Positive Technologies Система Определения и Предотвращения Телекоммуникационных Атак

Версия R2.5

Руководство по установке

POSITIVE TECHNOLOGIES

Дата редакции документа: 06.11.2020

Содержание

1. Об этом документе

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

Руководство адресовано специалистам, выполняющим установку и администрирование СОПТА.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

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

1.2. Другие источники информации о СОПТА

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

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

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки.

2. О СОПТА

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

В СОПТА реализованы следующие функции:

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

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

3. Требования к оборудованию и программному обеспечению

В данном разделе представлены требования к аппаратному и программному обеспечению для установки и использования СОПТА.

Таблица 2. Аппаратные требования для минимальной конфигурации

Параметр	Значение
CPU	Intel 8-ядерный 2,40 ГГц (с поддержкой набора инструкций AVX)
RAM	32 ГБ
HDD	2 × 1000 ГБ RAID 1
NIC	Ethernet 1 Гб

Таблица 3. Аппаратные требования для расширенной конфигурации

Параметр	Значение
CPU	Intel 16-ядерный 2,60 ГГц (с поддержкой набора инструкций AVX)
RAM	64 ГБ
HDD	4 × 500 ГБ RAID 1+0
NIC	Рекомендуемые сетевые карты: — Ethernet-контроллер Intel® 82599EB на 10 Гб — Ethernet-контроллер Intel® 82598EB на 10 Гб — Адаптер конвергентной сети Intel® Ethernet X520-LR1 — Ethernet-контроллер Intel® 82599ES на 10 Гб — Адаптер конвергентной сети Intel® Ethernet X520-SR2 — Адаптер сервера AT Intel® 10 Гб — Адаптер конвергентной сети Intel® Ethernet X520-SR1 — Адаптер конвергентной сети Intel® Ethernet X520-DA2 — Адаптер конвергентной сети Intel® Ethernet X540-T1 — Ethernet-контроллер Intel® 82599EN на 10 Гб — Адаптер конвергентной сети Intel® Ethernet X520-DA1 — Адаптер конвергентной сети Intel® Ethernet X550-T1 — Intel® Ethernet-контроллер X540-AT2

Параметр	Значение
	— Адаптер конвергентной сети Intel® Ethernet X550-T2 — Intel® Ethernet-контроллер X550-AT — Intel® Ethernet-контроллер X550-BT2 — Intel® Ethernet-контроллер X550-AT2 — Адаптер конвергентной сети Intel® Ethernet X540-T2 — Адаптер конвергентной сети Intel® Ethernet X520-QDA1

Для корректной обработки трафика необходимо предусмотреть отдельные сетевые интерфейсы для Firewall и механизма обнаружения атак.

Требования к программному обеспечению:

— Операционная система: Debian AMD64 10.

— Браузеры: Google Chrome 86 или новее, Mozilla Firefox 81 или новее.

4. Установка СОПТА

СОПТА предоставляется для установки в виде набора deb-пакетов (установочный комплект).

В данном разделе представлено описание установочного комплекта СОПТА и инструкции по установке продукта.

В этом разделе

4.1. Установочный комплект СОПТА

В таблице ниже представлено описание пакетов установочного комплекта СОПТА.

4.2. Подготовка к установке СОПТА

Перед установкой СОПТА убедитесь, что у вас есть права суперпользователя, стабильное интернет-соединение и что зеркала репозитория Debian версии `buster` указаны в файле `/etc/apt/sources.list`.

- Чтобы подготовить среду к установке СОПТА, сделайте следующее:

  1. Скопируйте установочный комплект СОПТА на сервер, на котором вы хотите установить СОПТА.
  2. Установите систему управления базами данных PostgreSQL и вспомогательные пакеты:

  Теперь ваша среда готова к установке СОПТА.

4.3. Процедура установки СОПТА

После того как вы подготовили свою среду, можно начать установку СОПТА.

Процедура установки состоит из установки компонентов СОПТА в порядке, указанном в данном разделе.

В этом разделе

4.3.1. Установка базы данных

- Чтобы установить базу данных СОПТА, выполните следующие действия:

1. Установите пакет интерактивной конфигурации базы данных:
   ```
   sudo dpkg -i tad-db-config_*.deb
   ```
   Примечание. Если вы используете мультисерверную установку, вы должны установить этот пакет на каждый сервер, на котором установлен удаленный компонент СОПТА.

