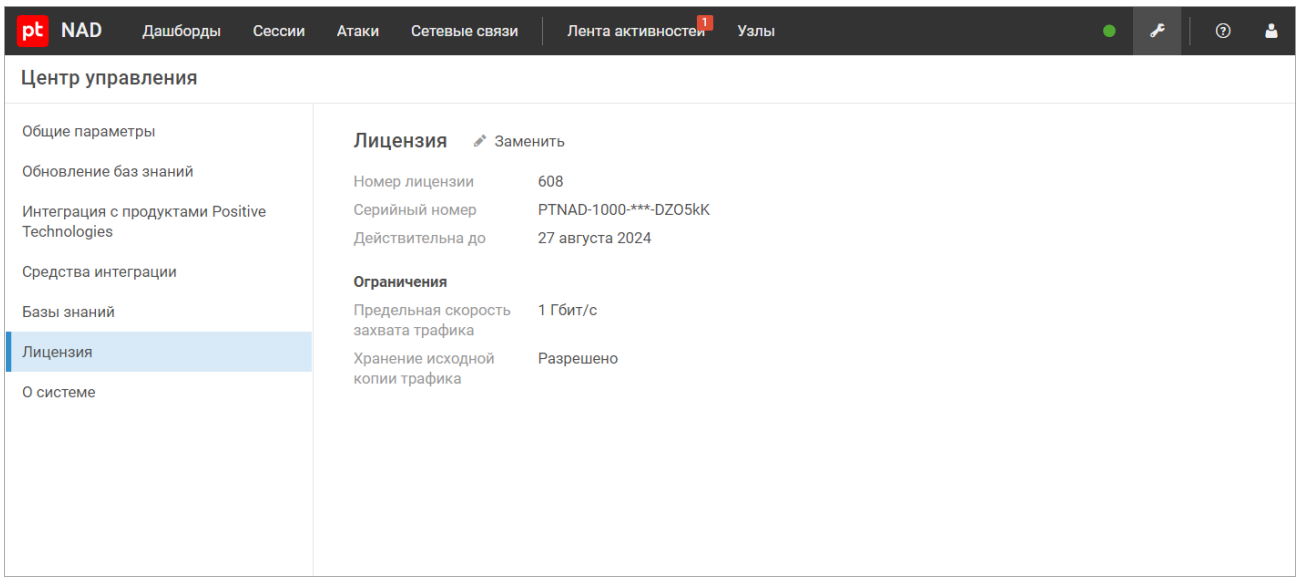

Рисунок 9. Информация о лицензии

Лицензия активирована.

См. также

Лицензирование (см. раздел 4)

5.3. Перенос параметров продукта из конфигурационных файлов в базу данных

После установки PT NAD 12.0 или обновления до этой версии вам нужно запустить скрипт для переноса параметров продукта из конфигурационных файлов в базу данных. Если этого не сделать, вы не сможете настраивать продукт в веб-интерфейсе.

- Чтобы перенести параметры продукта из конфигурационных файлов в базу данных:

  1. Запустите скрипт для переноса параметров:

     ```
     sudo /opt/ptsecurity/nad/bin/manage settings migrate
     ```

     Примечание. В многосерверной конфигурации скрипт нужно запускать на основном сервере.

  2. После завершения работы скрипта в веб-интерфейсе продукта в главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  3. Проверьте и при необходимости исправьте значения параметров на вкладках **Общие параметры**, **Обновление баз знаний**, **Интеграция с продуктами Positive Technologies** и **Средства интеграции**.

  4. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

5.4. Указание адреса веб-интерфейса PT NAD

Адрес веб-интерфейса нужно указать для того, чтобы пользователи могли перейти в PT NAD из внешних сервисов и программ, например из почтовых уведомлений.

- Чтобы указать адрес веб-интерфейса PT NAD:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. В блоке параметров **Веб-интерфейс** в поле **Адрес веб-интерфейса** введите IP-адрес или доменное имя, по которому доступен веб-интерфейс PT NAD. Порт указывать не нужно.
3. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Адрес веб-интерфейса PT NAD указан.

5.5. Настройка отправки уведомлений на электронную почту

Чтобы PT NAD мог отправлять уведомления на адреса электронной почты пользователей, вам нужно указать PT NAD параметры доступа к SMTP-серверу вашей организации.

Перед выполнением инструкции нужно указать адрес веб-интерфейса (см. раздел 5.4).

- Чтобы настроить отправку уведомлений на электронную почту:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
  2. В блоке параметров **Подключение к почтовому серверу** по кнопке **Настроить** откройте окно **Настройка подключения к почтовому серверу**.
  3. В поле **Адрес** укажите IP-адрес или доменное имя SMTP-сервера организации.
  4. В поле **Порт** укажите порт для подключения к SMTP-серверу.
  5. В поле **Логин** укажите логин для аутентификации на SMTP-сервере.
  6. В поле **Пароль** укажите пароль для аутентификации на SMTP-сервере.
  7. Выберите способ шифрования соединения с SMTP-сервером или отключите шифрование, если сервер не поддерживает его.
  8. В поле **Электронная почта отправителя** укажите адрес электронной почты для записи в поле From заголовков сообщений с уведомлениями от PT NAD.
  9. Нажмите кнопку **Сохранить**.
  10. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

      Изменения будут применены через некоторое время.

  Отправка уведомлений на электронную почту настроена.

Вы можете проверить корректность настройки с помощью команды:

```
sudo /opt/ptsecurity/nad/bin/manage sendtestemail <Ваш адрес электронной почты>
```

Например:

```
sudo /opt/ptsecurity/nad/bin/manage sendtestemail username@example.com
```

Если почтовые уведомления настроены правильно, на указанный адрес придет тестовое письмо.

5.6. Настройка обновления баз знаний

Вы можете настроить обновление списка правил и репутационных списков.

В этом разделе

5.6.1. Настройка получения индикаторов компрометации от PT Cybsi Provider

Если в сетевой инфраструктуре вашей организации установлена система MaxPatrol SIEM, вы можете настроить получение индикаторов компрометации от компонента PT Cybsi Provider (PT CP) этой системы.

Компонент PT CP автоматически получает индикаторы компрометации из баз знаний экспертного центра Positive Technologies и сторонних вендоров. Индикаторы компрометации — это сетевые артефакты, указывающие на потенциальную вредоносную активность в информационной системе организации.

Перед настройкой вам нужно убедиться, что компонент PT CP в MaxPatrol SIEM установлен и настроен. Инструкция приведена в Руководстве администратора MaxPatrol SIEM в разделе «Установка и первоначальная настройка компонента PT CP».

► Чтобы настроить получение индикаторов компрометации от PT CP:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. Выберите вкладку **Интеграция с продуктами Positive Technologies**.
3. В блоке параметров **Интеграция с PT Cybsi Provider** по кнопке **Настроить** откройте окно **Настройка интеграции с PT Cybsi Provider**.
4. В поле **Адрес сервера** укажите IP-адрес или доменное имя узла, на котором установлен PT CP.
5. В поле **Порт сервера** укажите порт 2443.
6. Если вам нужно, чтобы PT NAD проверял сертификат, которым подписывается PT CP, включите доверие сертификата организации (см. раздел 5.10).
7. Если такая проверка не нужна, выключите проверку сертификата.
8. Нажмите кнопку **Сохранить**.
9. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Получение индикаторов компрометации от PT CP настроено.

Индикаторы компрометации загружаются в PT NAD в виде репутационных списков. Обновления проверяются раз в минуту.

5.6.2. Настройка подключения PT NAD к прокси-серверу для получения обновлений базы знаний

Если сервер с установленным модулем nad-task-server подключается к интернету через прокси-сервер, требуется указать параметры подключения к этому прокси-серверу для получения обновлений базы знаний из внешнего источника.

► Чтобы настроить подключение к прокси-серверу:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. Выберите вкладку **Обновление баз знаний**.
3. В блоке параметров **Подключение к прокси-серверу** по кнопке **Настроить** откройте окно **Настройка подключения к прокси-серверу**.

4. Выберите протокол для подключения к прокси-серверу.
5. В поле **Адрес** укажите IP-адрес или доменное имя прокси-сервера.
6. В поле **Порт** укажите порт для доступа к прокси-серверу.
7. Если прокси-сервер требует аутентификации подключающихся к нему клиентов, в полях **Логин** и **Пароль** укажите учетные данные для аутентификации.
8. Нажмите кнопку **Сохранить**.
9. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Подключение к прокси-серверу настроено.

См. также

Настройка подключения локального зеркала к прокси-серверу (см. раздел 5.6.6.3)

5.6.3. Изменение частоты проверки обновлений для баз знаний

По умолчанию PT NAD проверяет наличие обновлений для баз знаний раз в час. Вы можете изменить эту частоту.

► Чтобы изменить частоту проверки обновлений для баз знаний:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
2. Выберите вкладку **Обновление баз знаний**.
3. В блоке параметров **Общие параметры обновления** по кнопке **Настроить** откройте окно **Настройка общих параметров обновления**.
4. В поле **Частота проверки обновлений (в секундах)** укажите частоту проверки обновлений.

   Минимальное значение — 300.
5. Нажмите кнопку **Сохранить**.
6. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Частота проверки обновлений для баз знаний изменена.

5.6.4. Настройка автообновления правил Proofpoint ET

PT NAD поддерживает правила Proofpoint ET для обнаружения атак. Вы можете настроить автоматическую загрузку в PT NAD правил как из общедоступного набора Proofpoint ET Open, так и из платного Proofpoint ET Pro. В последнем случае вам нужно самостоятельно купить этот набор и подготовить код (oinkcode), полученный при заказе этих правил. Более подробная информация о правилах Proofpoint ET доступна на сайте proofpoint.com.

Настройка автообновления правил Proofpoint ET Open

- Чтобы настроить автообновление правил Proofpoint ET Open:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **База знаний ETOpen** по кнопке **Настроить** откройте окно **Настройка базы знаний ETOpen**.
  4. Включите обновление от источника.
  5. В параметре **Тип источника** выберите вариант **HTTP-сервер**.
  6. Если вам не нужно, чтобы PT NAD проверял сертификат веб-сервера, с которого загружаются правила, отключите проверку сертификата.
  7. Нажмите кнопку **Сохранить**.
  8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

  Автообновление правил Proofpoint ET Open настроено.

Настройка автообновления правил Proofpoint ET Pro

- Чтобы настроить автообновление правил Proofpoint ET Pro:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **Базы знаний** по кнопке **Добавить** откройте окно **Добавление базы знаний**.

4. В параметре **Тип источника** выберите вариант **HTTP-сервер**.
5. В поле **Вендор** введите произвольное название вендора (например, `Proofpoint ET Pro`).
6. В поле **URL источника** введите `https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz` и вместо `<oinkcode>` укажите код, полученный при заказе правил Proofpoint ET Pro.
7. Если вам не нужно, чтобы PT NAD проверял сертификат веб-сервера, с которого загружаются правила, отключите проверку сертификата.
8. В поле **Файл с правилами для атак** введите `etpro.rules.tar.gz`.
9. Нажмите кнопку **Добавить**.
10. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

    Изменения будут применены через некоторое время.

Автообновление правил Proofpoint ET Pro настроено.

5.6.5. Настройка источника обновлений правил Proofpoint ET

По умолчанию обновление правил Proofpoint ET отключено. Вы можете настроить автоматическую загрузку этих правил из удаленного источника (см. раздел 5.6.4).

Получение обновлений Proofpoint ET Open из локального каталога

Если политика информационной безопасности организации запрещает доступ в интернет для PT NAD или если у сервера с установленным модулем nad-task-server отсутствует канал связи с интернетом, вы можете настроить получение обновлений правил Proofpoint ET Open из локального каталога. Для передачи файлов обновлений вы можете либо вручную копировать их в локальный каталог при помощи внешнего носителя, либо настроить автоматическую передачу обновлений внешними средствами.

► Чтобы настроить обновление правил Proofpoint ET Open из локального каталога:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
2. Выберите вкладку **Обновление баз знаний**.
3. В блоке параметров **База знаний ETOpen** по кнопке **Настроить** откройте окно **Настройка базы знаний ETOpen**.

4. Убедитесь, что обновление от источника включено.
5. В параметре **Тип источника** выберите вариант **Локальный каталог**.
6. При необходимости в поле **Путь к локальному каталогу** измените путь к локальному каталогу с обновлениями.
7. Нажмите кнопку **Сохранить**.
8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Обновление правил Proofpoint ET Open из локального каталога настроено.

Получение обновлений Proofpoint ET Pro из локального каталога

Если политика информационной безопасности организации запрещает доступ в интернет для PT NAD или если у сервера с установленным модулем nad-task-server отсутствует канал связи с интернетом, вы можете настроить получение обновлений правил Proofpoint ET Pro из локального каталога. Для передачи файлов обновлений вы можете либо вручную копировать их в локальный каталог при помощи внешнего носителя, либо настроить автоматическую передачу обновлений внешними средствами.

Перед выполнением инструкции нужно настроить автообновление правил ET Pro (см. раздел 5.6.4).

- Чтобы настроить обновление правил Proofpoint ET Pro из локального каталога:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **Базы знаний** в секции вендора Proofpoint ET Pro по кнопке **Настроить** откройте окно **Настройка базы знаний**.
  4. Убедитесь, что обновление от источника включено.
  5. В параметре **Тип источника** выберите вариант **Локальный каталог**.
  6. При необходимости в поле **Путь к локальному каталогу** измените путь к локальному каталогу с обновлениями.
  7. Нажмите кнопку **Сохранить**.
  8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

Обновление правил Proofpoint ET Pro из локального каталога настроено.

Получение обновлений Proofpoint ET Open из удаленного источника

- Чтобы настроить автообновление правил Proofpoint ET Open из удаленного источника:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **База знаний ETOpen** по кнопке **Настроить** откройте окно **Настройка базы знаний ETOpen**.
  4. Убедитесь, что обновление от источника включено.
  5. В параметре **Тип источника** выберите вариант **HTTP-сервер**.
  6. Если вам не нужно, чтобы PT NAD проверял сертификат веб-сервера, с которого загружаются правила, отключите проверку сертификата.
  7. Нажмите кнопку **Сохранить**.
  8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

  Автообновление правил Proofpoint ET Open из удаленного источника настроено.

Получение обновлений Proofpoint ET Pro из удаленного источника

Перед выполнением инструкции нужно настроить автообновление правил ET Pro (см. раздел 5.6.4).

- Чтобы настроить автообновление правил Proofpoint ET Pro из удаленного источника:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **Базы знаний** в секции вендора Proofpoint ET Pro по кнопке **Настроить** откройте окно **Настройка базы знаний**.
  4. Убедитесь, что обновление от источника включено.
  5. В параметре **Тип источника** выберите вариант **HTTP-сервер**.

6. Если вам не нужно, чтобы PT NAD проверял сертификат веб-сервера, с которого загружаются правила, отключите проверку сертификата.
7. Нажмите кнопку **Сохранить**.
8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Автообновление правил Proofpoint ET Pro из удаленного источника настроено.

5.6.6. Настройка обновления базы знаний Positive Technologies с помощью локального зеркала

PT NAD может работать на сервере в изолированном от интернета сегменте сети. В этом случае для получения обновлений правил и репутационных списков Positive Technologies нужно настроить локальное зеркало обновлений. Оно должно располагаться в демилитаризованной зоне (ДМЗ) и загружать обновления с сайта Positive Technologies (см. рисунок ниже). Для передачи обновлений с локального зеркала в PT NAD вы можете либо вручную копировать их при помощи внешнего носителя, либо настроить их автоматическую передачу.

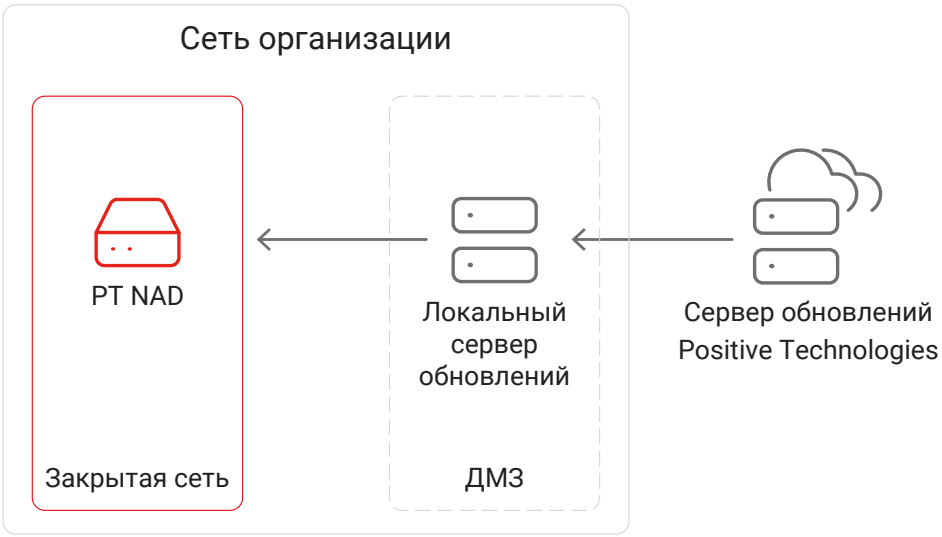

Рисунок 10. Обновление базы знаний Positive Technologies в закрытом сегменте сети

Для обновления правил и репутационных списков Positive Technologies через локальное зеркало нужно установить локальный сервер обновлений (см. раздел 5.6.6.2) и активировать на нем лицензию, приобретенную организацией (см. раздел 5.6.6.4).

Если между локальными серверами отсутствует сетевая связность, нужно также сменить источник обновлений (см. раздел 5.6.6.6) для базы знаний Positive Technologies с удаленного сервера на локальный каталог, после чего обновлять базу знаний вручную (см. раздел 5.6.6.7). Если сетевая связность между серверами есть, вы можете настроить автоматическое получение обновлений (см. раздел 5.6.6.8).

В этом разделе

5.6.6.1. Аппаратные и программные требования

Локальный сервер обновлений может быть установлен как на физическом сервере, так и в виртуальной среде.

Аппаратные требования

Для работы локального сервера обновлений потребуются следующие минимальные аппаратные ресурсы:

— 2 ядра процессора;

— 4 ГБ оперативной памяти;

— 150 ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений рекомендуется устанавливать на чистую 64-разрядную серверную версию Debian 10 Buster.

5.6.6.2. Установка локального сервера обновлений

В этом разделе приводится инструкция по установке локального сервера обновлений в демилитаризованной зоне.

Перед выполнением инструкции нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяют аппаратным и программным требованиям (см. раздел 5.6.6.1), а также выполнить подготовительные действия на этом сервере или виртуальной машине.

- Чтобы установить локальный сервер обновлений:

  1. Перейдите в каталог `repos/additional_packages` каталога с распакованным дистрибутивом.

     Например:

     ```
     cd /home/user/ptnad-installer/repos/additional_packages
     ```

  2. Запустите установку локального сервера обновлений:

     ```
     sudo dpkg -i pt-update-mirror-*.deb
     ```

  Локальный сервер обновлений установлен и запущен в виде службы подсистемы systemd. Вы можете проверять состояние сервера с помощью команды `systemctl status pt-update-mirror` и просматривать его журналы в файле `/var/log/pt-update-mirror/mirror.log`.

Теперь вам нужно активировать лицензию на установленном локальном сервере обновлений (см. раздел 5.6.6.4).

5.6.6.3. Настройка подключения локального зеркала к прокси-серверу

Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, нужно указать параметры подключения к этому прокси-серверу для активации лицензии и получения обновлений базы знаний с публичного сервера обновлений Positive Technologies.

- Чтобы настроить подключение локального сервера обновлений к интернету через прокси-сервер:

  1. Откройте файл `/etc/pt-update-mirror/config.json`:

     ```
     sudo nano /etc/pt-update-mirror/config.json
     ```

  2. В качестве значения параметра `proxy` введите адрес (и при необходимости порт) прокси-сервера, например:

     ```
     "proxy": "http://proxy.example.com:3128",
     ```

  3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения в параметрах `proxy-user` и `proxy-password` соответственно, например:

     ```
     "proxy-user": "username",
     "proxy-password": "P@ssw0rd",
     ```

4. Сохраните изменения в файле `/etc/pt-update-mirror/config.json`.
5. Перезапустите локальный сервер обновлений:

   ```
   sudo systemctl restart pt-update-mirror.service
   ```

Подключение локального сервера обновлений к интернету через прокси-сервер настроено.

См. также

Настройка подключения PT NAD к прокси-серверу для получения обновлений базы знаний (см. раздел 5.6.2)

5.6.6.4. Активация лицензии на локальном сервере обновлений

После установки локального сервера обновлений нужно активировать на нем лицензию, приобретенную организацией. Лицензия нужна для аутентификации локального сервера обновлений на публичном сервере обновлений Positive Technologies. Активация выполняется с помощью файла лицензии `license-access-token.key`. Вы можете найти этот файл на установочном диске из комплекта поставки или в электронном письме, поступившем на адрес, указанный при заказе лицензии.

Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, перед активацией лицензии нужно настроить подключение к этому прокси-серверу (см. раздел 5.6.6.3).

- Чтобы активировать лицензию на локальном сервере обновлений,

  выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token
  <Полный путь к файлу лицензии>
  ```

  Например:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token /home/
  user/license-access-token.key
  ```

  Появится сообщение вида `License from file = [<Путь к файлу лицензии>] activated`.

  Лицензия активирована.

Вы можете просмотреть параметры активированной лицензии при помощи команды `sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license view`.

См. также

Деактивация лицензии на локальном сервере обновлений (см. раздел 5.6.6.5)

5.6.6.5. Деактивация лицензии на локальном сервере обновлений

Если вам требуется прекратить работу с активированной лицензией на локальном сервере обновлений, вы можете деактивировать лицензию. Деактивация может понадобиться перед заменой лицензии в следующих случаях:

- Приобретена лицензия с обновленным сроком действия. При заказе лицензии устанавливается дата окончания срока ее действия. Если срок подходит к концу или истек, вы можете обратиться в техническую поддержку, чтобы продлить его или заказать новую лицензию. В последнем случае после получения файла новой лицензии вам нужно заменить лицензию в продукте.
- Одна и та же лицензия была активирована в нескольких экземплярах PT NAD. Поскольку одна лицензия может использоваться только в одном экземпляре продукта, вам нужно заменить лицензии так, чтобы в каждом экземпляре была активирована своя лицензия.

