

Ограничение на количество SNMP-trap

Для связи с оборудованием AxelINAC в основном использует SNMP-trap. В связи с тем, что trap, поступающие от разрешенных (skonfigurirovannykh) устройств, обрабатываются демоном, поэтому злоумышленник, желая создать определенную нагрузку на сервер AxelINAC, может заставить его генерировать нелегитимные SNMP-trap, или коммутатор может случайно сгенерировать большое количество trap, отправляемых в AxelINAC по неизвестной причине.

Для закрытия такой уязвимости можно ограничить количество SNMP-trap, поступающих с одного порта коммутатора, и принять меры при достижении этого предела. Например, если в течение минуты AxelINAC получит более 100 trap с одного порта коммутатора, порт коммутатора будет закрыт, а администратору будет отправлено уведомление по электронной почте.

Для того, чтобы выполнить настройку, в веб-интерфейсе AxelINAC перейдите в раздел **Конфигурация → Сетевое взаимодействие → SNMP**.

ID статьи: 641

Последнее обновление: 3 окт., 2024

Обновлено от: Егоров В.

Ревизия: 4

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.0.1 -> AxelINAC. Руководство администратора -> Оптимизация производительности -> Ограничение на количество SNMP-trap

<https://docs.axel.pro/entry/641/>