   Отобразится следующее сообщение:
   ```
   Хотите использовать/создать локальный кластер или подключиться к удаленному?
   ```
2. Выберите `localhost`.

   Если будут обнаружены другие кластеры PostgreSQL, появится следующее сообщение:
   ```
   На этой машине уже существуют кластеры. Использовать один из них или создать новый?
   ```
3. Выберите существующий кластер или выберите `Создать новый кластер`.

   Если вы создаете новый кластер, вам будет предложено ввести номер версии PostgreSQL, имя кластера, порт базы данных, каталог, который будет использоваться для хранения данных (обычно `/var/lib/postgresql/<версия PostgreSQL>/<имя кластера>`), и путь к файлу журнала базы данных (например, `/var/log/postgresql/<имя кластера>.log`), который будет создан после установки пакета.
4. В открывшемся окне **Имя базы данных** введите имя базы данных и нажмите `Ok`.

   Отобразится следующее сообщение:
   ```
   Имя пользователя, которому будет принадлежать база данных. Оно также будет использоваться компонентами для подключения к БД.
   ```
5. Введите имя пользователя базы данных и нажмите `Ok`.
6. В открывшемся окне нажмите `Да`, чтобы подтвердить создание файла конфигурации базы данных `/opt/ptsecurity/etc/database.ini`.
7. Установите схему базы данных:
   ```
   sudo dpkg -i tad-db-schema_*.deb
   ```
   Эта операция создаст базу данных с именем, указанным на шаге 4, и таблицы по умолчанию в этой базе данных.
8. Установите содержимое таблиц базы данных (префиксы страны и оператора):
   ```
   sudo dpkg -i tad-db-system-ref-books_*.deb
   ```

Это позволяет заполнить созданные таблицы базы данных содержимым.

База данных СОПТА установлена.

4.3.2. Установка коррелятора

- Чтобы установить коррелятор СОПТА, выполните следующие действия:

1. Установите пакет Correlator:
   ```
   sudo dpkg -i tad-correlator_*.deb
   ```
   Примечание. Если при обработке пакета обнаруживаются ошибки зависимости, устраните их:
   ```
   sudo apt-get -f install
   ```
2. Запустите Sensor и настройте его на автоматический запуск при запуске системы:
   ```
   sudo systemctl enable ptdpi
   sudo systemctl start ptdpi
   ```

Коррелятор СОПТА установлен.

4.3.3. Установка пакета локализации

- Чтобы установить пакет локализации,

  выполните команду:
  ```
  sudo dpkg -i tad-locales_*.deb
  ```

Примечание. Если интерфейс пользователя и серверное приложение установлены на разных серверах, установите пакет локализации на каждом из них.

4.3.4. Установка серверного приложения

- Чтобы установить серверного приложения СОПТА, выполните следующие действия:

1. Установите сторонние компоненты, необходимые для серверного приложения:

   Примечание. Если при обработке пакета обнаруживаются ошибки зависимости, устраните их:
   ```
   sudo apt-get -f install
   ```
2. Установите пакет серверного приложения:

Серверное приложение СОПТА установлено.

4.3.5. Установка интерфейса пользователя

- Чтобы установить интерфейс пользователя СОПТА, сделайте следующее:

  1. Установите пакет документации:
     ```
     sudo dpkg -i tad-documentation_*.deb
     ```
  2. Перезагрузите веб-сервер:
     ```
     sudo systemctl restart nginx.service
     ```

4.3.6. Установка межсетевого экрана SS7

- Чтобы установить межсетевой экран SS7,

  установите deb-пакет SS7 Firewall:
  ```
  sudo dpkg -i tad-fw_*.deb
  ```

  Примечание. Если при обработке пакета обнаруживаются ошибки зависимости, устраните их:
  ```
  sudo apt-get -f install
  ```

  Модуль SS7 Firewall установлен.

4.3.7. Установка межсетевого экрана Diameter

- Чтобы установить межсетевой экран Diameter,

  установите deb-пакет межсетевого экрана Diameter:
  ```
  sudo dpkg -i tad-fw-diameter_*.deb
  ```

  Примечание. Если при обработке пакета обнаруживаются ошибки зависимости, устраните их:
  ```
  sudo apt-get -f install
  ```

  Межсетевой экран Diameter установлен.

О компании

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

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

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com