  Примечание. При нехватке лицензий вашей организации нужно докупить их.

Деактивация выполняется с помощью файла `license-access-token.key`, который использовался для активации этой лицензии (см. раздел 5.6.6.4).

- Чтобы деактивировать лицензию на локальном сервере обновлений,

  выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license deactivate --license-token <Полный путь к файлу лицензии>
  ```

  Например:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license deactivate --license-token /home/user/license-access-token.key
  ```

  Появится сообщение вида `License from file = [<Путь к файлу лицензии>] deactivated`.

  Например:

  ```
  License from file = /home/user/license-access-token.key deactivated
  ```

  Лицензия деактивирована.

После деактивации лицензия на локальном сервере обновлений будет автоматически удалена.

5.6.6.6. Настройка обновления базы знаний Positive Technologies из локального каталога

По умолчанию PT NAD обновляет базу знаний Positive Technologies с публичного сервера Positive Technologies. Для обновления вручную с помощью локального зеркала нужно сменить источник обновления на локальный каталог.

► Чтобы настроить обновление базы знаний Positive Technologies из локального каталога:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. Выберите вкладку **Обновление баз знаний**.
3. В блоке параметров **База знаний PTSecurity** по кнопке **Настроить** откройте окно **Настройка базы знаний PTSecurity**.
4. Убедитесь, что обновление от источника включено.
5. В параметре **Тип источника** выберите вариант **Локальный каталог**.
6. При необходимости в поле **Путь к локальному каталогу** измените путь к локальному каталогу с обновлениями.
7. Нажмите кнопку **Сохранить**.
8. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Обновление базы знаний Positive Technologies из локального каталога настроено.

Теперь вы можете обновлять базу знаний Positive Technologies вручную (см. раздел 5.6.6.7).

См. также

Настройка обновления базы знаний Positive Technologies напрямую с публичного сервера (см. раздел 5.6.7)

5.6.6.7. Ручное обновление базы знаний Positive Technologies в закрытом сегменте сети

Если между локальным сервером обновлений в ДМЗ и PT NAD в закрытом сегменте сети отсутствует сетевая связность, вам нужно перенести обновления базы знаний Positive Technologies в закрытый сегмент сети вручную.

Перед выполнением инструкции нужно установить локальный сервер обновлений (см. раздел 5.6.6.2), активировать на нем лицензию (см. раздел 5.6.6.4) и настроить получение обновлений из локального каталога (см. раздел 5.6.6.6).

> **Примечание.** Вы можете узнать последнюю доступную для обновления версию базы знаний Positive Technologies при помощи команды `sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository view`. Версию базы знаний, установленную в продукте, можно посмотреть на вкладке **Базы знаний** страницы **Центр управления** (доступна по кнопке в главном меню).

► Чтобы вручную обновить базу знаний Positive Technologies в закрытом сегменте сети:

1. На локальном сервере обновлений в ДМЗ запустите получение обновлений с публичного сервера Positive Technologies:

   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
   ```

   Если сервер получит информацию о доступных обновлениях, появится сообщение `New data available for update`.

   Внимание! Сохраните текстовый результат выполнения команды. Он понадобится вам в дальнейшем.

2. На этом же сервере экспортируйте полученные обновления в файл экспорта-импорта обновлений:

   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --only-data-bases
   <Путь к файлу экспорта-импорта с его названием>
   ```

   Например:

   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --only-data-bases /
   home/user/tmp/update.tar.gz
   ```

   Появится сообщение `Export has been completed`.

3. На этом же сервере импортируйте обновления из файла экспорта-импорта во временный каталог:

   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror --db-path <Путь к временному каталогу>
   repository import <Путь к файлу экспорта-импорта с его названием>
   ```

   Например:

   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror --db-path /tmp/update-2022-05-16
   repository import /home/user/updates/update.tar.gz
   ```

4. Подтвердите импорт, нажав клавиши Y, Enter.

   Появится сообщение `Import has been completed`.

5. Скопируйте временный каталог с его содержимым на сервер PT NAD в закрытом сегменте сети с помощью внешнего носителя.

6. На сервере PT NAD в закрытом сегменте сети скопируйте архивы с обновлениями базы знаний из временного каталога в локальный каталог с обновлениями (см. раздел 5.6.6.6):

   ```
   sudo cp <Путь к временному каталогу, в который были импортированы обновления>/products/
   PTNAD.KB/<Версия базы знаний>/download/*.tar.gz <Путь к локальному каталогу с
   обновлениями>
   ```

   Например:

   ```
   sudo cp /tmp/update-2022-05-16/products/PTNAD.KB/7.2.749/download/*.tar.gz /opt/updates
   ```

   Версию базы знаний можно получать из результатов выполнения команды, упомянутой на первом шаге. Версия записывается в строку следующего вида:

   ```
   PTNAD.KB downloaded <Версия базы знаний>.
   ```

Например:

```
PTNAD.KB downloaded 7.2.749.
```

7. Дождитесь следующего по расписанию автоматического обновления баз знаний (см. раздел 5.6.3) или запустите процесс обновления на сервере PT NAD вручную:

   ```
   sudo /opt/ptsecurity/nad/bin/manage update --source fs -V PTSecurity
   ```

База знаний Positive Technologies обновлена в закрытом сегменте сети.

См. также

Настройка автоматического обновления базы знаний Positive Technologies в закрытом сегменте сети (см. раздел 5.6.6.8)

Настройка обновления базы знаний Positive Technologies напрямую с публичного сервера (см. раздел 5.6.7)

5.6.6.8. Настройка автоматического обновления базы знаний Positive Technologies в закрытом сегменте сети

Если между локальным сервером обновлений в ДМЗ и PT NAD в закрытом сегменте сети есть сетевая связность, вы можете настроить автоматическую передачу обновлений с публичного сервера Positive Technologies на сервер PT NAD через локальный сервер обновлений.

Локальное зеркало в ДМЗ запрашивает обновления с публичного сервера Positive Technologies в 13, 27, 42 и 58 минут каждого часа, вы можете изменить эту частоту на локальном сервере обновлений (см. раздел 5.6.6.9). PT NAD проверяет наличие обновлений для баз знаний раз в час, изменить частоту проверки можно на основном сервере (см. раздел 5.6.3) в закрытом сегменте.

Перед выполнением инструкции нужно:

1. Установить локальный сервер обновлений (см. раздел 5.6.6.2).
2. Активировать на нем лицензию (см. раздел 5.6.6.4).
3. Получить файлы `cert.crt` и `cert.key` сертификата, выданного центром сертификации вашей организации для локального сервера обновлений.

   Если у вас есть промежуточные сертификаты, которые нужно использовать, они должны быть сохранены в одном файле вместе с сертификатом открытого ключа (записаны после него).

Сертификат должен соответствовать следующим требованиям:

- иметь формат PEM;
- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Subject Alternative Name (SAN) содержать запись о доменном имени или IP-адресе локального сервера обновлений.

4. На основном сервере PT NAD включить доверие сертификата организации (см. раздел 5.10), которым был подписан сертификат локального сервера обновлений.

► Чтобы настроить автоматическое обновление базы знаний Positive Technologies в закрытом сегменте сети:

1. Скопируйте файлы `cert.crt` и `cert.key` сертификата локального сервера обновлений в каталог `/etc/pt-update-mirror/https_certs` на этом сервере.
2. Перезапустите локальный сервер обновлений:
   ```
   sudo systemctl restart pt-update-mirror.service
   ```
3. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
4. Выберите вкладку **Обновление баз знаний**.
5. В блоке параметров **Общие параметры обновления** по кнопке **Настроить** откройте окно **Настройка общих параметров обновления**.
6. В поле **Адрес сервера обновлений Positive Technologies** вместо адреса публичного сервера Positive Technologies укажите адрес локального сервера обновлений в ДМЗ, например `198.51.100.78`.
7. В поле **Порт сервера обновлений Positive Technologies** введите `8743`.
8. Нажмите кнопку **Сохранить**.
9. В блоке параметров **База знаний PTSecurity** по кнопке **Настроить** откройте окно **Настройка базы знаний PTSecurity**.
10. Убедитесь, что обновление от источника включено.
11. В параметре **Тип источника** выберите вариант **Сервер обновлений Positive Technologies**.

12. Нажмите кнопку **Сохранить**.
13. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

    Изменения будут применены через некоторое время.

Автоматическое обновление базы знаний Positive Technologies в закрытом сегменте сети настроено.

Вы можете проверить состояние автоматического запуска обновлений на локальном зеркале с помощью команды `sudo systemctl status pt-update-mirror-update.timer`.

См. также

Ручное обновление базы знаний Positive Technologies в закрытом сегменте сети (см. раздел 5.6.6.7)

Настройка обновления базы знаний Positive Technologies напрямую с публичного сервера (см. раздел 5.6.7)

5.6.6.9. Изменение частоты проверки обновлений для баз знаний на локальном зеркале

По умолчанию локальное зеркало в ДМЗ запрашивает обновления с публичного сервера Positive Technologies в 13, 27, 42 и 58 минут каждого часа. Вы можете изменить эту частоту.

- Чтобы изменить частоту проверки обновлений для баз знаний на локальном зеркале:

  1. Откройте файл `/etc/systemd/system/pt-update-mirror-update.timer`:
     ```
     sudo nano /etc/systemd/system/pt-update-mirror-update.timer
     ```
  2. В блоке параметров `Timer` в качестве значения параметра `OnCalendar` укажите нужное время получения обновлений в формате systemd.timer (например, `OnCalendar=*-*-* *:15,25,45,50:00`).
  3. Сохраните файл `pt-update-mirror-update.timer`.
  4. Примените изменения:
     ```
     sudo systemctl daemon-reload
     ```

  Частота проверки обновлений для баз знаний на локальном зеркале изменена.

5.6.7. Настройка обновления базы знаний Positive Technologies напрямую с публичного сервера

При необходимости вы можете вернуть параметры обновления базы знаний Positive Technologies к значениям по умолчанию — к обновлению напрямую с публичного сервера.

- Чтобы настроить обновление базы знаний Positive Technologies напрямую с публичного сервера:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **База знаний PTSecurity** по кнопке **Настроить** откройте окно **Настройка базы знаний PTSecurity**.
  4. Убедитесь, что обновление от источника включено.
  5. В параметре **Тип источника** выберите вариант **Сервер обновлений Positive Technologies**.
  6. Нажмите кнопку **Сохранить**.
  7. В блоке параметров **Общие параметры обновления** по кнопке **Настроить** откройте окно **Настройка общих параметров обновления**.
  8. В поле **Адрес сервера обновлений Positive Technologies** введите `update.ptsecurity.com`.
  9. Очистите поле **Порт сервера обновлений Positive Technologies**.
  10. Нажмите кнопку **Сохранить**.
  11. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

      Изменения будут применены через некоторое время.

  Обновление базы знаний Positive Technologies напрямую с публичного сервера настроено.

5.7. Настройка пользовательского веб-интерфейса

Вы можете настроить веб-интерфейс PT NAD под нужды пользователей продукта.

В этом разделе

5.7.1. Замена SSL-сертификата

SSL-сертификат нужен для того, чтобы пользователи PT NAD имели доступ к страницам веб-интерфейса продукта через HTTPS-соединение. При установке deb-пакета PT NAD устанавливается самоподписанный сертификат Positive Technologies. Поэтому при подключении к веб-интерфейсу пользователи по умолчанию получают предупреждение о том, что создаваемое подключение не защищено.

Вы можете заменить сертификат Positive Technologies на собственный доверенный. Он должен отвечать следующим требованиям:

- иметь формат PEM;
- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Subject Alternative Name (SAN) содержать запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта.

  Примечание. Если пользователи должны подключаться к веб-интерфейсу с того же сервера, на котором он установлен, в полях SAN также должны быть прописаны доменное имя localhost и IP-адрес 127.0.0.1.

Перед выполнением инструкции вам нужно загрузить на узел с установленным веб-сервером nginx файл SSL-сертификата открытого ключа и файл закрытого ключа, идущего с ним в паре. Если у вас есть промежуточные сертификаты, которые нужно использовать, они должны быть сохранены в одном файле вместе с сертификатом открытого ключа (записаны после него).

► Чтобы заменить SSL-сертификат:

1. Перейдите в каталог, в котором хранятся файлы вашего сертификата.

   Например:

   ```
   cd /home/username/cert
   ```

2. Переименуйте файлы вашего сертификата:

   ```
   cp <Название файла сертификата открытого ключа> server.crt
   cp <Названия файла закрытого ключа> server.key
   ```

   Например:

   ```
   cp example_com.pem server.crt
   cp example_com.key server.key
   ```

3. Создайте резервную копию сертификата Positive Technologies:

   ```
   tar cvzf <Название архива с создаваемой резервной копией> /etc/nginx/ssl/server*
   ```

   Например:

   ```
   tar cvzf backup.tar.gz /etc/nginx/ssl/server*
   ```

4. Скопируйте файлы вашего сертификата в каталог сертификата nginx:
   ```
   cp server.* /etc/nginx/ssl
   ```
   Например:
   ```
   cp server.* /etc/nginx/ssl
   ```
5. Перезагрузите веб-сервер nginx:
   ```
   sudo systemctl restart nginx.service
   ```
6. Перезапустите модуль nad-web-server:
   ```
   sudo systemctl restart nad-web-server.service
   ```

SSL-сертификат заменен.

Вы можете проверить работоспособность нового сертификата, открыв веб-интерфейс PT NAD. В адресной строке браузера, слева от адреса, должен появиться значок .

5.7.2. Изменение максимально допустимого периода в запросах к базе данных

По умолчанию период, за который PT NAD запрашивает информацию из базы данных, ограничен 10 днями. Вы можете увеличить этот период. Это позволит пользователям продукта:

- указывать больший период для фильтрации данных на страницах **Дашборды**, **Сессии**, **Атаки** и **Сетевые связи**;
- настраивать больший период в условиях для срабатывания уведомлений по фильтрам;
- настраивать ежемесячное получение автоматических отчетов (если новый период равен 31 дню).

► Чтобы изменить максимально допустимый период в запросах к базе данных:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.
2. В блоке параметров **Работа с данными** в поле **Максимальный допустимый период в запросах к БД (в днях)** измените период.

   Внимание! Уменьшение периода приведет к неработоспособности существующих правил генерации отчетов и уведомлений, параметры которых не соотносятся с новым периодом. После уменьшения периода уведомите пользователей о необходимости обновления таких правил.

   Примечание. Диапазон допустимых значений параметра — от 7 до 31.
3. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

Изменения будут применены через некоторое время.

Максимально допустимый период в запросах к базе данных изменен.

5.7.3. Изменение срока хранения узлов

При анализе трафика PT NAD собирает информацию об узлах, которые участвовали в сессиях. Пользователи могут просматривать эту информацию на странице **Узлы**. По умолчанию PT NAD удаляет записи об узлах после 30 дней их неактивности. 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. Вы можете изменить срок хранения.

- Чтобы изменить срок хранения узлов:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. В секции `Hosts management` раскомментируйте параметр `hosts.tracking_time` и в качестве его значения укажите срок хранения узлов в днях:

     ```
     hosts.tracking_time: <Количество дней>d
     ```

     Например:

     ```
     hosts.tracking_time: 30d
     ```

     Примечание. При обновлении PT NAD с версии 10.0 и ниже параметр отсутствует в файле и вам нужно его добавить самостоятельно.

  3. Сохраните файл `nad.settings.yaml`.

  4. Перезагрузите модули nad-task-server и nad-web-server:

     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  Срок хранения узлов изменен.

5.8. Настройка проверки целостности продукта

Проверка целостности помогает выявлять несанкционированные изменения бинарных и конфигурационных файлов продукта.

Проверка целостности осуществляется при помощи утилиты checksum, входящей в комплект поставки PT NAD. В ходе первичной настройки проверки целостности утилита вычисляет и записывает в текстовые файлы эталонные хеш-суммы SHA-256 бинарных и конфигурационных файлов продукта. В дальнейшем вы можете запускать утилиту checksum, чтобы сравнивать

текущие хеш-суммы файлов с эталонными и таким образом узнавать, выполнялось ли изменение продукта в обход его системы безопасности. Для защиты эталонных списков хеш-сумм от изменений файлы с этими списками подписываются криптографическим ключом.

В этом разделе

5.8.1. Создание ключей для проверки целостности

Перед генерацией списков с хеш-суммами файлов продукта вам нужно создать ключи, которые будут использоваться для подписи и валидации этих списков.

- Чтобы создать ключи для проверки целостности продукта:

  1. Перейдите в каталог с утилитой checksum:
     ```
     cd /opt/ptsecurity/nad/bin
     ```
  2. Сгенерируйте ключи для подписи и валидации списков:
     ```
     sudo ./checksum keygen
     ```
     В каталоге `/opt/ptsecurity/etc/.checksum` появятся два файла ключей: приватный ключ `key.pem` для подписи данных и публичный ключ `key.pub.pem` для валидации данных.

     Внимание! Настоятельно рекомендуется скопировать файлы ключей на внешний носитель для защиты от изменений.

     Внимание! Не удаляйте файлы ключей из каталога `/opt/ptsecurity/etc/.checksum`. Они будут использованы для подписи обновленных списков при изменении параметров продукта в интерфейсе.
  3. Перезагрузите модули nad-task-server и nad-web-server:
     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  Ключи для проверки целостности продукта созданы.

5.8.2. Генерация хеш-сумм бинарных и конфигурационных файлов PT NAD

Вы можете сгенерировать списки с хеш-суммами бинарных и конфигурационных файлов продукта и подписать их защищенным ключом. Полученные списки будут использованы в качестве эталонных при проверке целостности продукта (см. раздел 5.8.3).

Перед выполнением инструкции создайте ключи при помощи утилиты checksum (см. раздел 5.8.1).

- Чтобы сгенерировать хеш-суммы бинарных и конфигурационных файлов продукта:

  1. Перейдите в каталог с утилитой checksum:
     ```
     cd /opt/ptsecurity/nad/bin
     ```
  2. Запустите генерацию списков хеш-сумм и подписи этих списков ключом, сгенерированным утилитой checksum:
     - при помощи ключа, находящегося в каталоге по умолчанию:
       ```
       sudo -u nad ./checksum generate
       ```
     - при помощи ключа, находящегося в другом каталоге (например, на внешнем носителе):
       ```
       sudo -u nad ./checksum generate --private-key <путь к файлу ключа>
       ```
       Например:
       ```
       sudo -u nad ./checksum generate --private-key /media/keys/key.pem
       ```
       Появится следующее сообщение:
       ```
       INFO - "geoip" signed
       INFO - "signatures" signed
       INFO - "dga_model" signed
       INFO - "binaries" signed
       INFO - "dga_whitelist" signed
       INFO - "replists" signed
       INFO - "configs" signed
       ```

  В каталоге `/opt/ptsecurity/etc/.checksum` будут созданы файлы с расширением .sign, в которых будут записаны хеш-суммы SHA-256 бинарных и конфигурационных файлов продукта.

5.8.3. Проверка целостности продукта

В любой момент после генерации списков эталонных хеш-сумм (см. раздел 5.8.2) вы можете проверить, не подвергался ли продукт несанкционированным изменениям.

- Чтобы проверить целостность бинарных и конфигурационных файлов продукта:

  1. Перейдите в каталог с утилитой checksum:
     ```
     cd /opt/ptsecurity/nad/bin
     ```
  2. Запустите проверку целостности:
     - при помощи ключа, находящегося в каталоге по умолчанию:
       ```
       ./checksum validate
       ```
     - при помощи ключа, находящегося в другом каталоге (например, на внешнем носителе):
       ```
       ./checksum validate --public-key <путь к файлу ключа>
       ```

Например:

```
./checksum validate --public-key /media/keys/key.pub.pem
```

При успешной валидации появится сообщение:

