Ограничение на количество SNMP-trap

Для связи с оборудованием AxelNAC в основном использует SNMP-trap. В связи с тем, что trap, поступающие от разрешенных (сконфигурированных) устройств, обрабатываются демоном, поэтому злоумышленник, желая создать определенную нагрузку на сервер AxelNAC, может заставить его генерировать нелегитимные SNMP-trap, или коммутатор может случайно сгенерировать большое количество trap, отправляемых в AxelNAC 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 AxelNAC 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 AxelNAC перейдите в раздел **Конфигурация → Сетевое взаимодействие → SNMP**.

ID статьи: 100
Последнее обновление: 3 окт., 2024
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Оптимизация производительности -> Ограничение на количество SNMP-trap
https://docs.axel.pro/entry/100/