Radware DefencePro

?????????? ?? ?????????

Radware DefensePro — это аппаратно-программная платформа защиты сети, предназначенная для предотвращения DDoS-атак, обнаружения аномалий трафика и защиты сервисов на уровнях L2–L7. Устройство обеспечивает анализ трафика в реальном времени, применяет поведенческие и сигнатурные модели, автоматически блокирует сетевые атаки и передаёт информацию о состоянии защищаемой инфраструктуры.

Типы собираемых событий:

- Обнаружение и фиксация сетевых атак (Attack Start / Attack Update / Attack End)
- Поведенческие события и аномалии трафика
- Системные и аппаратные события (Health / System Status)
- События безопасности и протокольных нарушений
- Аудит действий пользователей

????????? ???????? ??????? ????? Syslog

Для интеграции Radware DefensePro с внешними системами мониторинга и SIEM необходимо настроить передачу событий по протоколу Syslog.

Ниже представлены два поддерживаемых способа конфигурирования: через интерфейс **APSolute Vision** и через **Web UI DefensePro**. Вы можете использовать любой из методов в зависимости от доступного интерфейса управления устройством

????????? ????? APSolute Vision

1. В интерфейсе APSolute перейдите в:
   "Configuration" > "Setup" → "Reporting Settings" → "Syslog"

   > В ряде версий APSolute OS 10.x путь к настройкам syslog может отображаться как **"Setup" > "System" > "Logging" > "Syslog"**.Это связано только с изменением структуры меню.

   Функциональность настройки syslog полностью соответствует инструкции

2. Установите флажок **"Enable Syslog"**
3. Выполните одно из действий:
   - Чтобы добавить новый syslog-сервер, нажмите кнопку **"Add"**.
   - Чтобы изменить существующую запись, дважды щёлкните по ней в таблице.
4. Заполните следующие параметры, в соответствии с конфигруацией и требованиями вашей SIEM, и нажмите **"Submit":**

- **"Enable Syslog Server"** — включает или отключает отправку сообщений.
- **"Syslog Server"** — IP-адрес сервера, принимающего syslog (SIEM).
- **"Source Port"** — порт, который DefensePro использует для отправки сообщений.
  - По умолчанию: **514**
  - Значение **0** означает использование случайного порта.
- **"Destination Port"** — порт на стороне SIEM, принимающий syslog-сообщения.
  - По умолчанию: **514**
- **"Facility"** — категория syslog-сообщений.
  - По умолчанию: **Local Use 6**
- **"Protocol"** — выбирается протокол передачи сообщений (выберите **UDP**)
- Убедитесь, что включены все типы отчётов:
  - **"Send Security-Event Reports to Syslog"** — отправка событий безопасности и атак.
  - **"Send Health-Event Reports to Syslog"** — отправка событий состояния системы и оборудования.
  - **"Send Audit-Event Reports to Syslog"** — отправка аудита действий пользователей.

> "**Syslog Server CA Certificate**" — используется только при передаче syslog поверх TLS (Syslog over TLS). При использовании UDP или обычного TCP это поле не заполняется.

????????? ????? Web UI DefensePro

1. Войдите в Web UI DefensePro.
2. Перейдите **"Services" → "Syslog Reporting"**
3. В поле **"Syslog Server Operational Status"** выберите **"Enabled"**.
4. Нажмите **"Create"**, чтобы добавить новую запись, или выберите существующую для редактирования.
5. Заполните следующие параметры, в соответствии с конфигруацией и требованиями вашей SIEM, ****и нажмите **"Set":**
   - **"Syslog Server"** — IP-адрес сервера SIEM/syslog.
   - **"Syslog Server Source Port"** — исходящий порт DefensePro (обычно **514**).
   - **"Syslog Server Destination Port"** — порт приёма на SIEM (обычно **514**).
   - **"Syslog Server Facility"** — оставьте **Local Use 6**, если нет иных требований.
   - **"Syslog Server Protocol"** — выберите **"UDP Protocol"**.
   - **"Syslog Health Sending"** — **"Enabled"**, отправка системных событий.
   - **"Syslog Security Sending"** — **"Enabled"**, отправка security/attack событий.
   - **"Syslog User Audit Sending"** — **"Enabled"**, отправка аудита действий пользователей.

>

> "**Syslog Server CA Certificate**" — используется только при передаче syslog поверх TLS (Syslog over TLS). При использовании UDP или обычного TCP это поле не заполняется.

Revision #1
Created 2026-05-25 10:38:47 UTC by lerat
Updated 2026-05-25 10:42:29 UTC by lerat