```
INFO - configs validated successful
INFO - binaries validated successful
INFO - geoip validated successful
INFO - replists validated successful
INFO - rules validated successful
INFO - Validation successful
```

Целостность бинарных и конфигурационных файлов продукта проверена.

5.9. Отключение передачи статистики о работе PT NAD

Для улучшения PT NAD Positive Technologies собирает данные о его работе в информационной инфраструктуре организации:

- информацию о количестве срабатываний правил вендоров;
- подробные данные об атаках;
- информацию о состоянии правил вендоров (какие правила включены, какие приоритеты установлены для правил, какие действия назначены при срабатывании правил);
- количество срабатываний репутационных списков;
- статистику трафика, которая включает в себя объем трафика, количество узлов, распределение трафика по протоколам и статистику ошибок при сборке сессий.

Примечание. Все данные передаются в Positive Technologies в зашифрованном виде.

Если политика информационной безопасности организации запрещает отправлять данные в сторонние компании, вы можете отключить передачу статистики.

► Чтобы отключить передачу статистики:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. В блоке параметров **Статистика работы системы** отключите отправку статистики в Positive Technologies.
3. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Передача статистики отключена.

5.10. Включение доверия сертификата организации

Чтобы обеспечить взаимодействие PT NAD с компонентами и системами, установленными на других серверах, нужно добавить корневой сертификат организации, которым подписываются сертификаты этих компонентов и систем, в список доверенных сертификатов PT NAD. Файл сертификата должен иметь расширение .crt. Если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты, файл должен включать в себя всю цепочку сертификатов.

> **Примечание.** Эта инструкция нужна только при настройке интеграции PT NAD с PT MC, настройке получения индикаторов компрометации от PT CP и при настройке автоматического обновления базы знаний Positive Technologies в закрытом сегменте сети.

- Чтобы включить доверие сертификата организации:

  1. Скопируйте полученный файл .crt на узел с установленным модулем nad-web-server в каталог `/usr/local/share/ca-certificates`.
  2. Обновите список доверенных сертификатов в операционной системе:

     ```
     sudo update-ca-certificates
     ```

     Появится сообщение `done`.

  Доверие сертификата организации включено.

См. также

Настройка автоматического обновления базы знаний Positive Technologies в закрытом сегменте сети (см. раздел 5.6.6.8)

Настройка аутентификации через PT MC (см. раздел 5.1.3)

Настройка получения индикаторов компрометации от PT Cybsi Provider (см. раздел 5.6.1)

6. Вход в PT NAD

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

— Вход напрямую в интерфейс PT NAD с учетными данными, настроенными вами или другим администратором PT NAD.

— 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 (см. раздел 5.1.3).

В этом разделе

6.1. Вход в PT NAD без сервиса единого входа

Для администрирования PT NAD вам нужно войти в его интерфейс, используя учетную запись с ролью администратора.

► Чтобы войти в PT NAD:

1. В адресной строке браузера введите IP-адрес или доменное имя веб-сервера PT NAD.

   Откроется страница входа в PT NAD.
2. В поле **Логин** введите логин учетной записи.
3. В поле **Пароль** введите пароль вашей учетной записи.
4. Нажмите кнопку **Войти**.

   Откроется страница **Дашборды**.

6.2. Вход в PT NAD через PT MC

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

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. В поле **Логин** введите логин учетной записи.
3. В поле **Пароль** введите пароль вашей 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.

4. Нажмите кнопку **Войти**.

   Откроется страница **Дашборды**.

7. 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

Главное меню (см. раздел 7.1)

Страницы интерфейса и рабочая область (см. раздел 7.2)

Индикатор состояния продукта (см. раздел 7.3)

См. также

Подсистема пользовательского интерфейса (см. раздел 2.2.4)

Настройка пользовательского веб-интерфейса (см. раздел 5.7)

7.1. Главное меню

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

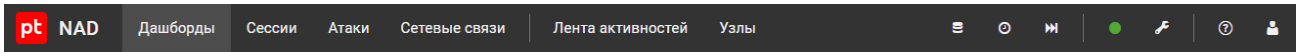

Рисунок 11. Главное меню PT NAD

Главное меню обеспечивает доступ к основным функциям PT NAD.

Переход к другим приложениям

При настроенной интеграции с MaxPatrol SIEM 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).

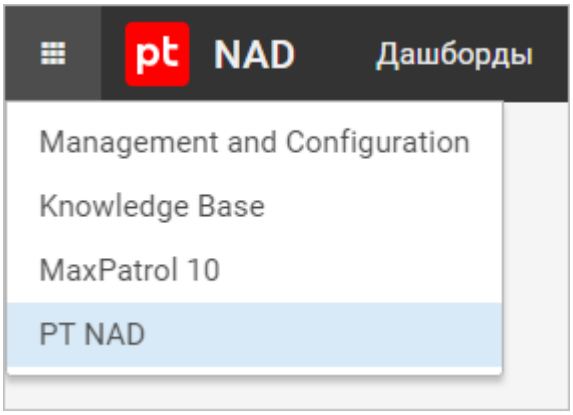

Рисунок 12. Меню перехода в другие приложения Positive Technologies

Переход к страницам продукта

Главное меню содержит разделы для перехода к страницам продукта (см. раздел 7.2):

- **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 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.

Отображение данных о трафике

В правой части главного меню находятся элементы управления, с помощью которых вы можете контролировать отображение данных о захваченном трафике:

выводит список хранилищ, позволяет выбрать хранилища для отображения их содержимого в интерфейсе, а также дает возможность импортировать в хранилища дампы трафика в формате PCAP.

позволяет выбрать период для фильтрации данных.

сбрасывает фильтры по периоду к значению по умолчанию (все события за последний час).

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

Прочие элементы управления

Среди прочего в главном меню также находится индикатор состояния продукта (см. раздел 7.3), 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.

7.2. 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 и фильтров, примененных в панели фильтрации.

7.3. 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.

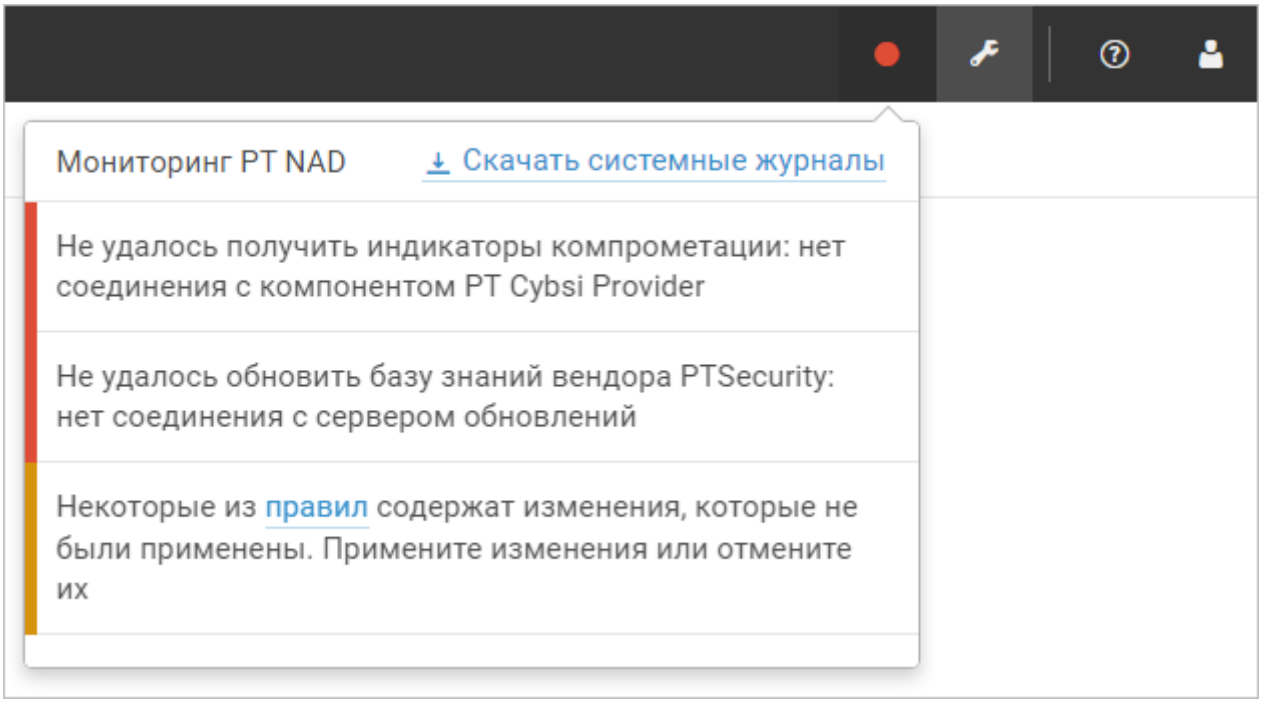

Рисунок 13. Состояние продукта

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

По нажатию на ссылку **Скачать системные журналы** на ваш компьютер скачивается архив с журналами PT NAD (см. раздел 11.2). Эта ссылка доступна только тем пользователям, у которых есть право доступа к Центру управления.

8. Просмотр информации о лицензии PT NAD

Вы можете просмотреть параметры лицензии, активированной в продукте.

- Чтобы просмотреть информацию о лицензии PT NAD:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**.

  2. Выберите вкладку **Лицензия**.

     На странице отобразится информация об активированной лицензии.

См. также

Лицензирование (см. раздел 4)

9. Замена лицензии PT NAD

Замена лицензии может потребоваться в следующих случаях:

— Приобретена лицензия с обновленным сроком действия. При заказе лицензии устанавливается дата окончания срока ее действия. Если срок подходит к концу или истек, вы можете обратиться в техническую поддержку, чтобы продлить его или заказать новую лицензию. В последнем случае после получения файла новой лицензии вам нужно заменить лицензию в продукте.

— Одна и та же лицензия была активирована в нескольких экземплярах PT NAD. Поскольку одна лицензия может использоваться только в одном экземпляре продукта, вам нужно заменить лицензии так, чтобы в каждом экземпляре была активирована своя лицензия.

Примечание. При нехватке лицензий вашей организации нужно докупить их.

► Чтобы заменить лицензию:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**.

2. Выберите вкладку **Лицензия**.

   На странице отобразится информация об активированной лицензии.

3. Нажмите кнопку **Заменить**.

   Откроется окно **Замена лицензии**.

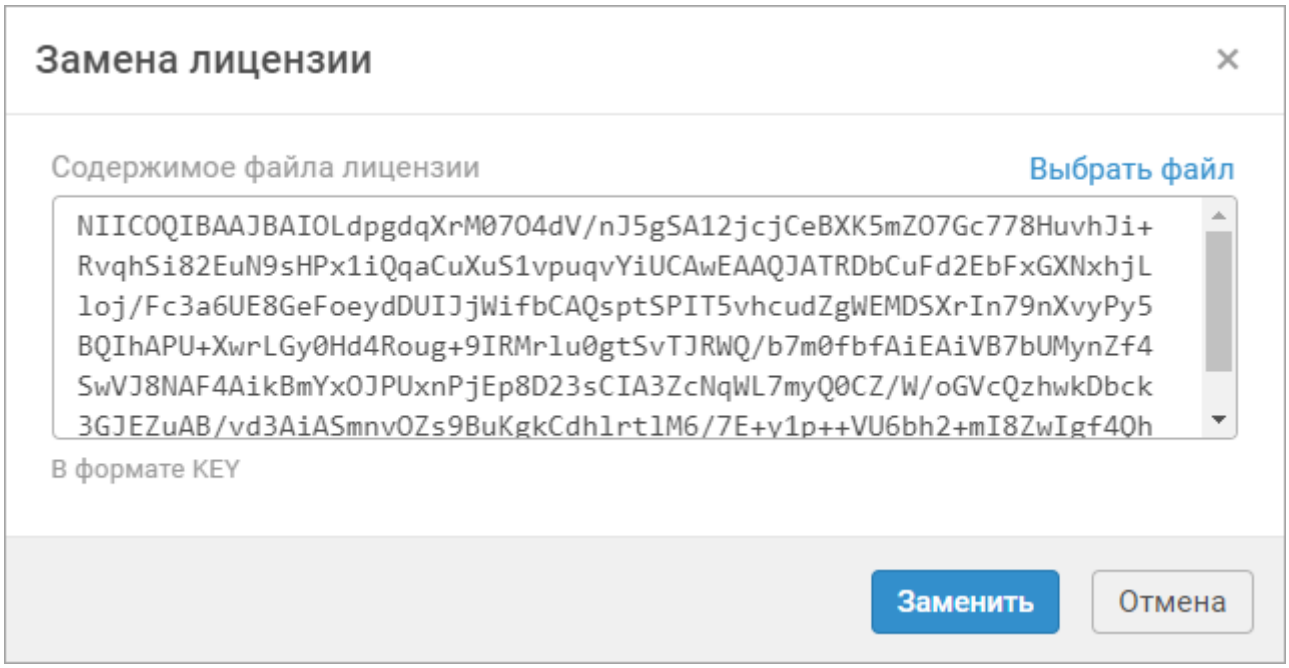

Рисунок 14. Замена лицензии

4. В поле перетащите файл новой лицензии или выберите его на своем компьютере по ссылке **Выбрать файл**.

   В поле появится содержимое файла лицензии.

5. Нажмите кнопку **Заменить**.

   Информация о новой лицензии отобразится на странице.

Лицензия заменена.

См. также

Лицензирование (см. раздел 4)

10. Администрирование PT NAD

Вы можете управлять работой PT NAD при наличии у вас соответствующих привилегий. Управление осуществляется на страницах, доступных в главном меню по кнопке .

Примечание. Этот раздел содержит инструкции по работе с журналом аудита, пользовательскими учетными записями, ролями и привилегиями, по автообновлению репутационных списков и правил. Инструкции, связанные с задачами оператора, приводятся в разделе «Администрирование PT NAD» в Руководстве оператора.

В этом разделе

10.1. Управление ролями и привилегиями

В PT NAD используется ролевая модель управления доступом. Роль — это набор привилегий, определяющих права доступа к функциям продукта.

По умолчанию в PT NAD существуют роли администратора и оператора. Администратор имеет полные права на доступ к функциям продукта. Оператор имеет все права, кроме прав на администрирование. Вы не можете удалять или изменять эти роли.

Вы можете создавать собственные роли, настраивать их привилегии и назначать роли учетным записям пользователей.

Примечание. Описанная в этом разделе функция недоступна, если в процессе установки PT NAD была настроена аутентификация с помощью сервиса единого входа PT MC.

В этом разделе

Создание пользовательской роли (см. раздел 10.1.1)

Изменение пользовательской роли (см. раздел 10.1.2)

Удаление пользовательской роли (см. раздел 10.1.3)

См. также

Управление учетными записями пользователей (см. раздел 10.2)

10.1.1. Создание пользовательской роли

- Чтобы создать пользовательскую роль:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Роли и привилегии**.

     Откроется страница **Роли и привилегии**.

  2. Нажмите кнопку **Добавить роль**.

     В таблице появится столбец **Новая роль**.

  3. При необходимости измените стандартное название роли.
  4. Установите флажки привилегий для создаваемой роли.
  5. Нажмите кнопку **Сохранить**.

  Пользовательская роль создана.

10.1.2. Изменение пользовательской роли

Вы можете изменить название роли и набор ее привилегий. Например, если после изменений в должностной инструкции сотрудника требуется расширить права доступа к функциям продукта.

Примечание. Системные роли администратора и оператора не могут быть изменены.

- Чтобы изменить пользовательскую роль:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Роли и привилегии**.

     Откроется страница **Роли и привилегии**.

  2. В панели инструментов нажмите кнопку **Изменить**.

     Таблица ролей и привилегий станет доступной для изменения.

3. Если вам нужно изменить название роли, наведите на него курсор, нажмите и в открывшемся поле введите новое название.
4. При необходимости переопределите набор привилегий роли.
5. Нажмите кнопку **Сохранить**.

Пользовательская роль изменена.

10.1.3. Удаление пользовательской роли

Вы можете удалять роли пользователей. При удалении роли учетные записи пользователей, которым эта роль была назначена, автоматически блокируются. Системные роли администратора и оператора не могут быть удалены.

- Чтобы удалить пользовательскую роль:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Роли и привилегии**.

   Откроется страница **Роли и привилегии**.
2. В панели инструментов нажмите кнопку **Изменить**.

   Таблица ролей и привилегий станет доступной для изменения.
3. Наведите курсор на название роли и нажмите .
4. Нажмите кнопку **Сохранить**.

Пользовательская роль удалена. Учетные записи пользователей, которым эта роль была назначена, заблокированы.

10.2. Управление учетными записями пользователей

Каждому пользователю PT NAD присваивается учетная запись. Вы можете создавать, изменять, удалять и блокировать учетные записи пользователей.

Примечание. Описанная в этом разделе функция недоступна, если в процессе установки PT NAD была настроена аутентификация с помощью сервиса единого входа PT MC.

В этом разделе

См. также

Управление ролями и привилегиями (см. раздел 10.1)

10.2.1. Создание учетной записи пользователя

Для предоставления пользователю доступа к интерфейсу PT NAD нужно создать учетную запись пользователя. Перед созданием учетной записи нужно убедиться, что в PT NAD есть роль (см. раздел 10.1) с необходимым для пользователя набором полномочий.

- Чтобы создать учетную запись пользователя:

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

     Откроется страница **Пользователи**.

  2. В панели инструментов нажмите кнопку **Добавить**.

     Откроется окно **Новый пользователь**.

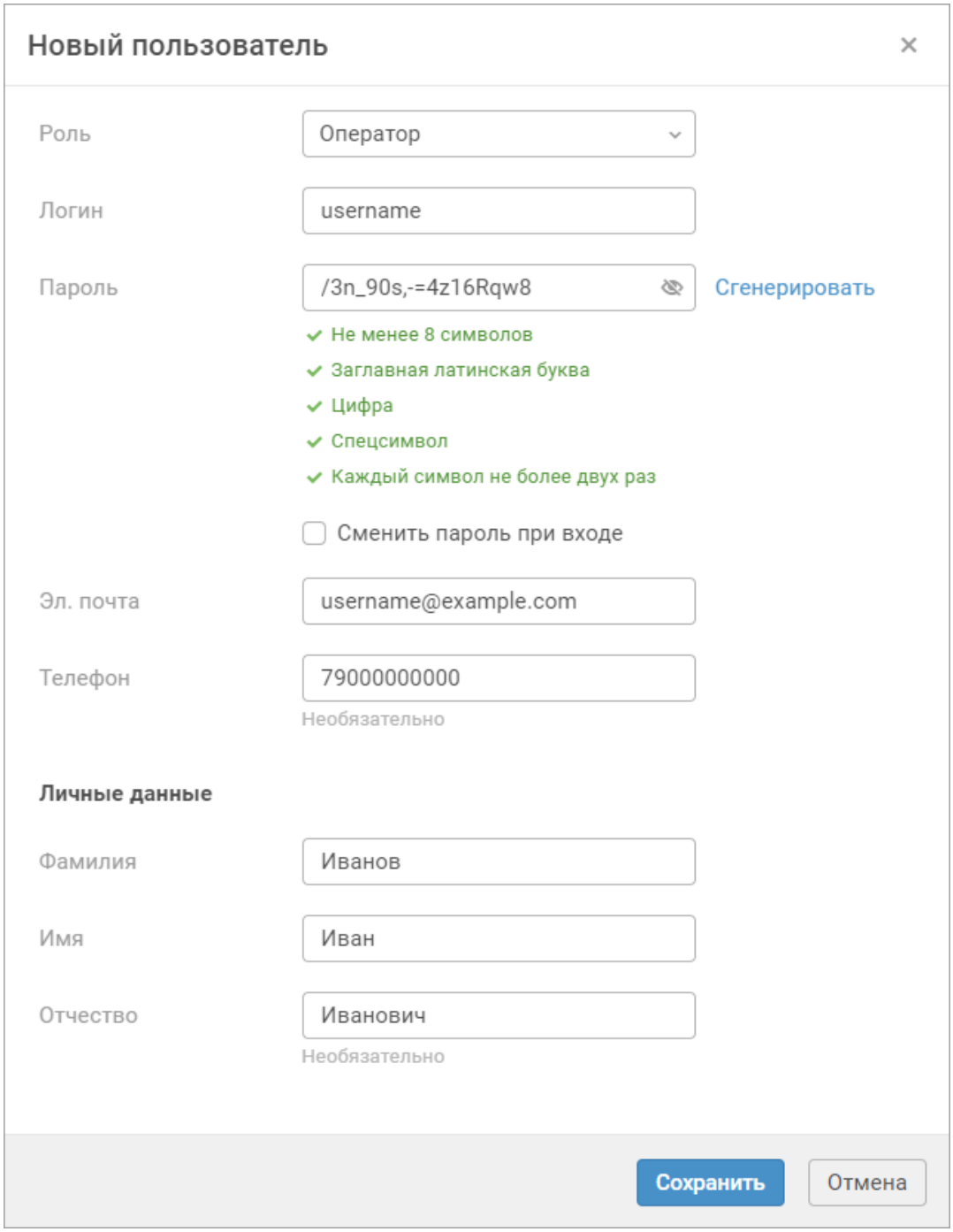

Рисунок 15. Создание учетной записи пользователя

3. В раскрывающемся списке выберите роль (см. раздел 10.1).
4. В поле **Логин** введите логин учетной записи.

   Примечание. Логин должен быть уникальным и может содержать только латинские буквы, цифры и символы «.», «-», «_», «@» и «+».
5. В поле **Пароль** введите пароль для учетной записи пользователя.

Примечание. Пароль должен быть не короче 8 символов и содержать как минимум одну строчную и одну прописную латинскую букву, одну цифру и один спецсимвол. Каждый символ не должен повторяться более двух раз. Вы можете сгенерировать пароль, соответствующий требованиям, по кнопке **Сгенерировать**.

6. Если политика информационной безопасности вашей организации требует, чтобы пользователь сменил пароль при первом входе в продукт, установите флажок.

   При первом входе в PT NAD пользователь не сможет использовать продукт, пока не сменит свой пароль.

7. Введите адрес электронной почты, фамилию и имя пользователя.
8. При необходимости введите отчество и номер телефона пользователя.

   Примечание. Номер телефона может содержать только цифры.

9. Нажмите кнопку **Сохранить**.

Учетная запись пользователя создана.

Вы можете заблокировать созданную учетную запись (см. раздел 10.2.3).

10.2.2. Изменение учетной записи пользователя

Вы можете вносить изменения в учетные записи пользователей. Например, если после изменения должности сотрудника требуется назначить новую роль.

► Чтобы изменить учетную запись пользователя:

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

   Откроется страница **Пользователи**.

2. Выберите учетную запись.

   Примечание. Вы можете найти пользователя, введя в поле поиска любые из его данных.

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

   Откроется окно **Изменение параметров пользователя**.

4. Внесите изменения.
5. Нажмите кнопку **Сохранить**.

Учетная запись пользователя изменена.

Изменения вступят в силу, когда пользователь в следующий раз войдет в продукт.

10.2.3. Блокировка учетной записи пользователя

Вы можете блокировать учетные записи пользователей. После блокировки пользователь не сможет войти в PT NAD.

Примечание. Вы не можете заблокировать собственную учетную запись.

- Чтобы заблокировать учетную запись пользователя:

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

     Откроется страница **Пользователи**.

  2. В строке с учетной записью пользователя включите ее блокировку в столбце **Заблокирован**.

     Примечание. Вы можете найти пользователя, введя в поле поиска любые из его данных.

  Учетная запись заблокирована.

Кроме того, вы можете заблокировать учетную запись пользователя при изменении ее параметров (см. раздел 10.2.2), установив флажок **Заблокирован**.

См. также

Активация учетной записи пользователя (см. раздел 10.2.4)

10.2.4. Активация учетной записи пользователя

Вы можете активировать ранее заблокированные учетные записи пользователей.

- Чтобы активировать учетную запись пользователя:

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

     Откроется страница **Пользователи**.

  2. В строке с учетной записью пользователя выключите ее блокировку в столбце **Заблокирован**.

     Примечание. Вы можете найти пользователя, введя в поле поиска любые из его данных.

  Учетная запись пользователя активирована.

Кроме того, вы можете активировать учетную запись пользователя при изменении ее параметров (см. раздел 10.2.2), сняв флажок **Заблокирован**.

См. также

Блокировка учетной записи пользователя (см. раздел 10.2.3)

10.2.5. Удаление учетной записи пользователя

Примечание. Вы не можете удалить собственную учетную запись.

- Чтобы удалить учетную запись пользователя:

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

     Откроется страница **Пользователи**.

  2. Выберите учетную запись.

     Примечание. Вы можете найти пользователя, введя в поле поиска любые из его данных.

  3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

  Учетная запись пользователя удалена.

10.3. Управление автообновлением правил и репутационных списков

Вы можете управлять автоматическим обновлением правил и репутационных списков. PT NAD получает обновления из базы знаний экспертного центра Positive Technologies (PTSecurity), а также загружает правила Proofpoint ET, если их загрузка была настроена (см. раздел 5.6.4). База знаний PTSecurity также включает в себя актуальную базу геолокации GeoLite2 от MaxMind, которая используется для обогащения сессий информацией о географических данных узлов.

По умолчанию автообновление включено. Его выключение может понадобиться на время настройки локального зеркала обновлений (см. раздел 5.6.6) или при наличии проблем с подключением к серверу обновлений.

- Чтобы включить или выключить автообновление правил и репутационных списков:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. Выберите вкладку **Обновление баз знаний**.
  3. В блоке параметров **Общие параметры обновления** по кнопке **Настроить** откройте окно **Настройка общих параметров обновления**.
  4. Включите или выключите автообновление.
  5. Нажмите кнопку **Сохранить**.
  6. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

На странице **Центр управления** на вкладке **Обновление баз знаний** отображается информация о базах знаний: их версии, названия вендоров, которые их поставляют, даты их выпуска и загрузки в PT NAD.

См. также

Настройка обновления баз знаний (см. раздел 5.6)

10.4. Журнал аудита

В этом разделе приводятся описание функции аудита и инструкции по ее использованию.

Аудит — отслеживание действий пользователей с целью оценки их деятельности или анализа работы продукта в целом. PT NAD записывает в журнал аудита информацию обо всех операциях, которые пользователи выполняют в продукте, кроме перехода между страницами, а также фильтрации, просмотра и поиска данных.

В зависимости от предоставленных прав пользователи продукта могут просматривать журнал аудита, включать или выключать запись событий в журнал и удалять из него записи.

Максимальный объем журнала аудита по умолчанию — 10 тысяч записей. Ротация записей журнала (см. раздел 10.4.5) включена по умолчанию: самые старые записи удаляются автоматически. Если отключить ротацию, то при достижении максимального объема журнала PT NAD приостанавливает запись новых событий и отправляет уведомление пользователю (см. раздел 10.4.6). Чтобы возобновить запись, вам нужно очистить журнал (см. раздел 10.4.4) и включить запись событий (см. раздел 10.4.1).

В этом разделе

Включение и выключение записи событий в журнал аудита (см. раздел 10.4.1)

Просмотр журнала аудита (см. раздел 10.4.2)

Поиск записей в журнале аудита (см. раздел 10.4.3)

Удаление записей из журнала аудита (см. раздел 10.4.4)

Настройка ротации записей журнала аудита (см. раздел 10.4.5)

Настройка уведомлений о заполнении журнала аудита при отключенной ротации (см. раздел 10.4.6)

10.4.1. Включение и выключение записи событий в журнал аудита

Примечание. В зависимости от предоставленных прав возможность управления записью в журнал аудита может быть отключена.

Запись событий в журнал аудита по умолчанию включена.

- Чтобы включить или выключить запись событий в журнал аудита:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Журнал аудита**.

Откроется страница **Журнал аудита**.

2. В верхней левой части страницы включите или выключите запись событий.

Запись событий в журнал аудита включена или выключена.

10.4.2. Просмотр журнала аудита

- Чтобы просмотреть журнал аудита,

  в главном меню нажмите и в раскрывшемся меню выберите пункт **Журнал аудита**.

  Откроется страница **Журнал аудита**.

  Примечание. Вы можете просмотреть информацию о пользователе, который выполнил ту или иную операцию, нажав по ссылке в столбце **Пользователь**. Имена пользователей, учетные записи которых были удалены, написаны серым цветом.

10.4.3. Поиск записей в журнале аудита

- Чтобы найти запись в журнале аудита:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Журнал аудита**.

     Откроется страница **Журнал аудита**.

  2. В поле поиска введите логин учетной записи пользователя, действие, тип объекта, результат или детали.

     Вы можете ввести значение целиком или его часть. Поиск может выполняться по нескольким столбцам одновременно, например «admin modify dga success».

  На странице **Журнал аудита** отобразятся события, удовлетворяющие введенным критериям поиска.

10.4.4. Удаление записей из журнала аудита

Примечание. В зависимости от прав, предоставленных вам администратором, возможность удаления записей из журнала аудита может быть отключена.

- Чтобы удалить записи из журнала аудита:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Журнал аудита**.

     Откроется страница **Журнал аудита**.

  2. В списке событий выберите одну или несколько записей для удаления.

Примечание. Вы можете выбрать несколько событий, удерживая клавишу Ctrl или Shift. Для выбора всех событий нужно выбрать одно из них и нажать комбинацию клавиш Ctrl+A.

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

Записи удалены из журнала аудита.

10.4.5. Настройка ротации записей журнала аудита

Ротация записей журнала аудита включена по умолчанию. Самые старые записи удаляются автоматически, если превышен максимальный объем журнала или максимальный срок хранения записей. Запись новых событий не будет приостанавливаться, и пользователь не будет получать уведомления о заполнении журнала.

- Чтобы настроить ротацию записей журнала аудита:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

   Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

   Дальнейшая настройка выполняется в блоке параметров **Журнал аудита**.

2. В поле **Максимальное количество записей** укажите максимальное количество записей в журнале аудита.

   Значение по умолчанию — `10000`.

3. Если необходимо, отключите или включите ротацию записей журнала аудита.

   Примечание. Если отключить ротацию записей, то необходимо вручную очищать журнал (см. раздел 10.4.4) при его заполнении. Для получения уведомлений о скором заполнении журнала или остановке записи событий нужно настроить уведомления (см. раздел 10.4.6) журнала аудита.

4. В поле **Срок хранения записей (в днях)** укажите максимальное количество дней хранения записей журнала аудита.

   Значение по умолчанию — `30`. Минимальное значение — `1`.

   Примечание. Параметр работает только при включенной ротации журнала аудита.

5. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

   Изменения будут применены через некоторое время.

Ротация журнала аудита настроена.

10.4.6. Настройка уведомлений о заполнении журнала аудита при отключенной ротации

Если вы отключили ротацию журнала аудита (см. раздел 10.4.5), то при достижении максимального объема журнала записи необходимо удалять вручную (см. раздел 10.4.4). В противном случае запись событий в журнал остановится, и ее нужно будет включить (см. раздел 10.4.1).

Уведомления о том, что журнал скоро заполнится или уже заполнен и запись остановлена, отображаются в интерфейсе PT NAD и отправляются по электронной почте (опционально). Кроме того, вы можете настроить запись сообщений о заполнении журнала аудита по протоколу syslog (см. раздел 10.10.2.2).

Уведомления отправляются пользователям с правами на изменение журнала аудита.

> **Примечание.** Уведомления отправляются только при отключенной ротации записей журнала аудита (см. раздел 10.4.5).

- Чтобы настроить уведомления о заполнении журнала аудита:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

     Дальнейшая настройка выполняется в блоке параметров **Журнал аудита**.

  2. В поле **Максимальное количество записей** укажите максимальное количество записей в журнале аудита.

     Значение по умолчанию — `10000`.

  3. Включите или отключите уведомления о заполнении журнала.

     Примечание. Перед включением параметра нужно настроить отправку уведомлений на электронную почту (см. раздел 5.5).

  4. В поле **Пороговое количество записей для уведомления** укажите количество записей в журнале аудита, по превышении которого должно срабатывать уведомление о скором заполнении журнала.

     Значение по умолчанию — `9000`.

  5. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

  Уведомления журнала аудита настроены.

10.5. Управление уведомлениями о несанкционированном доступе

Уведомления о неуспешных попытках входа в интерфейс PT NAD отправляются на электронную почту пользователей, имеющих права на просмотр журнала аудита (см. раздел 10.4). По умолчанию уведомление отправляется, если пользователь три раза подряд ввел неправильный пароль с одним и тем же логином. В соответствии с политикой информационной безопасности вашей организации вы можете изменить количество попыток ввода пароля или отключить уведомления.

Для рассылки уведомлений о неуспешных попытках входа должна быть настроена отправка уведомлений на электронную почту (см. раздел 5.5).

- Чтобы изменить количество попыток или отключить уведомления:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. В блоке параметров **Защита системы** в поле **Попыток входа в систему** укажите количество попыток ввода пароля или `0`, чтобы отключить уведомления.

  3. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

     Изменения будут применены через некоторое время.

10.6. Резервное копирование и восстановление PT NAD

Вы можете создать резервную копию с конфигурацией и базой данных PT NAD. В случае возникновения проблем с физическим сервером вы можете установить PT NAD на работающий сервер и восстановить его конфигурацию и базу данных из ранее созданной резервной копии.

В этом разделе

10.6.1. Создание архива с резервной копией PT NAD

Внимание! Данные, сохраняемые модулем Elasticsearch (сессии, атаки, сетевые взаимодействия), не попадают в резервную копию.

► Чтобы создать резервную копию PT NAD:

1. Перейдите в каталог, в который вам нужно сохранить резервную копию, например:
   ```
   cd /media/usb/backup
   ```
2. Запустите процесс создания резервной копии:
   - для создания резервной копии и конфигурации, и базы данных:
     ```
     sudo /opt/ptsecurity/nad/bin/backup create <Название архива с резервной копией>
     ```
   - для создания резервной копии только конфигурации:
     ```
     sudo /opt/ptsecurity/nad/bin/backup --without-db create <Название файла с резервной копией>
     ```
     Например:
     ```
     sudo /opt/ptsecurity/nad/bin/backup --without-db create backup_28-06-2019.tar.gz
     ```
     Начнется создание резервной копии в виде архива Tar, сжатого по методу gzip. По окончании процесса появится сообщение `Creating backup complete`.

Резервная копия PT NAD создана.

Внимание! Сохраните архив с резервной копией на внешний носитель.

10.6.2. Восстановление PT NAD из резервной копии

Внимание! Восстанавливайте PT NAD из резервной копии, только если она была создана в той же версии продукта. В противном случае работоспособность PT NAD после восстановления не гарантируется.

► Чтобы восстановить PT NAD из резервной копии:

1. Остановите все запущенные службы PT NAD:
   ```
   sudo ptdpictl stop-all
   sudo ptdpictl disable-all
   sudo systemctl stop nad-web-server
   sudo systemctl stop nad-task-server
   sudo systemctl stop ptdpistat
   sudo systemctl stop nad-reporter
   sudo systemctl stop pyfpta
   ```
2. Перейдите в каталог с архивом резервной копии, например:
   ```
   cd /media/usb/backup
   ```
3. Запустите восстановление из резервной копии:
   ```
   sudo /opt/ptsecurity/nad/bin/backup restore <Название файла с резервной копией>
   ```
   Начнется восстановление PT NAD из резервной копии. По окончании процесса появится сообщение `Restoring from backup complete`.
4. Запустите остановленные ранее службы:
   ```
   sudo ptdpictl enable-all
   sudo ptdpictl start-all
   ```

