Общие сведения

Одной из важных ключевых концепций решений NAC является разграничение доступа к сети. Например, сотрудник финансового отдела не может иметь тот же уровень доступа к сети, что и сотрудник отдела маркетинга. Гости также не должны иметь тот же уровень доступа, что и обычные сотрудники организации.

Для идентификации и разграничения пользователей в AxelNAC используются роли. AxelNAC может разграничивать доступ к сети используя один или все следующие методы на базе:

- списка управления доступом ACL;
- виртуальных сетей (VLAN).

Выбор метода зависит от типа соединения: проводного или Wi-Fi. Роль в AxelNAC в конечном итоге будет сопоставлена с VLAN или ACL. Необходимо определить, какие роли будут использоваться в организации для доступа к сети.

AxelNAC динамически вычисляет роли на основе правил аутентификации (т. е. набора условий и действий). При этом используется первое правило, которое удовлетворяет указанным критериям. Затем роли сопоставляются с VLAN или пулом VLAN, или внутренними ролями, или ACL на оборудовании из модуля. Для пула VLAN вместо определения идентификатора VLAN можно задать, например, такое значение: **20..23,27..30**. Это означает, что VLAN, которые возвращает AxelNAC, могут принимать значения от 20 до 23 и от 27 до 30 (включительно).

ID статьи: 556
Последнее обновление: 3 июл., 2024
Обновлено от: Егоров В.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Управление доступом к сети на основе ролей -> Общие сведения
https://docs.axel.pro/entry/556/