```
sudo systemctl start nad-web-server
sudo systemctl start nad-task-server
sudo systemctl start ptdpistat
sudo systemctl start nad-reporter
sudo systemctl start pyfpta
```

PT NAD восстановлен из резервной копии.

10.7. Настройка периода запуска ретроспективного анализа

Для обнаружения новейших угроз 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 один раз в час. Вы можете изменить период запуска, например для снижения нагрузки на сервер с PT NAD — или для того, чтобы привести этот период в соответствие с политикой информационной безопасности в вашей организации.

- Чтобы настроить период запуска ретроспективного анализа:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:
     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```
     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.
  2. В параметре `retrospective_search_period` укажите новый период запуска ретроспективного анализа в секундах, например:
     ```
     retrospective_search_period: 7200
     ```
  3. Сохраните файл `nad.settings.yaml`.
  4. Перезагрузите модули nad-task-server и nad-web-server:
     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  Период запуска ретроспективного анализа настроен.

См. также

Управление записью syslog-сообщений с результатами ретроспективного анализа (см. раздел 10.10.2.1)

10.8. Настройка лимитов обработки трафика

Вы можете настраивать ограничения для анализа соединений, записи PCAP и обнаружения атак.

В этом разделе

10.8.1. Настройка лимитов анализа соединений

Вы можете настроить ограничения анализа соединений в PT NAD. Ограничения настраиваются при помощи лимитов для конкретных протоколов, по которым передается трафик, или лимитов, общих для всех или нераспознанных протоколов. Если объем данных, переданных в соединении, достигает лимита, PT NAD приостанавливает анализ этого соединения и добавляет флаг PARSE_LIMIT в свойства сессии.

> **Примечание.** По умолчанию лимит настроен для данных, передаваемых только по DHCP, и равен 32 КБ.

Примечание. Значение `0` с единицей измерения (например, `0kb`) снимает соответствующее ограничение.

- Чтобы настроить лимиты анализа соединений:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Если вам нужно настроить лимит для конкретных протоколов, добавьте в любое место в файле строки следующего вида:

     - Если название протокола присутствует в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:
       ```
       ptdpi-logger.yaml.protocols.<Название протокола>.parse-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>
       ```
       Например:
       ```
       ptdpi-logger.yaml.protocols.sip.parse-limit: 10kb
       ptdpi-logger.yaml.protocols.tls.parse-limit: 15kb
       ```
     - Если названия протокола нет в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:
       ```
       ptdpi-logger.yaml.protocols.<Название протокола>: {parse-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>}
       ```

Например:

```
ptdpi-logger.yaml.protocols.mysql: {parse-limit: 10kb}
```

Примечание. Вы можете получить список названий протоколов, выполнив команду `/opt/ptsecurity/dpi/ptdpi --list-app-layer-protos`.

3. Если вам нужно настроить лимит для протоколов, которые PT NAD не может распознать, добавьте в любое место в файле следующую строку:

   ```
   ptdpi-logger.yaml.protocols._undetected_.parse-limit: <Лимит><Единица измерения: kb, mb или gb>
   ```

   Например:

   ```
   ptdpi-logger.yaml.protocols._undetected_.parse-limit: 30kb
   ```

4. Если вам нужно настроить лимит для протоколов, лимиты для которых не были указаны отдельно, добавьте в любое место в файле следующую строку:

   ```
   ptdpi-logger.yaml.protocols._defaults_.parse-limit: <Лимит><Единица измерения: kb, mb или gb>
   ```

   Например:

   ```
   ptdpi-logger.yaml.protocols._defaults_.parse-limit: 40kb
   ```

5. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

6. Перезапустите сенсор:

   ```
   sudo ptdpictl restart
   ```

Лимиты анализа соединений настроены.

10.8.2. Настройка лимитов записи PCAP

Вы можете настроить ограничения записи PCAP в PT NAD, чтобы снизить нагрузку на дисковую подсистему сервера. Ограничения настраиваются при помощи лимитов для конкретных протоколов, по которым передается трафик, или лимитов, общих для всех или нераспознанных протоколов. Если объем данных, переданных в соединении, достигает лимита, PT NAD приостанавливает запись PCAP этого соединения и добавляет флаг PCAP_LIMIT в свойства сессии.

Примечание. Значение `0` с единицей измерения (например, `0kb`) снимает соответствующее ограничение.

- Чтобы настроить лимиты записи PCAP:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```

  2. Если вам нужно настроить лимит для конкретных протоколов, добавьте в любое место в файле строки следующего вида:

     - Если название протокола присутствует в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:

       ```
       ptdpi-logger.yaml.protocols.<Название протокола>.pcap-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>
       ```

Например:

```
ptdpi-logger.yaml.protocols.sip.pcap-limit: 10kb
ptdpi-logger.yaml.protocols.tls.pcap-limit: 15kb
```

- Если названия протокола нет в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:

  ```
  ptdpi-logger.yaml.protocols.<Название протокола>: {pcap-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>}
  ```

  Например:

  ```
  ptdpi-logger.yaml.protocols.mysql: {pcap-limit: 10kb}
  ```

  Примечание. Вы можете получить список названий протоколов, выполнив команду `/opt/ptsecurity/dpi/ptdpi --list-app-layer-protos`.

3. Если вам нужно настроить лимит для протоколов, которые PT NAD не может распознать, добавьте в любое место в файле следующую строку:

   ```
   ptdpi-logger.yaml.protocols._undetected_.pcap-limit: <Лимит><Единица измерения: kb, mb или gb>
   ```

   Например:

   ```
   ptdpi-logger.yaml.protocols._undetected_.pcap-limit: 30kb
   ```

4. Если вам нужно настроить лимит для протоколов, лимиты для которых не были указаны отдельно, добавьте в любое место в файле следующую строку:

   ```
   ptdpi-logger.yaml.protocols._defaults_.pcap-limit: <Лимит><Единица измерения: kb, mb или gb>
   ```

   Например:

   ```
   ptdpi-logger.yaml.protocols._defaults_.pcap-limit: 40kb
   ```

5. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
6. Перезапустите сенсор:

   ```
   sudo ptdpictl restart
   ```

Лимиты записи PCAP настроены.

10.8.3. Настройка лимитов обнаружения атак

Вы можете настроить ограничения обнаружения атак в PT NAD. Ограничения настраиваются при помощи лимитов для конкретных протоколов, по которым передается трафик, или лимитов, общих для всех или нераспознанных протоколов. Если объем данных, переданных в соединении, достигает лимита, PT NAD приостанавливает обнаружение атак в рамках этого соединения и добавляет флаг RULES_DETECT_LIMIT в свойства сессии.

Примечание. Значение `0` с единицей измерения (например, `0kb`) снимает соответствующее ограничение.

- Чтобы настроить лимиты обнаружения атак:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```

  2. Если вам нужно настроить лимит для конкретных протоколов, добавьте в любое место в файле строки следующего вида:

     - Если название протокола присутствует в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:

       ```
       ptdpi-logger.yaml.protocols.<Название протокола>.rules-detect-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>
       ```

       Например:

       ```
       ptdpi-logger.yaml.protocols.sip.rules-detect-limit: 10kb
       ptdpi-logger.yaml.protocols.tls.rules-detect-limit: 15kb
       ```

     - Если названия протокола нет в секции `protocols` файла `/opt/ptsecurity/etc/current/ptdpi-logger.yaml`:

       ```
       ptdpi-logger.yaml.protocols.<Название протокола>: {rules-detect-limit: <Лимит для протокола><Единица измерения: kb, mb или gb>}
       ```

       Например:

       ```
       ptdpi-logger.yaml.protocols.mysql: {rules-detect-limit: 10kb}
       ```

       Примечание. Вы можете получить список названий протоколов, выполнив команду `/opt/ptsecurity/dpi/ptdpi --list-app-layer-protos`.

  3. Если вам нужно настроить лимит для протоколов, которые PT NAD не может распознать, добавьте в любое место в файле следующую строку:

     ```
     ptdpi-logger.yaml.protocols._undetected_.rules-detect-limit: <Лимит><Единица измерения: kb, mb или gb>
     ```

     Например:

     ```
     ptdpi-logger.yaml.protocols._undetected_.rules-detect-limit: 30kb
     ```

  4. Если вам нужно настроить лимит для протоколов, лимиты для которых не были указаны отдельно, добавьте в любое место в файле следующую строку:

     ```
     ptdpi-logger.yaml.protocols._defaults_.rules-detect-limit: <Лимит><Единица измерения: kb, mb или gb>
     ```

     Например:

     ```
     ptdpi-logger.yaml.protocols._defaults_.rules-detect-limit: 40kb
     ```

  5. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

  6. Перезапустите сенсор:

     ```
     sudo ptdpictl restart
     ```

  Лимиты обнаружения атак настроены.

10.9. Изменение ротации данных в потоковых хранилищах

Чтобы избежать переполнения дискового пространства, PT NAD удаляет старые данные из потоковых хранилищ. По умолчанию PCAP-файлы с исходной копией трафика ротируются, когда их объем начинает занимать 90% от доступного дискового пространства, а метаданные трафика хранятся две недели независимо от доступного объема свободного места.

Примечание. В многосерверной конфигурации инструкцию нужно выполнять на основном сервере.

- Чтобы изменить ротацию данных в потоковых хранилищах:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Если нужно изменить максимальное время хранения метаданных трафика, в секции `Elastic settings` укажите новое значение параметра `es_store_days`. Значение задается в днях.
  3. Если нужно изменить процент места в файловой системе, выделенный под хранение PCAP-файлов с исходной копией трафика, в секции `Pcap storage settings` укажите новое значение параметра `pcap_max_used_percent`.
  4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  5. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart-all
     ```

  Ротация данных в потоковых хранилищах изменена.

10.10. Настройка записи и отправки сообщений по протоколу syslog

PT NAD может записывать в системный журнал (syslog):

— информацию об активностях;

— информацию о выявленных атаках;

— информацию об обнаруженных индикаторах компрометации;

— результаты ретроспективного анализа;

— уведомления о заполнении журнала аудита.

Операторы могут включать запись в системный журнал пользовательских уведомлений по фильтрам в параметрах уведомлений в Личном кабинете и при настройке фильтров. Подробная инструкция приведена в разделе «Настройка уведомлений по личному фильтру» в Руководстве оператора. Запись другой информации включается в конфигурационных файлах PT NAD.

Вы можете включить запись сообщений в локальный системный журнал, а также настроить отправку сообщений по протоколу syslog на удаленный сервер. Это может понадобиться для централизованного сбора и анализа событий ИБ в информационной инфраструктуре организации, а также для инвентаризации активов и проверки результативности атак в системах SIEM, в том числе в MaxPatrol SIEM.

В этом разделе

10.10.1. Настройка syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации

В PT NAD есть возможность записи и отправки syslog-сообщений с информацией об атаках, индикаторах компрометации и активностях, обнаруживаемых с помощью системных и общих правил для активностей. По умолчанию syslog-сообщения имеют:

— категорию субъекта 3 (facility — system daemons);

— уровень опасности 6 (severity — informational);

— метку отправителя ptdpi-syslog-notifier.

Вы можете:

— включить запись сообщений в локальный системный журнал;

— настроить отправку сообщений на удаленные серверы;

— изменить категорию субъекта и метку ПО, от имени которого отправляются сообщения;

— настроить генерацию сообщений определенных типов (например, только об обнаруженных индикаторах компрометации или только об атаках).

Перед выполнением инструкции нужно указать адрес веб-интерфейса (см. раздел 5.4) и обеспечить получение syslog-сообщений на удаленном сервере.

- Чтобы настроить syslog-сообщения с информацией об активностях, атаках и индикаторах компрометации:

  1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

2. Выберите вкладку **Средства интеграции**.
3. В блоке параметров **Статусы интеграции** включите syslog.
4. В блоке параметров **Syslog-подключения** по кнопке **Добавить** откройте окно **Добавление syslog-подключения**.
5. В поле **Название подключения** введите произвольное название syslog-подключения.
6. Если вам нужно отправлять syslog-сообщения на удаленный сервер, в поле **Получатель syslog-сообщений** введите протокол UDP (по умолчанию) или TCP, адрес и порт, например `tcp://198.51.100.1:514`.
7. Если вам нужно записывать syslog-сообщения локально, в поле **Получатель syslog-сообщений** укажите сокет домена Unix, например `/dev/log`.
8. Если вам не нужны сообщения с определенной информацией, в параметре **Типы syslog-сообщений** снимите флажки с ненужных типов данных.
9. Если вам нужно изменить стандартную категорию субъекта, в поле **Категория субъекта** укажите числовое или строковое значение необходимой категории субъекта, например `3` или `daemon`.
10. Если вам нужно изменить метку ПО, от имени которого отправляются сообщения, в поле **Метка ПО** измените название метки.
11. Если требуется, чтобы PT NAD отправлял данные об активностях на русском языке, в параметре **Язык данных в syslog-сообщениях** выберите русский язык.
12. Нажмите кнопку **Добавить**.
13. Если необходимо добавить дополнительные подключения с другими параметрами, повторите шаги 4—12.
14. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

    Изменения будут применены через некоторое время.

Syslog-сообщения с информацией об активностях, атаках и индикаторах компрометации настроены.

10.10.2. Настройка syslog-сообщений с результатами ретроспективного анализа и уведомлениями о заполнении журнала аудита

- Чтобы настроить syslog-сообщения с результатами ретроспективного анализа и уведомлениями о заполнении журнала аудита:

  1. Откройте файл `/etc/rsyslog.d/45-ptdpi.conf`:

```
sudo nano /etc/rsyslog.d/45-ptdpi.conf
```

2. Если вам нужно настроить отправку syslog-сообщений на удаленный сервер, раскомментируйте строку 5 и измените значения параметров `target`, `port` и `protocol` на нужные:

   ```
   action(type="omfwd" target="<IP-адрес удаленного сервера>" port="<Порт удаленного сервера>" protocol="<Протокол передачи syslog-сообщений (udp или tcp)>")
   ```

   Например:

   ```
   action(type="omfwd" target="198.51.100.100" port="514" protocol="udp")
   ```

3. Если вам нужно отключить запись сообщений в локальный системный журнал, закомментируйте строку 6:

   ```
   #action(type="omfile" file="/opt/ptsecurity/log/alert.log")
   ```

   Для повторного включения записи в локальный журнал нужно снова закомментировать строку 6.

4. Сохраните изменения в файле `/etc/rsyslog.d/45-ptdpi.conf`.

5. Перезапустите службу rsyslog:

   ```
   systemctl restart rsyslog.service
   ```

Syslog-сообщения настроены. Теперь вам нужно включить запись syslog-сообщений с результатами ретроспективного анализа и о заполнении журнала аудита.

В этом разделе

Управление записью syslog-сообщений с результатами ретроспективного анализа (см. раздел 10.10.2.1)

Управление записью syslog-сообщений о заполнении журнала аудита (см. раздел 10.10.2.2)

10.10.2.1. Управление записью syslog-сообщений с результатами ретроспективного анализа

- Чтобы включить или выключить запись syslog-сообщений с результатами ретроспективного анализа:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. Измените значение параметра `retrospective_notify_syslog` на `true` (если нужно включить запись сообщений) или на `false` (если нужно выключить).

3. Сохраните файл `nad.settings.yaml`.
4. Перезагрузите модули nad-task-server и nad-web-server:

   ```
   sudo systemctl restart nad-task-server.service
   sudo systemctl restart nad-web-server.service
   ```

Запись syslog-сообщений с результатами ретроспективного анализа включена или выключена.

См. также

Настройка периода запуска ретроспективного анализа (см. раздел 10.7)

Формат syslog-сообщений (см. раздел 10.10.3)

10.10.2.2. Управление записью syslog-сообщений о заполнении журнала аудита

Syslog-сообщения о заполнении журнала аудита будут записываться только при отключении ротации журнала аудита (см. раздел 10.4.5).

- Чтобы включить или выключить запись syslog-сообщений о заполнении журнала аудита:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. В секции `Audit settings` раскомментируйте параметр `journal_notify_syslog` и в качестве его значения укажите `true` (если нужно включить запись сообщений) или `false` (если нужно выключить).
  3. Сохраните файл `nad.settings.yaml`.
  4. Перезагрузите модули nad-task-server и nad-web-server:

     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  Запись syslog-сообщений о заполнении журнала аудита включена или выключена.

См. также

Формат syslog-сообщений (см. раздел 10.10.3)

Настройка уведомлений о заполнении журнала аудита при отключенной ротации (см. раздел 10.4.6)

10.10.3. Формат syslog-сообщений

PT NAD генерирует syslog-сообщения в соответствии с RFC 5424. Общий формат сообщения:

```
<Заголовок сообщения>: <Текст сообщения>
```

В этом разделе

10.10.3.1. Формат заголовка syslog-сообщений

Заголовок syslog-сообщения имеет определенный формат в зависимости от типа этого сообщения.

Активности, обнаруженные атаки и индикаторы компрометации

```
<Значение приоритета (PRI)><Время генерации сообщения> <Название узла, где было
сгенерировано сообщение> <Метка ПО, сгенерировавшего сообщение>: syslog_notifier.<Тип
сообщения>: <Сообщение>
```

Например:

```
<30>Apr 20 00:31:07 server1.example.com ptdpi-syslog-notifier: syslog_notifier.alert:
{"flow_id": "gB7a72ST2kHAfb8rhxYda3", "flow_url": "https:// server1.example.com/#/
sessions/list/gB7a72ST2kHAfb8rhxYda2", "type": "alert", "ts_start":
"2023-04-19T21:31:06.344699", "src": {"ip": "198.51.100.0.205", "mac":
"00-00-5E-00-53-11"}, "dst": {"ip": "198.51.100.0.193", "mac": "00-00-5E-00-53-2B"},
"alert": {"s_id": 19000003, "s_msg": "test"}
```

По умолчанию при генерации заголовков PT NAD использует следующие значения:

- PRI — `30` (рассчитывается с использованием facility `3` и severity `6`);
- метка ПО — `ptdpi-syslog-notifier`;
- тип сообщения — `detection` для сообщений об активностях, `alert` для сообщений об атаках и `reputation` для сообщений об индикаторах компрометации;
- сообщение — набор параметров сообщения в формате JSON.

Вы можете изменить значение facility и метку ПО (см. раздел 10.10.1). Остальные параметры изменить нельзя.

Результаты ретроспективного анализа и уведомления о заполнении журнала аудита

```
<Значение приоритета (PRI)><Время генерации сообщения> <Название узла, где было
сгенерировано сообщение> <Название процесса, сгенерировавшего сообщение>[<PID
процесса, сгенерировавшего сообщение>]
```

Например:

```
<13>Oct 22 16:15:25 nad-host nad-event[2677]
```

Примечание. За генерацию сообщений о срабатывании правил отвечает процесс ptdpi, остальных сообщений — nad-event.

10.10.3.2. Формат тела syslog-сообщений

Формат тела syslog-сообщения зависит от типа этого сообщения.

Активность

Тело syslog-сообщения с информацией об активности записывается в формате JSON и имеет следующую структуру:

```
{
  "id": "Integer",
  "detection_url": "String",
  "identity_key": "String",
  "criticality": "Integer",
  "created": "String",
  "updated": "String",
  "start": "String",
  "end": "String",
  "duration": "String",
  "title": "String",
  "type": {
    "id": "String",
    "name": "String",
    "text": "String",
    "description": "String",
    "recommendation": "String",
  },
  "filter": "String",
  "params": [Array]
}
```

Таблица 3. Поля в syslog-сообщении об активности

Поле	Обязательное	Описание
id	Да	Идентификатор карточки активности
detection_url	Да	Ссылка для перехода к карточке активности
identity_key	Да	Идентификатор активности

Поле	Обязательное	Описание
criticality	Да	Уровень опасности активности. Возможные значения: — high — высокий; — medium — средний; — low — низкий
created	Да	Дата и время обнаружения активности в формате гггг-ММ-ддТчч:мм:сс.cccccc
updated	Да	Дата и время последнего обновления информации об активности в формате гггг-ММ-ддТчч:мм:сс.cccccc
start	Да	Дата и время первой сессии, в которой замечена активность в формате гггг-ММ-ддТчч:мм:сс.cccccc
end	Да	Дата и время последней сессии, в которой замечена активность в формате гггг-ММ-ддТчч:мм:сс.cccccc
duration	Да	Продолжительность активности (разница между последней и первой сессиями) в формате дд чч:мм:сс
title	Нет	Название активности
type	Да	Набор параметров по типу активности
type → id	Да	Идентификатор типа активности
type → name	Нет	Название типа активности
type → text	Нет	Сообщение об активности
type → description	Нет	Описание активности
type → recommendation	Нет	Рекомендации для активности
filter	Нет	Условия фильтрации трафика при переходе из карточки активности к дашборду
params	Нет	Набор параметров типа активности. Уникален для каждого типа

Для полей name, text, description и recommendation значения сохраняются на языке, указанном при настройке syslog-сообщений (см. раздел 10.10.1).

Например:

```
{
  "id": 1517,
  "detection_url": "https://localhost/#/detections/main/1517",
  "identity_key": "user_notification_12",
```

```
  "criticality": "low",
  "created": "2023-06-16T16:15:53.733922",
  "updated": "2023-06-20T09:05:48.188108",
  "start": "2023-06-16T15:45:49",
  "end": "2023-06-20T09:04:40",
  "duration": "3 17:18:51",
  "type": {
    "id": "user_notifications",
    "name": "Уведомление по пользовательскому фильтру",
    "text": "Сессий больше 0 за 00:10:00 по фильтру example"
  },
  "title": "Сессий больше 0 за 10 минут",
  "filter": "proto == \"tcp\" && app_proto == \"tls\"",
  "params": {
    "op": "gt",
    "val": 0,
    "metric": "connections_count",
    "interval": "00:10:00",
    "filter_name": "example",
    "interval_unit": "minute"
  }
}
```


Атака

Тело syslog-сообщения с информацией об обнаруженной атаке записывается в формате JSON и имеет следующую структуру:


```
{
  "flow_id": "String",
  "flow_url": "String",
  "type": "String",
  "ts_start": "String",
  "proto": "String",
  "app_proto": "String",
  "src": {
    "ip": "String",
    "port": Integer,
    "mac": "String",
    "host_id": "String",
    "dns": "String",
    "geo": {
      "location": [Array of strings],
      "country": "String",
      "city": "String",
      "asn": "String",
      "org": "String"
```

```
    }
  },
  "dst": {
    <Тот же набор полей, что и в "src">
  },
  "alert": {
    "s_id": Integer,
    "s_rev": Integer,
    "s_msg": "String",
    "s_cls": "String",
    "s_pr": Integer,
    "s_g": Integer,
    "ts": "String",
    "tx_id": Integer,
    "to_server": Boolean,
    "to_client": Boolean,
    "payload": "String"
  }
}
```

Таблица 4. Поля в syslog-сообщении об атаке

Поле	Обязательное	Описание
`flow_id`	Да	Идентификатор сессии
`flow_url`	Да	Ссылка на карточку сессии, в которой PT NAD обнаружил атаку
`type`	Да	Тип сообщения. В сообщении этого типа всегда `alert`
`ts_start`	Да	Время начала сессии в формате гггг-ММ-ддТчч:мм:сс.сс-cccc
`proto`	Да	Транспортный протокол
`app_proto`	Да	Прикладной протокол
`src`	Да	Данные об отправителе
`dst`	Да	Данные о получателе
`src` → `ip`, `dst` → `ip`	Да	IP-адрес
`src` → `port`, `dst` → `port`	Да	Порт
`src` → `mac`, `dst` → `mac`	Да	MAC-адрес

Поле	Обяза-тельное	Описание
src → host_id, dst → host_id	Нет	Идентификатор узла
src → dns, dst → dns	Нет	Доменное имя
src → geo, dst → geo	Нет	Географические данные узла
geo → location	Да	Географические координаты
geo → country	Да	Двухбуквенный код страны согласно ISO 3166-1
geo → asn	Да	Уникальный номер автономной системы (autonomous system number), присвоенный узлу
geo → city	Да	Город
geo → org	Да	Организация
alert	Да	Информация о сработавшем правиле и атаке
alert → s_id	Да	Идентификатор правила
alert → s_rev	Да	Ревизия правила
alert → s_msg	Да	Название атаки
alert → s_cls	Нет	Класс атаки
alert → _pr	Нет	Числовое обозначение уровня опасности атаки. Возможные значения: — 1 — высокий; — 2 — средний; — 3 — низкий; — 4 — другие события
alert → s_g	Нет	Групповой идентификатор правила
alert → ts	Нет	Время обнаружения атаки в формате гггг-ММ-ддТчч:мм:сс.cccccc
alert → tx_id	Нет	Порядковый номер транзакции сессии, которая вызвала срабатывание. Отсчет транзакций начинается с нуля
alert → to_server	Нет	Была ли атака направлена в сторону получателя
alert → to_client	Нет	Была ли атака направлена в сторону отправителя
alert → payload	Нет	Сегмент трафика, который вызвал срабатывание

Пример сообщения об атаке:


```
{
  "flow_id": "xxxxxxxxxxxxxxx",
  "flow_url": "https://nad.example/#/sessions/list/xxxxxxxxxxxx?
sources=2&from=1664765281166&to=1664779681182",
  "type": "alert",
  "ts_start": "2022-10-03T02:48:01.166738",
  "proto": "tcp",
  "app_proto": "http",
  "src": {
    "ip": "192.0.2.1",
    "port": 33210,
    "mac": "00:00:5E:00:53:2B",
    "host_id": "H9",
    "geo": {}
  },
  "dst": {
    "ip": "203.0.113.1",
    "port": 80,
    "mac": "00:00:5E:00:53:11",
    "dns": "example.net",
    "geo": {
      "location": [
        55.7482,
        37.6177
      ],
      "country": "RU",
      "city": "Moscow"
    }
  },
  "alert": {
    "s_id": 1234567890,
    "s_rev": 1,
    "s_msg": "Attack",
    "s_cls": "Unknown Traffic",
    "s_pr": 3,
    "s_g": 1,
    "ts": "2022-10-03T02:48:01.181376",
    "tx_id": 0,
    "to_server": true,
    "payload": ""
  }
}
```

Индикаторы компрометации

Тело syslog-сообщения с информацией об индикаторах компрометации записывается в формате JSON и имеет следующую структуру:

```
{
  "flow_id": "String",
  "flow_url": "String",
  "type": "String",
  "ts_start": "String",
  "proto": "String",
  "app_proto": "String",
  "src": {
    "ip": "String",
    "port": Integer,
    "mac": "String",
    "host_id": "String",
    "dns": "String",
    "geo": {
      "location": [Array of strings],
      "country": "String",
      "city": "String",
      "asn": "String",
      "org": "String"
    }
  },
  "dst": {
    <Тот же набор полей, что и в "src">
  },
  "rpt": [
    {
      "where": "String",
      "id": Integer,
      "type": "String",
      "cat": "String",
      "color": "String",
      "host": "String",
      "ip": "String",
      "md5": "String",
      "url": "String",
      "ref": "String",
      "sandbox": Boolean,
      "verdict": "String"
    },
    {
      ...
    }
```

```
    ]
  }
```

Таблица 5. Поля в syslog-сообщении об индикаторах компрометации

Поле	Обязательное	Описание
`flow_id`	Да	Идентификатор сессии
`flow_url`	Да	Ссылка на карточку сессии, в которой PT NAD обнаружил индикаторы компрометации
`type`	Да	Тип сообщения. В сообщении этого типа всегда `reputation`
`ts_start`	Да	Время начала сессии в формате гггг-ММ-ддТчч:мм:сс.сс-cccc
`proto`	Да	Транспортный протокол
`app_proto`	Да	Прикладной протокол
`src`	Да	Данные об отправителе
`dst`	Да	Данные о получателе
`src` → `ip`, `dst` → `ip`	Да	IP-адрес
`src` → `port`, `dst` → `port`	Да	Порт
`src` → `mac`, `dst` → `mac`	Да	MAC-адрес
`src` → `host_id`, `dst` → `host_id`	Нет	Идентификатор узла
`src` → `dns`, `dst` → `dns`	Нет	Доменное имя
`src` → `geo`, `dst` → `geo`	Нет	Географические данные узла
`geo` → `location`	Да	Географические координаты
`geo` → `country`	Да	Двухбуквенный код страны согласно ISO 3166-1
`geo` → `asn`	Да	Уникальный номер автономной системы (autonomous system number), присвоенный узлу
`geo` → `city`	Да	Город
`geo` → `org`	Да	Организация
`rpt`	Да	Информация об обнаруженных индикаторах компрометации

Поле	Обязательное	Описание
`rpt` → `where`	Да	Где был обнаружен индикатор компрометации. Возможные значения: — `dns` — сообщение протокола DNS; — `files` — хеш-сумма MD5; — `flow.dst` — трафик от получателя; — `flow.src` — трафик от отправителя; — `http` — сообщения протокола HTTP; — `http.x-f-for` — поле X-Forwarded-For в заголовке HTTP-сообщения; — `tls.sni` — Server Name Indication (SNI) в протоколе TLS
`rpt` → `id`	Да	Идентификатор объекта соединения, в котором был обнаружен индикатор компрометации: — В случае HTTP-, TLS- и DNS-соединений — порядковый номер транзакции сессии, в которой был обнаружен индикатор компрометации (отсчет транзакций начинается с нуля). — Если индикатор компрометации сработал на файл — порядковый номер этого файла в сессии (отсчет файлов начинается с нуля). — В остальных случаях — `0`
`rpt` → `type`	Да	Способ, который был применен для обнаружения индикатора компрометации. Возможные значения: — `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 Sandbox или PT MultiScanner определил файл, переданный в ходе сессии, как опасный (при настроенной интеграции с этими продуктами)

Поле	Обязательное	Описание
`rpt → cat`	Да	Название репутационного списка, с помощью которого был обнаружен индикатор компрометации, или тип вредоносного ПО, обнаруженного PT Sandbox или PT MultiScanner (при настроенной интеграции с этими продуктами)
`rpt → color`	Да	Числовое обозначение цвета репутационного списка. Возможные значения: — `0` — белый; — `1` — красный; — `2` — черный; — `3` — серый; — `4` — желтый; — `5` — синий; — `6` — зеленый; — `7` — оранжевый
`rpt → host`	Нет	Доменное имя
`rpt → ip`	Нет	IP-адрес
`rpt → md5`	Нет	Хеш-сумма MD5
`rpt → url`	Нет	URL
`rpt → ref`	Нет	Ссылка на карточку файла в PT Sandbox или PT MultiScanner, если индикатор компрометации был обнаружен при помощи этих продуктов
`rpt → sandbox`	Нет	Было ли выявлено опасное поведение файла в ходе поведенческого анализа (при настроенной интеграции с PT MultiScanner версии ниже 3.0 или с PT Sandbox): — `true` — выявлено опасное поведение файла; — `false` — опасное поведение не выявлено или поведенческий анализ не проводился
`rpt → verdict`	Нет	Семейство вредоносного ПО, к которому принадлежит файл (при настроенной интеграции с PT MultiScanner версии ниже 3.0 или с PT Sandbox)

Пример сообщения с информацией об обнаруженных индикаторах компрометации:

```
{
  "flow_id": "xxxxxxxxxxxxxxx",
```

```
  "flow_url": "https://nad.example/#/sessions/list/xxxxxxxxxxxxx?
sources=2&from=1664765281166&to=1664779681182",
  "type": "reputation",
  "ts_start": "2022-10-03T02:48:01.166738",
  "proto": "tcp",
  "app_proto": "http",
  "src": {
    "ip": "192.0.2.1",
    "port": 33210,
    "mac": "00:00:5E:00:53:2B",
    "host_id": "H9",
    "geo": {}
  },
  "dst": {
    "ip": "203.0.113.1",
    "port": 80,
    "mac": "00:00:5E:00:53:11",
    "dns": "example.net",
    "geo": {
      "location": [
        55.7482,
        37.6177
      ],
      "country": "RU",
      "city": "Moscow"
    }
  },
  "rpt": [
    {
      "cat": "ip_mask",
      "color": "1",
      "id": 0,
      "ip": "192.0.2.143",
      "type": "ip",
      "where": "flow.src"
    },
    {
      "cat": "ip_mask",
      "color": "1",
      "id": 0,
      "ip": "203.0.113.45",
      "type": "ip",
      "where": "flow.dst"
    }
  ]
}
```

Ретроспективный анализ

```
Retrospective analysis based on reputation list "<Название репутационного списка>"
started at <Начало ретроспективного анализа> and found <Количество сессий> sessions
for period from <Начало первой сессии> to <Завершение последней сессии>
```

Например:

```
Retrospective analysis based on reputation list "list_a" started at
2020-10-22T12:42:56.180015 and found 158922 sessions for period from
2020-10-20T00:02:27.530905Z to 2020-10-22T12:36:29.896237Z
```

Журнал аудита

При приближении к пороговому значению заполненности журнала аудита PT NAD генерирует сообщение:

```
Log is 93% full
```

При заполнении журнала аудита:

```
Log is full. Audit is stopped.
```

10.11. Настройка отправки сообщений при помощи механизма webhook

Поддержка механизма webhook в PT NAD позволяет отправлять в сторонние системы сообщения об атаках, индикаторах компрометации и активностях, обнаруживаемых при помощи системных и общих правил для активностей.

Перед выполнением инструкции нужно указать адрес веб-интерфейса (см. раздел 5.4).

- Чтобы настроить отправку сообщений при помощи механизма webhook:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**. По умолчанию выбрана вкладка **Общие параметры**.

  2. Выберите вкладку **Средства интеграции**.
  3. В блоке параметров **Статусы интеграции** включите webhook.
  4. В блоке параметров **Webhook-подключения** по кнопке **Добавить** откройте окно **Добавление webhook-подключения**.
  5. В поле **Название подключения** введите произвольное название webhook-подключения.
  6. В поле **URL для приема сообщений** укажите URL на удаленном сервере для приема сообщений при помощи механизма webhook.

7. Если вам не нужны сообщения с определенной информацией, в параметре **Типы сообщений** снимите флажки.
8. Если PT NAD не должен проверять сертификат удаленного сервера, отключите проверку сертификата.
9. Если необходимо изменить стандартный тайм-аут запроса на подключение, укажите новый тайм-аут в поле **Тайм-аут запроса (в секундах)**.
10. Если требуется, чтобы PT NAD отправлял данные об активностях на русском языке, в параметре **Язык сообщений** выберите русский язык.
11. Нажмите кнопку **Добавить**.
12. Если необходимо добавить дополнительные подключения с другими параметрами, повторите шаги 4—11.
13. Нажмите кнопку **Применить все** и в открывшемся окне подтвердите применение.

    Изменения будут применены через некоторое время.

Отправка сообщений при помощи механизма webhook настроена.

Теперь вам нужно настроить стороннюю систему для приема и обработки сообщений, получаемых от PT NAD. В ответ на успешное получение сообщения от PT NAD система должна прислать ответное сообщение с любым содержимым и кодом ниже 400, например 200. Для отладки отправки вы можете воспользоваться файлом `/opt/ptsecurity/log/ptdpi-notifier.log`. При успешной отправке сообщения PT NAD генерирует в этот файл запись вида `<Название подключения>: sent successfully`, например `remote1: sent successfully`.

10.12. Управление ссылками на внешние аналитические ресурсы

Операторы могут просматривать информацию об IP-адресах, доменах и файлах на внешних ресурсах (например, VirusTotal или Censys). Переход к внешним ресурсам осуществляется по ссылкам на тех страницах PT NAD, где отображаются эти IP-адреса, домены и файлы.

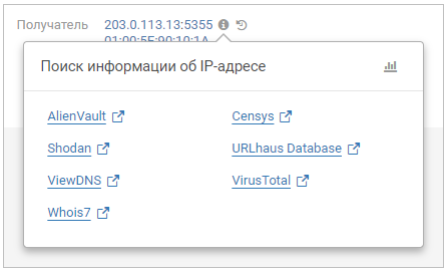

Рисунок 16. Ссылки на внешние аналитические ресурсы

Вы можете добавлять и удалять свои ссылки на внешние ресурсы, временно отключать пользовательские и предустановленные ссылки, а также изменять формат их URL.

В этом разделе

10.12.1. Добавление ссылок на внешние аналитические ресурсы

В дополнение к установленным по умолчанию ссылкам вы можете добавлять свои.

- Чтобы добавить пользовательские ссылки на внешние ресурсы:

  1. Создайте YAML-файл с параметрами ссылок на новые внешние ресурсы.

     Ссылку на каждый добавляемый ресурс нужно настраивать в виде блока параметров:

     ```
     <Название ресурса>:
       enabled: true
       resources:
       - type: <Тип объекта>
         url: <Формат URL>
       - type: <Тип объекта>
         url: <Формат URL>
       ...
     ```

     Допустимые значения для типа объекта: `ipv4`, `ipv6`, `dns`, `md5` и `sha256`.

     В формате URL для подстановки значений нужно использовать переменную `{VALUE}`.

     Например:

     ```
     example.com:
       enabled: true
       resources:
       - type: ipv4
         url: https://example.com/ipv4/{VALUE}
     example.net:
       enabled: true
       resources:
       - type: md5
         url: https://example.net/check?type=file&hash={VALUE}
       - type: dns
         url: https://example.net/check?type=domain&addr={VALUE}
     ```

  2. На узле с веб-интерфейсом загрузите созданный файл в PT NAD:

     ```
     sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path <Путь к файлу с конфигурацией>
     ```

Например:

```
sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path /home/user/custom_links.yaml
```

Появится сообщение `Inserted <Количество добавленных ссылок> external resources`.

Пользовательские ссылки на внешние ресурсы добавлены.

Внимание! Не удаляйте созданный конфигурационный файл. Он может пригодиться для изменения пользовательских ссылок.

Для удаления пользовательских ссылок нужно сбросить конфигурацию (см. раздел 10.12.4).

10.12.2. Отключение и включение ссылок на внешние аналитические ресурсы

Вы можете отключать ссылки на определенные внешние аналитические ресурсы, например, если эти ресурсы временно не работают. После возобновления работы ресурсов отключенные ссылки можно включить.

- Чтобы отключить или включить ссылки на внешние ресурсы:

1. Откройте YAML-файл с параметрами пользовательских ссылок (см. раздел 10.12.1).
2. В блоках со ссылками, которые нужно отключить или включить, смените значение параметра `enabled` на `false` (ссылка выключена) или `true` (ссылка включена).

   Например:

   ```
   example.com:
     enabled: false
     resources:
     - type: ipv4
       url: https://example.com/ipv4/{VALUE}
   example.net:
     enabled: false
     resources:
     - type: md5
       url: https://example.net/check?type=file&hash={VALUE}
     - type: dns
       url: https://example.net/check?type=domain&addr={VALUE}
   ...
   ```

3. Если вам нужно отключить одну или несколько предустановленных ссылок, скопируйте блоки с параметрами этих ссылок из файла `/opt/ptsecurity/data/nad/nad.external_resources.yaml` в файл с пользовательскими ссылками и аналогично измените значение параметра `enabled` на `false`.

   Например:

   ```
   <Блоки с параметрами пользовательских ссылок>
   Shodan:
   ```

```
  enabled: false
  resources:
  - type: ipv4
    url: https://www.shodan.io/host/{VALUE}
```

Внимание! Не изменяйте файл `/opt/ptsecurity/data/nad/nad.external_resources.yaml`.

4. Сохраните изменения в файле конфигурации ссылок.
5. На узле с веб-интерфейсом загрузите обновленный файл в PT NAD:

   ```
   sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path <Путь к файлу с конфигурацией>
   ```

   Например:

   ```
   sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path /home/user/custom_links.yaml
   ```

   Появится сообщение `Updated <Количество обновленных ссылок> external resources`.

10.12.3. Изменение формата URL в ссылках на внешние аналитические ресурсы

Если на внешнем ресурсе изменился формат адресации веб-страниц и ссылки в PT NAD перестали работать, вам нужно исправить формат URL в конфигурации продукта.

- Чтобы изменить формат URL в ссылках на внешние аналитические ресурсы:

  1. Откройте YAML-файл с параметрами пользовательских ссылок (см. раздел 10.12.1).
  2. В блоках со ссылками, формат URL которых нужно изменить, исправьте значения в параметрах `resources` → `url`.

     Например:

     ```
     example.com:
       enabled: true
       resources:
       - type: ipv4
         url: <Исправленный формат URL>
     example.net:
       enabled: true
       resources:
       - type: md5
         url: <Исправленный формат URL>
       - type: dns
         url: <Старый формат URL>
     ...
     ```

3. Если вам нужно изменить формат URL в предустановленных ссылках, скопируйте блоки с параметрами этих ссылок из файла `/opt/ptsecurity/data/nad/nad.external_resources.yaml` в файл с пользовательскими ссылками и аналогично исправьте значения в параметрах `resources` → `url`.

   Например:

   ```
   <Блоки с параметрами пользовательских ссылок>
   MalShare:
     enabled: true
     resources:
     - type: md5
       url: <Исправленный формат URL>
   ```

   Внимание! Не изменяйте файл `/opt/ptsecurity/data/nad/nad.external_resources.yaml`.

4. Сохраните изменения в файле конфигурации ссылок.
5. На узле с веб-интерфейсом загрузите обновленный файл в PT NAD:

   ```
   sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path <Путь к файлу с конфигурацией>
   ```

   Например:

   ```
   sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -f / --file-path /home/user/custom_links.yaml
   ```

   Появится сообщение `Updated <Количество обновленных ссылок> external resources`.

Формат URL в ссылках на внешние аналитические ресурсы изменен.

10.12.4. Сброс конфигурации ссылок на внешние аналитические ресурсы

Вы можете отменить все пользовательские изменения в конфигурации ссылок на внешние аналитические ресурсы. Пользовательские ссылки будут удалены, параметры предустановленных ссылок возвращены к значениям по умолчанию.

- Чтобы сбросить конфигурацию ссылок на внешние аналитические ресурсы,

  на узле с веб-интерфейсом выполните команду:

  ```
  sudo /opt/ptsecurity/nad/bin/manage external_resources upsert -r
  ```

  Появится сообщение о количестве обновленных, добавленных и удаленных ссылок.

Конфигурация ссылок на внешние аналитические ресурсы сброшена.

11. Диагностика и устранение неисправностей

В этом разделе описываются возможные проблемы в работе PT NAD, варианты их решения, а также приводится инструкция по сбору файлов журналов для их отправки в службу технической поддержки.

В этом разделе

11.1. Просмотр версий компонентов PT NAD

Вы можете просмотреть версии установленного в организации экземпляра PT NAD и отдельных его компонентов. Эта информация может понадобиться при обращении в службу технической поддержки Positive Technologies.

- Чтобы просмотреть версии компонентов PT NAD:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**.

  2. Выберите вкладку **О системе**.

     На странице отобразятся версии PT NAD и его компонентов.

     Примечание. Версию PT NAD можно также узнать, нажав в главном меню.

См. также

Архитектура и алгоритм работы PT NAD (см. раздел 2.2)

11.2. Скачивание системных журналов для отправки в техническую поддержку

Если вам не удалось решить проблему в работе продукта самостоятельно, вы можете скачать системные журналы PT NAD и отправить их в службу технической поддержки Positive Technologies для анализа.

- Чтобы скачать системные журналы,

  в главном меню нажмите на индикатор состояния продукта и во всплывающем окне нажмите ссылку **Скачать системные журналы**.

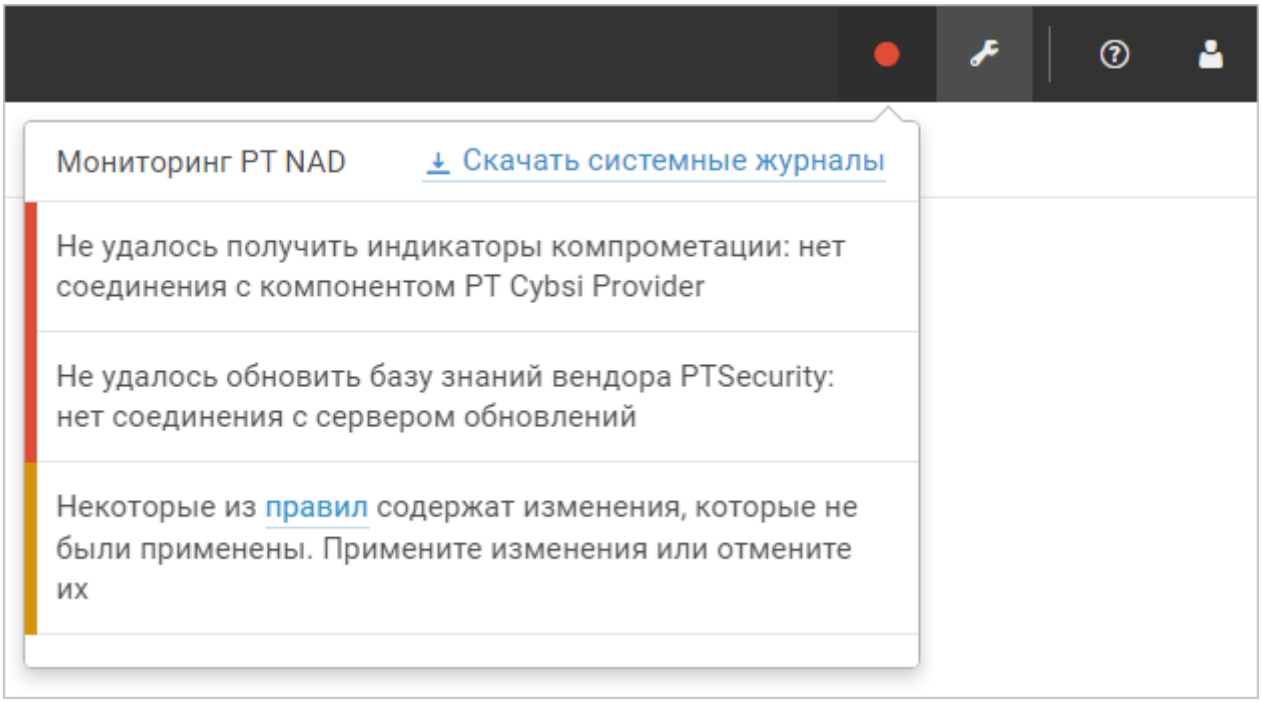

Рисунок 17. Скачивание журналов PT NAD

PT NAD начнет собирать файлы журналов продукта. Этот процесс может занять несколько минут в зависимости от общего размера файлов журналов, а также от аппаратных ресурсов сервера или виртуальной машины с установленным PT NAD. По окончании сборки архив `logs_<Название узла>_ГГГГММДД_ччмм.zip` будет сохранен на вашем компьютере (время в названии архива — в UTC).

11.3. Устранение проблем с лицензией

В этом разделе приводятся описания ошибок, связанных с лицензированием продукта (см. раздел 4), и даются инструкции по их устранению.

В этом разделе

11.3.1. Устранение ошибки «В системе нет лицензии»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «В системе нет лицензии».

Возможные причины

Лицензия не была активирована после установки PT NAD.

После установки PT NAD нужно активировать лицензию, приобретенную вашей организацией. Для этого нужно загрузить файл лицензии `license-access-token.key` в продукт. Вы можете найти этот файл на установочном диске из комплекта поставки или в электронном письме, поступившем на адрес, указанный при заказе лицензии.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что с основного сервера PT NAD разрешен доступ по HTTPS к поддомену update [сайта Positive Technologies]:

     ```
     wget -Sq -O /dev/null https://update.ptsecurity.com/test
     ```

     Результат выполнения команды будет начинаться со строки `HTTP/1.1 200 OK`.

  2. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Центр управления**.

     Откроется страница **Центр управления**.

  3. Выберите вкладку **Лицензия**.

  4. Нажмите кнопку **Добавить**.

     Откроется окно **Добавление лицензии**.

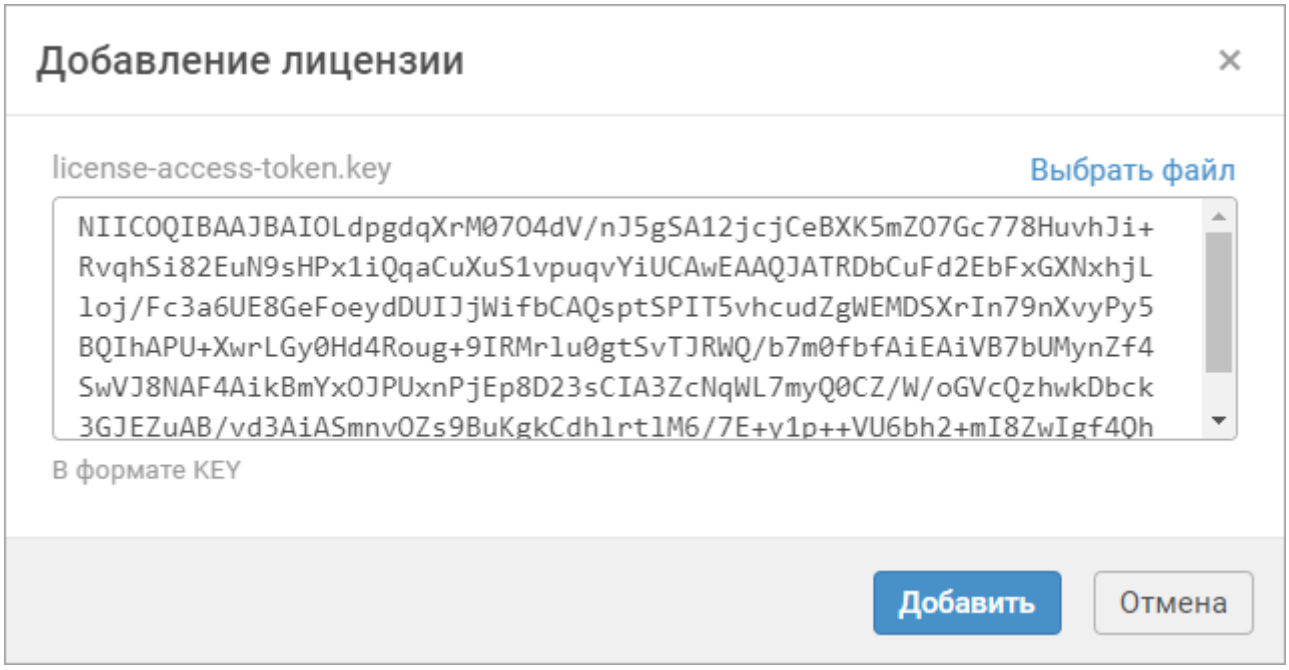

Рисунок 18. Добавление лицензии

5. По ссылке **Выбрать файл** выберите файл лицензии на своем компьютере.

   В поле появится содержимое файла лицензии.

6. Нажмите кнопку **Добавить**.

   На странице отобразится информация об активированной лицензии.

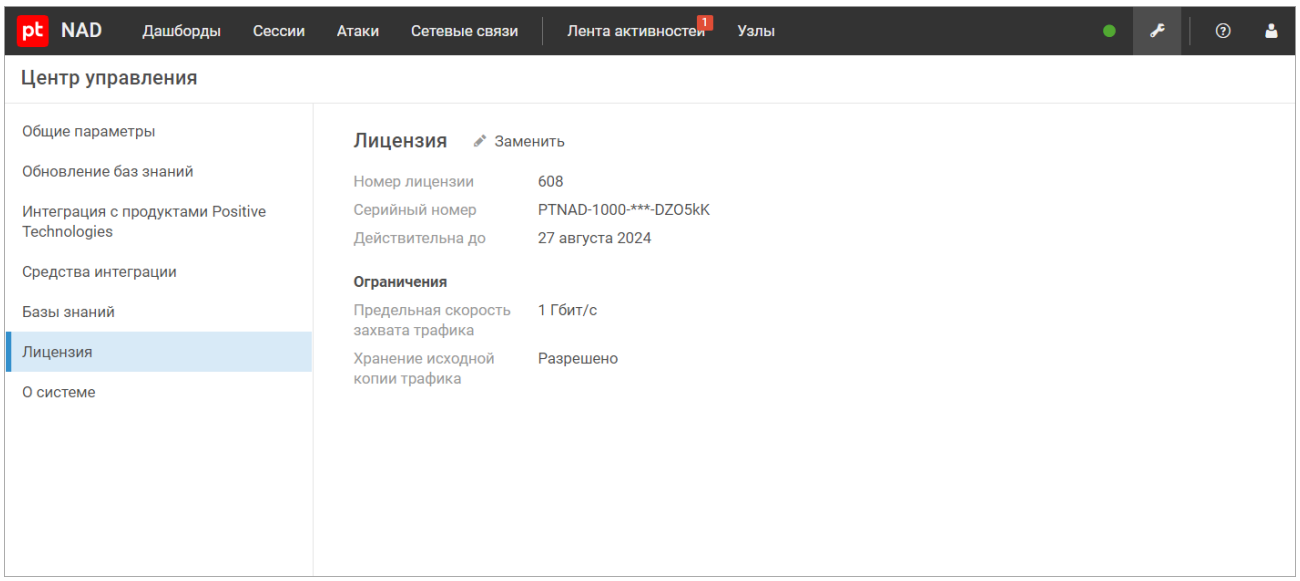

Рисунок 19. Информация о лицензии

См. также

Лицензирование (см. раздел 4)

11.3.2. Устранение ошибки «Истек срок действия лицензии»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Истек срок действия лицензии».

Возможные причины

Истек срок действия лицензии, указанный при ее заказе.

Решение

- Чтобы решить проблему:

  1. Обратитесь в техническую поддержку с просьбой продлить срок действия лицензии.
  2. Если техническая поддержка прислала вам новый файл лицензии, замените ее в интерфейсе (см. раздел 9).

См. также

Лицензирование (см. раздел 4)

11.3.3. Устранение ошибки «Срок действия лицензии истекает»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Срок действия лицензии истекает <Время до истечения срока>».

Возможные причины

Срок действия лицензии, указанный при ее заказе, скоро истекает.

Решение

- Чтобы решить проблему:

  1. Обратитесь в техническую поддержку с просьбой продлить срок действия лицензии.
  2. Если техническая поддержка прислала вам новый файл лицензии, замените ее в интерфейсе (см. раздел 9).

См. также

Лицензирование (см. раздел 4)

11.4. Устранение проблем с обновлением базы знаний

В этом разделе приводятся описания ошибок, связанных с обновлением базы списка правил и репутационных списков, и даются инструкции по устранению этих ошибок.

В этом разделе

Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора> до версии <Номер версии>» (см. раздел 11.4.1)

Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>» (см. раздел 11.4.2)

Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>: недействительный лицензионный ключ» (см. раздел 11.4.3)

Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>: нет соединения с сервером обновлений» (см. раздел 11.4.4)

Устранение ошибки «Не удалось получить индикаторы компрометации: некорректный токен PT Cybsi Provider» (см. раздел 11.4.5)

Устранение ошибки «Не удалось получить индикаторы компрометации: нет соединения с компонентом PT Cybsi Provider» (см. раздел 11.4.6)

11.4.1. Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора> до версии <Номер версии>»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось обновить базу знаний вендора <Название вендора> до версии <Номер версии>».

Возможные причины

Указаны неверные параметры обновления в конфигурационном файле или получен некорректный пакет обновлений от сервера вендора.

Решение

- Чтобы решить проблему:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Дальнейшая настройка выполняется в секции `Auto-updates settings`.

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. Если сервер с установленным модулем nad-task-server подключается к интернету через прокси-сервер для получения обновлений базы знаний с внешнего источника, проверьте работу этого прокси-сервера и корректность настройки подключения к нему в параметре `proxy`:

     ```
     proxy: <http или https>://<Логин>:<Пароль>@<Адрес прокси-сервера>:<Порт>
     proxy: http://username:P@ssw0rd@proxy.example.com:3128
     ```

  3. Если сервер с установленным модулем nad-task-server подключается к локальному зеркалу (см. раздел 5.6.6) для получения обновлений базы знаний, проверьте работу этого зеркала и корректность настройки подключения к нему в параметре `update_server`:

     ```
     update_server: <Адрес локального сервера обновлений>:8743
     ```

     Например:

     ```
     update_server: 198.51.100.78:8743
     ```

  4. Если PT NAD не должен проверять сертификаты веб-серверов, с которых загружаются правила, проверьте наличие строки:

     ```
     verify: false
     ```

  5. Если настроено обновление правил Proofpoint ET Open с удаленного источника, проверьте наличие строк:

     ```
     updater.ETOpen.http.enabled: true
     updater.ETOpen.http.url: https://rules.emergingthreats.net/open/suricata-4.0/
     emerging.rules.tar.gz
     updater.ETOpen.http.rules: emerging.rules.tar.gz
     ```

     Эти строки могут быть представлены в следующем виде:

     - `updater` → `ETOpen` → `http` → `enabled: true`;
     - `updater` → `ETOpen` → `http` → `url: https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz`;
     - `updater` → `ETOpen` → `http` → `rules: emerging.rules.tar.gz`.

6. Если настроено обновление правил Proofpoint ET Open с локального каталога, проверьте наличие строк:

   ```
   updater.ETOpen.http.enabled: false
   updater.ETOpen.fs.enabled: true
   updater.ETOpen.fs.path: <Путь к каталогу с обновлениями правил Proofpoint ET Open>
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETOpen` → `http` → `enabled: false`;
   - `updater` → `ETOpen` → `fs` → `enabled: true`;
   - `updater` → `ETOpen` → `fs` → `path: <Путь к каталогу с обновлениями правил Proofpoint ET Open>`.

7. Если настроено обновление правил Proofpoint ET Pro с удаленного источника, проверьте наличие строк:

   ```
   updater.ETPro.http.enabled: true
   updater.ETPro.http.url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz
   updater.ETPro.http.rules: etpro.rules.tar.gz
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETPro` → `http` → `enabled: true`;
   - `updater` → `ETPro` → `http` → `url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz`;
   - `updater` → `ETPro` → `http` → `rules: etpro.rules.tar.gz`.

   Вместо `<oinkcode>` должен быть указан код, полученный при заказе правил Proofpoint ET Pro.

8. Если настроено обновление правил Proofpoint ET Pro с локального каталога, проверьте наличие строк:

   ```
   updater.ETPro.http.enabled: false
   updater.ETPro.fs.enabled: true
   updater.ETPro.fs.path: <Путь к каталогу с обновлениями правил Proofpoint ET Pro>
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETPro` → `http` → `enabled: false`;
   - `updater` → `ETPro` → `fs` → `enabled: true`;
   - `updater` → `ETPro` → `fs` → `path: <Путь к каталогу с обновлениями правил Proofpoint ET Pro>`.

9. Сохраните файл `nad.settings.yaml`.

10. Перезагрузите модули nad-task-server и nad-web-server:

    ```
    sudo systemctl restart nad-task-server.service
    sudo systemctl restart nad-web-server.service
    ```

11. Если решить проблему не удалось, обратитесь в службу технической поддержки Positive Technologies.

11.4.2. Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось обновить базу знаний вендора <Название вендора>».

Возможные причины

Указаны неверные параметры обновления в конфигурационном файле или получен некорректный пакет обновлений от сервера вендора.

Решение

- Чтобы решить проблему:

1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

   ```
   sudo nano /opt/ptsecurity/etc/nad.settings.yaml
   ```

   Дальнейшая настройка выполняется в секции `Auto-updates settings`.

   Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

2. Если сервер с установленным модулем nad-task-server подключается к интернету через прокси-сервер для получения обновлений базы знаний с внешнего источника, проверьте работу этого прокси-сервера и корректность настройки подключения к нему в параметре `proxy`:

   ```
   proxy: <http или https>://<Логин>:<Пароль>@<Адрес прокси-сервера>:<Порт>
   proxy: http://username:P@ssw0rd@proxy.example.com:3128
   ```

3. Если сервер с установленным модулем nad-task-server подключается к локальному зеркалу (см. раздел 5.6.6) для получения обновлений базы знаний, проверьте работу этого зеркала и корректность настройки подключения к нему в параметре `update_server`:

   ```
   update_server: <Адрес локального сервера обновлений>:8743
   ```

   Например:

   ```
   update_server: 198.51.100.78:8743
   ```

4. Если PT NAD не должен проверять сертификаты веб-серверов, с которых загружаются правила, проверьте наличие строки:

   ```
   verify: false
   ```

5. Если настроено обновление правил Proofpoint ET Open с удаленного источника, проверьте наличие строк:

   ```
   updater.ETOpen.http.enabled: true
   updater.ETOpen.http.url: https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz
   updater.ETOpen.http.rules: emerging.rules.tar.gz
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETOpen` → `http` → `enabled: true`;
   - `updater` → `ETOpen` → `http` → `url: https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz`;
   - `updater` → `ETOpen` → `http` → `rules: emerging.rules.tar.gz`.

6. Если настроено обновление правил Proofpoint ET Open с локального каталога, проверьте наличие строк:

   ```
   updater.ETOpen.http.enabled: false
   updater.ETOpen.fs.enabled: true
   updater.ETOpen.fs.path: <Путь к каталогу с обновлениями правил Proofpoint ET Open>
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETOpen` → `http` → `enabled: false`;
   - `updater` → `ETOpen` → `fs` → `enabled: true`;
   - `updater` → `ETOpen` → `fs` → `path: <Путь к каталогу с обновлениями правил Proofpoint ET Open>`.

7. Если настроено обновление правил Proofpoint ET Pro с удаленного источника, проверьте наличие строк:

   ```
   updater.ETPro.http.enabled: true
   updater.ETPro.http.url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz
   updater.ETPro.http.rules: etpro.rules.tar.gz
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETPro` → `http` → `enabled: true`;
   - `updater` → `ETPro` → `http` → `url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz`;
   - `updater` → `ETPro` → `http` → `rules: etpro.rules.tar.gz`.

   Вместо `<oinkcode>` должен быть указан код, полученный при заказе правил Proofpoint ET Pro.

8. Если настроено обновление правил Proofpoint ET Pro с локального каталога, проверьте наличие строк:

   ```
   updater.ETPro.http.enabled: false
   updater.ETPro.fs.enabled: true
   updater.ETPro.fs.path: <Путь к каталогу с обновлениями правил Proofpoint ET Pro>
   ```

   Эти строки могут быть представлены в следующем виде:

   - `updater` → `ETPro` → `http` → `enabled: false`;
   - `updater` → `ETPro` → `fs` → `enabled: true`;
   - `updater` → `ETPro` → `fs` → `path: <Путь к каталогу с обновлениями правил Proofpoint ET Pro>`.

9. Сохраните файл `nad.settings.yaml`.
10. Перезагрузите модули nad-task-server и nad-web-server:

    ```
    sudo systemctl restart nad-task-server.service
    sudo systemctl restart nad-web-server.service
    ```

11. Если решить проблему не удалось, обратитесь в службу технической поддержки Positive Technologies.

11.4.3. Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>: недействительный лицензионный ключ»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось обновить базу знаний вендора <Название вендора>: недействительный лицензионный ключ».

Возможные причины

Серийный номер лицензии не существует или срок его действия закончился.

Решение

- Чтобы решить проблему,

  проверьте, правильно ли указан серийный номер лицензии (см. раздел 9).

11.4.4. Устранение ошибки «Не удалось обновить базу знаний вендора <Название вендора>: нет соединения с сервером обновлений»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось обновить базу знаний вендора <Название вендора>: нет соединения с сервером обновлений».

Возможные причины

Сервер обновлений вендора по какой-то причине недоступен или его адрес неверно указан в конфигурационном файле.

Решение

- Чтобы решить проблему:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Дальнейшая настройка выполняется в секции `Auto-updates settings`.

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. Если сервер с установленным модулем nad-task-server подключается к интернету через прокси-сервер для получения обновлений базы знаний с внешнего источника, проверьте работу этого прокси-сервера и корректность настройки подключения к нему в параметре `proxy`:

     ```
     proxy: <http или https>://<Логин>:<Пароль>@<Адрес прокси-сервера>:<Порт>
     proxy: http://username:P@ssw0rd@proxy.example.com:3128
     ```

  3. Если сервер с установленным модулем nad-task-server подключается к локальному зеркалу (см. раздел 5.6.6) для получения обновлений базы знаний, проверьте работу этого зеркала и корректность настройки подключения к нему в параметре `update_server`:

     ```
     update_server: <Адрес локального сервера обновлений>:8743
     ```

     Например:

     ```
     update_server: 198.51.100.78:8743
     ```

  4. Если PT NAD не должен проверять сертификаты веб-серверов, с которых загружаются правила, проверьте наличие строки:

     ```
     verify: false
     ```

  5. Если в тексте ошибки указан ETOpen, проверьте наличие строки:

     ```
     updater.ETOpen.http.url: https://rules.emergingthreats.net/open/suricata-4.0/
     emerging.rules.tar.gz
     ```

Эта строка может быть представлена в следующем виде:

- `updater → ETOpen → http → url: https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz`;

6. Если в тексте ошибки указан ETPro, проверьте наличие строки:
   `updater.ETPro.http.url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz`

   Эта строка может быть представлена в следующем виде:

   - `updater → ETPro → http → url: https://rules.emergingthreatspro.com/<oinkcode>/suricata-4.0/etpro.rules.tar.gz`;

     Вместо `<oinkcode>` должен быть указан код, полученный при заказе правил Proofpoint ET Pro.

7. Сохраните файл `nad.settings.yaml`.
8. Перезагрузите модули nad-task-server и nad-web-server:
   ```
   sudo systemctl restart nad-task-server.service
   sudo systemctl restart nad-web-server.service
   ```

11.4.5. Устранение ошибки «Не удалось получить индикаторы компрометации: некорректный токен PT Cybsi Provider»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось получить индикаторы компрометации: некорректный токен PT Cybsi Provider».

Возможные причины

Для корректной синхронизации списка индикаторов компрометации PT NAD и компонент PT Cybsi Provider (PT CP) системы MaxPatrol SIEM выполняют проверку по токену. Ошибка возникает, если токен не прошел проверку по одной из следующих причин:

— PT CP был переустановлен после того, как была настроена его интеграция с PT NAD.

— PT CP был восстановлен из резервной копии после того, как была настроена его интеграция с PT NAD.

— В конфигурационном файле PT NAD указан адрес узла, на котором установлен другой экземпляр PT CP.

Решение

- Чтобы решить проблему:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. В значении параметра `cybsi_host` проверьте корректность IP-адреса или домена узла, на котором установлен PT CP, и наличие порта 2443, например:

     ```
     cybsi_host: '203.0.113.11:2443'
     ```

  3. Сохраните файл `nad.settings.yaml`.

  4. Перезагрузите модули nad-task-server и nad-web-server:

     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  5. Если ошибка сохраняется, на узле с PT NAD запустите процесс удаления и повторного получения индикаторов компрометации:

     ```
     sudo /opt/ptsecurity/nad/bin/manage cybsi import --init
     ```

     Процесс займет продолжительное время (до нескольких часов).

11.4.6. Устранение ошибки «Не удалось получить индикаторы компрометации: нет соединения с компонентом PT Cybsi Provider»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Не удалось получить индикаторы компрометации: нет соединения с компонентом PT Cybsi Provider».

Возможные причины

PT NAD не удалось связаться с компонентом PT Cybsi Provider (PT CP) системы MaxPatrol SIEM по одной из следующих причин:

— В конфигурационном файле PT NAD указан неверный адрес узла, на котором установлен PT CP.

— Проблемы соединения с узлом, на котором установлен PT CP, например доступ заблокирован межсетевым экраном.

Решение

- Чтобы решить проблему:

  1. Откройте конфигурационный файл `/opt/ptsecurity/etc/nad.settings.yaml` на узле с установленными модулями nad-task-server и nad-web-server:

     ```
     sudo nano /opt/ptsecurity/etc/nad.settings.yaml
     ```

     Примечание. Если модули nad-task-server и nad-web-server установлены на разных узлах, вам нужно изменить файл `nad.settings.yaml` на обоих узлах.

  2. В значении параметра `cybsi_host` проверьте корректность IP-адреса или домена узла, на котором установлен PT CP, и наличие порта 2443, например:

     ```
     cybsi_host: '203.0.113.11:2443'
     ```

  3. Сохраните файл `nad.settings.yaml`.

  4. Перезагрузите модули nad-task-server и nad-web-server:

     ```
     sudo systemctl restart nad-task-server.service
     sudo systemctl restart nad-web-server.service
     ```

  5. Если ошибка сохраняется, проверьте сетевой доступ к PT CP.

11.5. Устранение проблем в работе компонентов PT NAD

В этом разделе описываются ошибки, связанные с недоступностью модулей PT NAD или другими проблемами в их работе, а также приводятся рекомендации по устранению этих ошибок.

В этом разделе

11.5.1. Устранение ошибки «Модуль nad-reporter недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль nad-reporter недоступен».

Возможные причины

Модуль nad-reporter не запущен или недоступен.

Решение

- Чтобы решить проблему:

  1. Перезапустите модуль nad-reporter:
     ```
     sudo systemctl restart nad-reporter.service
     ```
  2. Проверьте состояние модуля nad-reporter:
     ```
     systemctl status nad-reporter.service
     ```
     При успешном запуске появится сообщение:
     ```
     active (running)
     ```
  3. Если модуль nad-reporter запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.2. Устранение ошибки «Модуль pyfpta недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль pyfpta недоступен».

Возможные причины

Модуль pyfpta не запущен или недоступен.

Решение

- Чтобы решить проблему:

  1. Перезапустите модуль pyfpta:
     ```
     sudo systemctl restart pyfpta.service
     ```
  2. Проверьте состояние модуля pyfpta:
     ```
     systemctl status pyfpta.service
     ```
     При успешном запуске появится сообщение:
     ```
     active (running)
     ```
  3. Если модуль pyfpta запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.3. Устранение ошибки «Модуль nad-task-server остановлен или работает некорректно»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль nad-task-server остановлен или работает некорректно».

Возможные причины

Модуль nad-task-server не запущен или работает некорректно. Статистика работы PT NAD может быть неактуальной.

Решение

- Чтобы решить проблему:

  1. Перезапустите модуль nad-task server:
     ```
     sudo systemctl restart nad-task-server.service
     ```
  2. Проверьте состояние модуля nad-task-server:
     ```
     systemctl status nad-task-server.service
     ```

При успешном запуске появится сообщение:

```
active (running)
```

3. Если модуль nad-task-server запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

См. также

Устранение ошибки «Узел <Название узла>: модуль nad-task-server недоступен» (см. раздел 11.5.9)

11.5.4. Устранение ошибки «Модуль ptdpi-broker недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль ptdpi-broker недоступен».

Возможные причины

Модуль ptdpi-broker не запущен или недоступен.

Решение

- Чтобы решить проблему:

1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. Убедитесь, что значения параметров `broker_type` и `broker_host` установлены правильно:

   - Если все модули подсистем установлены на одном физическом сервере, значение параметра `broker_type` должно быть `local`.
   - Если модули подсистем установлены на разных серверах и виртуальных машинах, на основном узле должно быть указано `broker_type:local` и в параметре `broker_host` должен быть указан внешний IP-адрес этого узла.

3. Запустите PT NAD:

   ```
   sudo ptdpictl start-all
   ```

4. Проверьте состояние модулей:

   ```
   ptdpictl status-all
   ```

При успешном запуске появится сообщение:

```
ptdpi-broker.service running
```

5. Если модуль ptdpi-broker запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.5. Устранение ошибки «Модуль ptdpi-worker@dns недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль ptdpi-worker@dns недоступен».

Возможные причины

Модуль ptdpi-worker@dns не запущен или недоступен.

Решение

- Чтобы решить проблему:

1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. Убедитесь, что в параметре `workers` указано `dns es`.
3. Запустите PT NAD:

   ```
   sudo ptdpictl start-all
   ```

4. Проверьте состояние модулей:

   ```
   ptdpictl status-all
   ```

   При успешном запуске появится сообщение:

   ```
   ptdpi-worker@dns.service dns running
   ```

5. Если модуль ptdpi-worker@dns запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.6. Устранение ошибки «Модуль ptdpi-worker@es недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль ptdpi-worker@es недоступен».

Возможные причины

Модуль ptdpi-worker@es не запущен или недоступен.

Решение

- Чтобы решить проблему:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Убедитесь, что в параметре `workers` указано `dns es`.
  3. Запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  4. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```
     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@es.service es running
     ```
  5. Если модуль ptdpi-worker@es запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки PT NAD для дальнейшего анализа.

11.5.7. Устранение ошибки «Сенсор недоступен или выключен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Сенсор недоступен или выключен».

Возможные причины

Сенсор не запущен или недоступен.

Решение

- Чтобы решить проблему:

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

     Откроется страница **Сенсоры**.
  2. Включите сенсор.
  3. Если включить сенсор из интерфейса по какой-либо причине не удалось, на узле с установленным модулем ptdpi выполните команду:
     ```
     sudo ptdpictl start
     ```

При успешном запуске появится сообщение:

```
ptdpictl start... OK
```

Примечание. Вы можете проверить состояние сенсора командой `sudo ptdpictl status`. Если модуль запущен, появится сообщение `ptdpictl status... ptdpi.service running`.

4. Если сенсор запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

См. также

Сенсор (см. раздел 2.2.1)

11.5.8. Устранение ошибки «Сервис мониторинга недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Сервис мониторинга недоступен».

Возможные причины

Модуль ptdpistat не запущен или недоступен.

Решение

- Чтобы решить проблему:

1. Запустите модуль ptdpistat:

```
sudo systemctl start ptdpistat
```

2. Если модуль запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

См. также

Подсистема мониторинга (см. раздел 2.2.5)

11.5.9. Устранение ошибки «Узел <Название узла>: модуль nad-task-server недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль nad-task-server недоступен».

Возможные причины

Модуль nad-task-server не запущен или недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле перезапустите модуль nad-task server:
     ```
     sudo systemctl restart nad-task-server.service
     ```
  2. Проверьте состояние модуля nad-task-server:
     ```
     systemctl status nad-task-server.service
     ```
     При успешном запуске появится сообщение:
     ```
     active (running)
     ```
  3. Если модуль nad-task-server запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

См. также

Устранение ошибки «Модуль nad-task-server остановлен или работает некорректно» (см. раздел 11.5.3)

11.5.10. Устранение ошибки «Узел <Название узла>: модуль ptdpistat недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpistat недоступен».

Возможные причины

Модуль ptdpistat не запущен или недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле перезапустите модуль ptdpistat:
     ```
     sudo systemctl restart ptdpistat.service
     ```
  2. Проверьте состояние модуля ptdpistat:
     ```
     systemctl status ptdpistat.service
     ```

При успешном запуске появится сообщение:

```
active (running)
```

3. Если модуль ptdpistat запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.11. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@ad недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@ad недоступен».

Возможные причины

Модуль ptdpi-worker@ad недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:

     ```
     sudo ptdpictl start-all
     ```

  2. Проверьте состояние модулей:

     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:

     ```
     ptdpi-worker@ad.service ad running
     ```

  3. Если модуль ptdpi-worker@ad запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

В многосерверной конфигурации модуль ptdpi-worker@ad работает только на основном сервере. Если модуль был запущен на дополнительном сервере по ошибке, вы можете отключить его на этом сервере.

- Чтобы отключить модуль ptdpi-worker@ad:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```

  2. Из значения параметра `workers` удалите `ad`.

  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@ad отключен.

11.5.12. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@alert недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@alert недоступен».

Возможные причины

Модуль ptdpi-worker@alert недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  2. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@alert.service alert running
     ```
  3. Если модуль ptdpi-worker@alert запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

В многосерверной конфигурации модуль ptdpi-worker@alert работает только на основном сервере. Если модуль был запущен на дополнительном сервере по ошибке, вы можете отключить его на этом сервере.

- Чтобы отключить модуль ptdpi-worker@alert:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Из значения параметра `workers` удалите `alert`.
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@alert отключен.

11.5.13. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@hosts недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@hosts недоступен».

Возможные причины

Модуль ptdpi-worker@hosts недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  2. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@hosts.service hosts running
     ```
  3. Если модуль ptdpi-worker@hosts запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

В многосерверной конфигурации модуль ptdpi-worker@hosts работает только на основном сервере. Если модуль был запущен на дополнительном сервере по ошибке, вы можете отключить его на этом сервере.

- Чтобы отключить модуль ptdpi-worker@hosts:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Из значения параметра `workers` удалите `hosts`.
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@hosts отключен.

11.5.14. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@icap недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@icap недоступен».

Возможные причины

Модуль ptdpi-worker@icap недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  2. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@icap.service icap running
     ```
  3. Если модуль ptdpi-worker@icap запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

Если вам не нужен модуль ptdpi-worker@icap на указанном узле, вы можете его отключить.

- Чтобы отключить модуль ptdpi-worker@icap:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Из значения параметра `workers` удалите `icap`.

     Примечание. Если в значении параметра указано только `icap`, строку с ним нужно удалить целиком.
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@icap отключен.

11.5.15. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@mpx недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@mpx недоступен».

Возможные причины

Модуль ptdpi-worker@mpx недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  2. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@mpx.service mpx running
     ```
  3. Если модуль ptdpi-worker@mpx запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

Если вам не нужен модуль ptdpi-worker@mpx на указанном узле, вы можете его отключить.

- Чтобы отключить модуль ptdpi-worker@mpx:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Из значения параметра `workers` удалите `mpx`.

     Примечание. Если в значении параметра указано только `mpx`, строку с ним нужно удалить целиком.
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@mpx отключен.

11.5.16. Устранение ошибки «Узел <Название узла>: модуль ptdpi-worker@notifier недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: модуль ptdpi-worker@notifier недоступен».

Возможные причины

Модуль ptdpi-worker@notifier недоступен на узле, указанном в сообщении об ошибке.

Решение

- Чтобы решить проблему:

  1. На указанном узле запустите PT NAD:
     ```
     sudo ptdpictl start-all
     ```
  2. Проверьте состояние модулей:
     ```
     ptdpictl status-all
     ```

     При успешном запуске появится сообщение:
     ```
     ptdpi-worker@notifier.service notifier running
     ```
  3. Если модуль ptdpi-worker@notifier запустить не удалось, скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

В многосерверной конфигурации модуль ptdpi-worker@notifier работает только на основном сервере. Если модуль был запущен на дополнительном сервере по ошибке, вы можете там его отключить.

- Чтобы отключить модуль ptdpi-worker@notifier:

  1. На указанном узле откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Из значения параметра `workers` удалите `notifier`.
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

4. Перезапустите сенсор:
   ```
   sudo ptdpictl restart-all
   ```
5. Перезапустите модуль ptdpistat:
   ```
   sudo systemctl restart ptdpistat.service
   ```

Модуль ptdpi-worker@notifier отключен.

См. также

Настройка отправки сообщений при помощи механизма webhook (см. раздел 10.11)

Настройка syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации (см. раздел 10.10.1)

11.5.17. Устранение проблем в работе модуля Elasticsearch

В этом разделе описываются ошибки в работе модуля Elasticsearch, а также приводятся рекомендации по устранению этих ошибок.

В этом разделе

Устранение ошибки «В кластере Elasticsearch осталось менее 10% свободного места» (см. раздел 11.5.17.1)

Устранение ошибки «В кластере Elasticsearch осталось менее 20% свободного места» (см. раздел 11.5.17.2)

Устранение ошибки «За последний час проиндексирован не весь трафик» (см. раздел 11.5.17.3)

Устранение ошибки «Модуль Elasticsearch недоступен» (см. раздел 11.5.17.4)

Устранение ошибки «Статус кластера Elasticsearch — желтый» (см. раздел 11.5.17.5)

Устранение ошибки «Статус кластера Elasticsearch — красный» (см. раздел 11.5.17.6)

11.5.17.1. Устранение ошибки «В кластере Elasticsearch осталось менее 10% свободного места»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «В кластере Elasticsearch осталось менее 10% свободного места».

Возможные причины

В файловой системе, выделенной под хранение файлов формата JSON с метаданными трафика, осталось менее 10% свободного места.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что согласно параметрам планировщика Cron в файле `/etc/cron.d/ptdpi` скрипт `es-cleaner.py` выполняется регулярно.
  2. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  3. Проверьте значение параметра `es_store_days` в секции `Elastic settings`.

     Параметр задает время хранения файлов формата JSON в днях. При необходимости нужно уменьшить значение.
  4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  5. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart-all
     ```
  6. Если файлы формата JSON хранятся не на отдельных жестких дисках или файловых системах, проверьте использование дискового пространства при помощи утилит df и du. При необходимости удалите неиспользуемые файлы, например файлы журналов и резервные копии.
  7. Если решить проблему не удалось, отправьте файл `/opt/ptsecurity/log/ptdpi-estools.log` в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.17.2. Устранение ошибки «В кластере Elasticsearch осталось менее 20% свободного места»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «В кластере Elasticsearch осталось менее 20% свободного места».

Возможные причины

В файловой системе, выделенной под хранение файлов формата JSON с метаданными трафика, осталось менее 20% свободного места.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что согласно параметрам планировщика Cron в файле `/etc/cron.d/ptdpi` скрипт `es-cleaner.py` выполняется регулярно.
  2. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  3. Проверьте значение параметра `es_store_days` в секции `Elastic settings`.

     Параметр задает время хранения файлов формата JSON в днях. При необходимости нужно уменьшить значение.
  4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  5. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart-all
     ```
  6. Если файлы формата JSON хранятся не на отдельных жестких дисках или файловых системах, проверьте использование дискового пространства при помощи утилит df и du. При необходимости удалите неиспользуемые файлы, например файлы журналов и резервные копии.
  7. Если решить проблему не удалось, отправьте файл `/opt/ptsecurity/log/ptdpi-estools.log` в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.17.3. Устранение ошибки «За последний час проиндексирован не весь трафик»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «За последний час проиндексирован не весь трафик».

Возможные причины

Модуль Elasticsearch не справляется с нагрузкой и не успевает индексировать трафик.

Решение

Если нет других проблем в работе модуля Elasticsearch, вам нужно либо добавить новые узлы (nodes) в кластер Elasticsearch, либо изменить параметры кластера. Подробную информацию см. на сайте разработчика Elasticsearch.

11.5.17.4. Устранение ошибки «Модуль Elasticsearch недоступен»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Модуль Elasticsearch недоступен».

Возможные причины

Модуль Elasticsearch не запущен или недоступен.

Решение

- Чтобы решить проблему:

  1. На узле с установленным модулем Elasticsearch запустите этот модуль:
     ```
     sudo systemctl start elasticsearch.service
     ```
  2. Проверьте состояние модуля Elasticsearch:
     ```
     sudo systemctl status elasticsearch.service
     ```
  3. Если модуль Elasticsearch запустить не удалось, отправьте файлы из каталога `/var/log/elasticsearch` в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.17.5. Устранение ошибки «Статус кластера Elasticsearch — желтый»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Статус кластера Elasticsearch — желтый».

Возможные причины

Не для всех данных в Elasticsearch есть необходимое количество копий. Это может быть вызвано:

— некорректной настройкой репликации данных в Elasticsearch;

— выходом из строя одного или нескольких узлов (nodes) Elasticsearch;

— временными проблемами синхронизации кластера Elasticsearch.

Решение

Скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.5.17.6. Устранение ошибки «Статус кластера Elasticsearch — красный»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Статус кластера Elasticsearch — красный».

Возможные причины

Часть данных в модуле Elasticsearch недоступна. Это может быть вызвано:

— выходом из строя одного или нескольких узлов (nodes) Elasticsearch;

— временными проблемами синхронизации кластера Elasticsearch.

Решение

Скачайте архив с файлами системных журналов (см. раздел 11.2) и отправьте его в службу технической поддержки Positive Technologies для дальнейшего анализа.

11.6. Устранение проблем с журналом аудита

В этом разделе приводятся описания ошибок, связанных с журналом аудита (см. раздел 10.4), и даются инструкции по устранению этих ошибок.

В этом разделе

11.6.1. Устранение ошибки «Журнал аудита переполнен, поэтому запись событий приостановлена. Очистите журнал и включите запись событий»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Журнал аудита переполнен, поэтому запись событий приостановлена. Очистите журнал и включите запись событий».

Возможные причины

Количество записей в журнале аудита достигло значения, указанного в параметре `journal_limit` (по умолчанию — 10 000).

Решение

- Чтобы решить проблему:

  1. Удалите записи из журнала аудита (см. раздел 10.4.4) или увеличьте максимальное количество записей в журнале (см. раздел 10.4.6).
  2. Включите запись событий (см. раздел 10.4.1).

См. также

Журнал аудита (см. раздел 10.4)

11.6.2. Устранение ошибки «Журнал аудита почти заполнен. Очистите его»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Журнал аудита почти заполнен. Очистите его».

Возможные причины

Количество записей в журнале аудита достигло значения, указанного в параметре `journal_threshold` (по умолчанию — 9000).

Решение

- Чтобы решить проблему,

  удалите записи из журнала аудита (см. раздел 10.4.4) или увеличьте максимальное количество записей в журнале (см. раздел 10.4.6).

См. также

Журнал аудита (см. раздел 10.4)

11.7. Устранение проблем с захватом трафика

В этом разделе приводятся описания ошибок, связанных с захватом трафика продуктом, и даются рекомендации по их устранению.

В этом разделе

11.7.1. Устранение ошибки «Узел <Название узла>: более 0.5% потерь при захвате трафика»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: более 0.5% потерь при захвате трафика». Эта ошибка означает, что потери при захвате трафика сенсором составляют 0,5—5%.

Возможные причины

Сенсор не справляется с захватом всего потока трафика.

Решение

- Чтобы решить проблему,

  в параметрах сенсора исключите из захвата часть трафика.

  Подробную информацию см. в разделе «Управление сенсорами и фильтрами захвата трафика» в Руководстве оператора.

11.7.2. Устранение ошибки «Узел <Название узла>: более 5% потерь при захвате трафика»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: более 5% потерь при захвате трафика». Эта ошибка означает, что потери при захвате трафика сенсором составляют более 5%.

Возможные причины

Сенсор не справляется с захватом всего потока трафика.

Решение

- Чтобы решить проблему,

  в параметрах сенсора исключите из захвата часть трафика.

  Подробную информацию см. в разделе «Управление сенсорами и фильтрами захвата трафика» в Руководстве оператора.

11.7.3. Устранение ошибки «Узел <Название узла>: нет трафика за последние 5 минут»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: нет трафика за последние 5 минут».

Возможные причины

За последние 5 минут в продукт не поступал трафик для анализа.

Решение

- Чтобы решить проблему:

  1. Проверьте подключение сетевых кабелей к серверу с установленным PT NAD.
  2. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  3. В значении параметра `capture_if` проверьте корректность названия сетевого интерфейса, трафик с которого должен захватываться.

     Например:
     ```
     capture_if: eth2
     ```
  4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  5. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart-all
     ```

11.8. Устранение проблем с записью исходной копии трафика

В этом разделе приводятся описания ошибок, связанных с записью продуктом исходной копии трафика в формате PCAP на дисковую подсистему сервера PT NAD, а также даются рекомендации по устранению этих ошибок.

В этом разделе

11.8.1. Устранение ошибки «Узел <Название узла>: есть ошибки записи трафика в PCAP-файлы»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: есть ошибки записи трафика в PCAP-файлы».

Возможные причины

На указанном узле за последние 24 часа произошла как минимум одна ошибка записи трафика в хранилище файлов PCAP из-за сбоя в дисковой подсистеме.

Решение

- Чтобы решить проблему,

  проверьте работу жестких дисков и при необходимости замените их.

11.8.2. Устранение ошибки «Узел <Название узла>: за последний час более 5% от всего трафика не было записано»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: за последний час более 5% от всего трафика не было записано».

Возможные причины

Дисковая подсистема не справляется с записью всего потока трафика.

Решение

- Чтобы решить проблему,

  в параметрах сенсора исключите из захвата часть трафика.

  Подробную информацию см. в разделе «Управление сенсорами и фильтрами захвата трафика» в Руководстве оператора.

11.8.3. Устранение ошибки «Узел <Название узла>: за последний час был записан не весь трафик»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: за последний час был записан не весь трафик».

Возможные причины

Дисковая подсистема не справляется с записью всего потока трафика.

Решение

- Чтобы решить проблему,

  в параметрах сенсора исключите из захвата часть трафика.

  Подробную информацию см. в разделе «Управление сенсорами и фильтрами захвата трафика» в Руководстве оператора.

11.9. Устранение проблем с нехваткой аппаратных ресурсов

В этом разделе приводятся описания ошибок, связанных с недостатком аппаратных ресурсов на сервере PT NAD, и даются инструкции по устранению этих ошибок.

В этом разделе

Устранение ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан более чем на 80%, возможны проблемы с разбором трафика» (см. раздел 11.9.3)

Устранение ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан, часть трафика не разбирается» (см. раздел 11.9.4)

11.9.1. Устранение ошибки «Узел <Название узла>: в файловой системе <Точка монтирования> закончилось свободное место»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: в файловой системе <Точка монтирования> закончилось свободное место».

Возможные причины

В файловой системе с указанной точкой монтирования закончилось свободное место.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что согласно параметрам планировщика Cron в файле `/etc/cron.d/ptdpi` скрипты `es-cleaner.py` и `ptdpi-watch-diskspace` выполняются регулярно.
  2. При необходимости измените ротацию данных в потоковых хранилищах (см. раздел 10.9).
  3. Проверьте использование дискового пространства в файловой системе при помощи утилит df и du. При необходимости удалите неиспользуемые файлы, например файлы журналов и резервные копии.

11.9.2. Устранение ошибки «Узел <Название узла>: в файловой системе <Точка монтирования> осталось менее 5% свободного места»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: в файловой системе <Точка монтирования> осталось менее 5% свободного места».

Возможные причины

В файловой системе с указанной точкой монтирования осталось меньше 5% свободного места.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что согласно параметрам планировщика Cron в файле `/etc/cron.d/ptdpi` скрипты `es-cleaner.py` и `ptdpi-watch-diskspace` выполняются регулярно.
  2. При необходимости измените ротацию данных в потоковых хранилищах (см. раздел 10.9).
  3. Проверьте использование дискового пространства в файловой системе при помощи утилит df и du. При необходимости удалите неиспользуемые файлы, например файлы журналов и резервные копии.

11.9.3. Устранение ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан более чем на 80%, возможны проблемы с разбором трафика»

В главном меню отображается желтый индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан более чем на 80%, возможны проблемы с разбором трафика».

Возможные причины

Аппаратный ресурс, выделенный в конфигурации сенсора под определенную функцию, исчерпан более чем на 80%.

Таблица 6. Аппаратные ресурсы

Название	Тип	Функция	Лимит по умолчанию
Total.defrag.memuse	ОЗУ	Дефрагментация IPv4- и IPv6-пакетов	32 МБ
Total.flow.memuse	ОЗУ	Отслеживание активных соединений	3 ГБ (≈5,6 млн соединений)
Total.tcp.memuse	ОЗУ	Отслеживание активных TCP-соединений	2 ГБ (≈7,5 млн соединений)
Total.files.memuse	ОЗУ	Сборка файлов, переданных в сессиях	1 ГБ
Total.seg.memuse	ОЗУ	Сборка TCP-соединений	8 ГБ

Название	Тип	Функция	Лимит по умолчанию
Total.files.disk_used	Файловые дескрипторы	Сборка файлов, переданных в сессиях	3840

Нужно устранить проблему до полного исчерпания ресурса, иначе соответствующая функция перестанет работать.

Решение

Обратитесь в службу технической поддержки для настройки лимитов сенсора.

11.9.4. Устранение ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан, часть трафика не разбирается»

В главном меню отображается красный индикатор состояния продукта, по нажатию на который открывается всплывающая подсказка с текстом ошибки «Узел <Название узла>: ресурс <Название ресурса> исчерпан, часть трафика не разбирается».

Возможные причины

Аппаратный ресурс (см. раздел 11.9.3), выделенный в конфигурации сенсора под определенную функцию, исчерпан. Нужно устранить проблему для восстановления работы функции.

Решение

Обратитесь в службу технической поддержки для настройки лимитов сенсора.

11.10. Устранение ошибок при сборке сессий

В этом разделе описываются причины возникновения отдельных ошибок и флагов, которые появляются в записях сессий, а также даются рекомендацию по устранению этих ошибок и флагов.

В этом разделе

11.10.1. Устранение ошибок BAD_CHECKSUM

В списке сессий есть записи с флагом BAD_CHECKSUM «В трафике сессии есть поврежденные пакеты. Нарушение их целостности обнаружено при проверке контрольных сумм».

Возможные причины

PT NAD вычисляет контрольную сумму захваченного пакета TCP и сравнивает ее с контрольной суммой из заголовка того же пакета. Если контрольные суммы различаются, пакет считается поврежденным. При наличии хотя бы одного поврежденного пакета в сессии PT NAD добавляет флаг BAD_CHECKSUM в атрибуты этой сессии.

Решение

В нормальной ситуации получатель отклоняет поврежденный пакет, и отправитель пересылает его повторно. Однако в некоторых случаях (из-за особенностей настройки сетевого оборудования) может потребоваться отключить проверку контрольных сумм в PT NAD, поскольку поврежденные пакеты не анализируются и могут повлиять на корректную сборку сессии.

- Чтобы отключить проверку контрольных сумм:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Добавьте в конец файла строку:
     ```
     checksum_checks: no
     ```
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  4. Перезапустите сенсор:
     ```
     sudo ptdpictl restart
     ```

  Проверка контрольных сумм отключена.

Для повторного включения проверки контрольных сумм вам нужно изменить значение указанного параметра на `yes` и перезапустить сенсор.

11.10.2. Устранение ошибок OUT_OF_WINDOW

В списке сессий есть записи с ошибкой OUT_OF_WINDOW «Не удалось завершить анализ TCP-соединения. Потери данных превысили лимит».

Возможные причины

Объем данных, потерянных в TCP-соединении, превысил указанное в конфигурации PT NAD значение (по умолчанию — 10 КБ). До закрытия TCP-соединения указанный в конфигурационном файле PT NAD лимит может быть переопределен параметрами самого соединения, но это значение не может быть меньше указанного в конфигурации.

Решение

Вы можете повысить лимит для OUT_OF_WINDOW в конфигурации PT NAD.

- Чтобы изменить лимит для OUT_OF_WINDOW:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Добавьте в конец файла строку:
     ```
     ptdpi.yaml.stream.min-window-size: <Лимит в байтах>
     ```
     Например:
     ```
     ptdpi.yaml.stream.min-window-size: 15000
     ```
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  4. Перезапустите сенсор:
     ```
     sudo ptdpictl restart
     ```

  Лимит для OUT_OF_WINDOW изменен.

11.10.3. Устранение ошибок REASM_LIMIT

В списке сессий есть записи с ошибкой REASM_LIMIT «Не удалось завершить сборку сессии. Количество пакетов, переданных в TCP-соединении без подтверждения, достигло установленного лимита».

Возможные причины

Количество пакетов, переданных в TCP-соединении без подтверждения получателя (сегмент ACK), превысило указанное в конфигурации PT NAD значение (по умолчанию — 1000).

Решение

Вы можете повысить лимит для REASM_LIMIT в конфигурации PT NAD.

- Чтобы изменить лимит для REASM_LIMIT:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Добавьте в конец файла строку:
     ```
     ptdpi.yaml.stream.max-packets-latency: <Количество пакетов>
     ```
     Например:
     ```
     ptdpi.yaml.stream.max-packets-latency: 1200
     ```
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  4. Перезапустите сенсор:
     ```
     sudo ptdpictl restart
     ```

  Лимит для REASM_LIMIT изменен.

11.10.4. Устранение ошибок RES_LIMIT

В списке сессий есть записи с ошибкой RES_LIMIT «Не удалось проанализировать часть трафика сессии. Недостаточно памяти».

Возможные причины

PT NAD исчерпал объем памяти, выделенный для анализа TCP-соединения (по умолчанию — 8 ГБ).

Решение

Исчерпание памяти приводит к тому, что PT NAD перестает анализировать новые TCP-соединения. Чтобы решить эту проблему, вы можете выделить для анализа TCP-соединения больше памяти. Перед этим рекомендуется убедиться, что исчерпание памяти случается часто и длится продолжительное время.

Внимание! Выделение большего объема памяти может увеличить потребление ОЗУ сенсором.

Примечание. При настроенной интеграции с Grafana вы можете отслеживать процент потребления выделенной памяти на дашборде **DPI internal** с помощью виджета **DPI memuse** (показатель **reassemble**).

- Чтобы увеличить объем памяти, выделенный для анализа TCP-соединения:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. Добавьте в конец файла строку:
     ```
     ptdpi.yaml.stream.reassembly.memcap: <Объем><Единица измерения: kb, mb или gb>
     ```
     Например:
     ```
     ptdpi.yaml.stream.reassembly.memcap: 9gb
     ```

3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
4. Перезапустите сенсор:

   ```
   sudo ptdpictl restart
   ```

Объем памяти для анализа TCP-соединения увеличен.

12. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- предоставление рекомендаций по настройке продукта (оптимизации параметров) в процессе его эксплуатации;
- консультации по использованию функциональных возможностей продукта;
- диагностику сбоев, включая поиск причин и информирование клиента о выявленных проблемах;
- предоставление решений или возможностей обойти проблему с сохранением необходимой производительности;
- устранение ошибок в рамках выпуска обновлений;
- рассмотрение предложений по доработке продукта.

Вы можете получать техническую поддержку на специальном портале.

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

В этом разделе

12.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

Портал 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.

Техническая поддержка на портале предоставляется на русском и английском языках.

12.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

12.3. Как служба технической поддержки работает с запросами

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

В этом разделе

12.3.1. Предоставление информации для технической поддержки

Для решения проблем с продуктом вам необходимо предоставить специалисту технической поддержки следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, которые требуются для анализа;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- оптимальный канал для удаленного доступа к продукту и его диагностики (выбирается по согласованию).

Если информация не будет предоставлена в течение двух недель с момента запроса, специалист технической поддержки имеет право закрыть заявку, предварительно уведомив вас об этом.

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

12.3.2. Типы запросов

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

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

Доработка продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы также 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 реализации доработки остаются на усмотрение Positive Technologies.

12.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 7).

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

Таблица 7. Время реакции на запрос и время его обработки

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

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

12.3.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

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

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

Работы по запросу считаются выполненными, если:

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

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

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

— проблема классифицирована как неподдерживаемая.

Глоссарий

PT NAD Sensor

Упрощенная версия PT NAD, которая используется для интеграции с MaxPatrol SIEM. Позволяет снизить требования к аппаратным ресурсам за счет отключения или ограничения функций, не имеющих значения для работы в MaxPatrol SIEM.

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

Сетевое взаимодействие или группа взаимодействий, которые по специальным правилам определяются как целенаправленная угроза информационной безопасности.

аудит действий пользователя

Отслеживание действий пользователей в продукте Positive Technologies с целью оценки их деятельности или анализа работы продукта в целом.

исходная копия трафика

Сетевые данные, которые были захвачены сенсором 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.

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. PT NAD 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 сенсора, которая отвечает за захват и анализ сетевого трафика, а также выявление атак на основе правил и репутационных списков.

правило для атаки

Элемент сигнатурного анализа сетевого трафика, содержащий совокупность признаков, по которым сенсор 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 экспертами в области информационной безопасности и поставляются в PT NAD в виде пакетов. Операторы могут создавать или изменять отдельные правила в интерфейсе продукта. Срабатывание правила приводит к созданию записи об атаке.

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. PT NAD распознает отдельные сессии в общем потоке трафика, получает о них и об их участниках детальную информацию, которую сохраняет в базе данных. Эта информация используется для автоматического поиска событий ИБ. Операторы также могут самостоятельно изучать сессии в интерфейсе продукта для расследования инцидентов ИБ.

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.