Определение сетевых устройств

Определение используется только для принудительного назначения VLAN. В режиме Inline данный функционал недоступен.

AxelNAC необходимо знать, какими коммутаторами, точками доступа или контроллерами она управляет, их тип и конфигурацию. Изменить эту конфигурацию можно из веб-интерфейса в разделе **Политики и контроль доступа → Сетевые устройства**.

Раздел сетевого устройства для каждого сетевого устройства (управляемого AxelNAC), включает в себя:

- IP/MAC/диапазон сетевого устройства;
- поставщик/тип сетевого устройства;
- порты uplink сетевого устройства (магистральные и неуправляемые IfIndex);
- переопределение VLAN для каждого сетевого устройства (при необходимости).

Любые порты, объявленные как uplink, игнорируются и не управляются AxelNAC. Этот параметр настраивается во вкладке **Определение** окна конфигурации сетевого устройства. Для каждого сетевого устройства может быть задан свой список uplink.

Режимы работы

Сетевые устройства используют три различных режима работы:

- **Тестирование:** служба **pfsetvlan** записывает в лог-файлы все, что происходит на сетевом устройстве, но при этом никакие изменения VLAN не происходят.
- **Регистрация:** служба **pfsetvlan** автоматически регистрирует все MAC-адреса, видимые на портах сетевого устройства, но при этом никакие изменения VLAN не происходят.
- **Продуктивный:** служба **pfsetvlan** отправляет SNMP-записи для изменения VLAN на портах сетевого устройства.

RADIUS

Чтобы задать секретную фразу RADIUS, определите ее в веб-интерфейсе при добавлении сетевого устройства.

Секретная фраза RADIUS необходима для поддержки динамической аутентификации RADIUS (CoA или Disconnect), как определено в RFC3576.

SNMPv1, v2c и v3

Для связи с большинством сетевых устройств используется протокол SNMP. AxelNAC поддерживает SNMPv3, который используется для двунаправленного обмена данными: от сетевого устройства к AxelNAC и от AxelNAC к сетевому устройству. Рекомендуется использовать SNMP только для сетевых устройств, которые некорректно взаимодействуют с AxelNAC.

От AxelNAC к сетевому устройству

На вкладке **SNMP** окна конфигурации сетевого устройства установите следующие параметры:

SNMPVersion = 3
SNMPEngineID = AA5ED139B81D4A328D18ACD1
SNMPUserNameRead = readUser
SNMPAuthProtocolRead = MD5
SNMPAuthPasswordRead = authpwdread
SNMPPrivProtocolRead = AES
SNMPPrivPasswordRead = privpwdread
SNMPUserNameWrite = writeUser
SNMPAuthProtocolWrite = MD5
SNMPAuthPasswordWrite = authpwdwrite
SNMPPrivProtocolWrite = AES
SNMPPrivPasswordWrite = privpwdwrite

От сетевого устройства к AxelNAC

На вкладке **SNMP** окна конфигурации сетевого устройства установите следующие параметры:

SNMPVersionTrap = 3
SNMPUserNameTrap = readUser
SNMPAuthProtocolTrap = MD5
SNMPAuthPasswordTrap = authpwdread
SNMPPrivProtocolTrap = AES
SNMPPrivPasswordTrap = privpwdread

Конфигурация сетевого устройства

Чтобы включить SNMPv3 в обоих направлениях на сетевом устройстве Cisco, выполните следующую конфигурацию:

snmp-server engineID local AA5ED139B81D4A328D18ACD1
snmp-server group readGroup v3 priv
snmp-server group writeGroup v3 priv read v1default write v1default snmp-server user readUser readGroup v3 auth md5 authpwdread priv aes 128 privpwdread
snmp-server user writeUser writeGroup v3 auth md5 authpwdwrite priv aes 128 privpwdwrite
snmp-server enable traps port-security snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.0.50 version 3 priv readUser port-security

Получить идентификатор движка SNMPv3 (SNMPEngineID) можно с помощью команды show snmp engineid.

Тестирование связи с сетевым устройством

Пакет net-snmp позволяет протестировать SNMPv3-связь с сетевым устройством:

snmpget -v3 -l authPriv -u readUser -a MD5 -A "authpwdread"
-x AES -X "privpwdread" IP-АДРЕС_СЕТЕВОГО_УСТРОЙСТВА sysName.0

Длина пароля должна составлять не менее 8 символов.

Интерфейс командной строки: Telnet и SSH

В некоторых случаях AxelNAC может устанавливать интерактивный сеанс командной строки с сетевым устройством. Для этого можно использовать протоколы **Telnet** и **SSH**. Перейдите на вкладку CLI окна конфигурации сетевого устройства, выберите транспортный протокол и укажите учетные данные для доступа.

Интерфейс веб-служб

AxelNAC может периодически устанавливать диалог веб-служб с сетевым устройством. Для этого перейдите на вкладку**Веб-службы** окна конфигурации сетевого устройства, выберите транспортный протокол и укажите учетные данные для доступа.

Трансляция ролей сетевым устройствам

Некоторые сетевые устройства поддерживают назначение пользователю определенного набора правил (межсетевых экранов или ACL). Эти правила более точно контролируют, что может или не может делать пользователь, по сравнению с VLAN, которая неэффективно много тратит на управление сетью. AxelNAC может назначать роли на коммутаторах и контроллерах Wi-Fi, которые поддерживают назначение на основе ролей.

Для этого обеспечьте назначение внутренних и внешних ролей либо на сетевом устройстве, либо в родительской группе сетевых устройств, с помощью веб-интерфейса AxelNAC в разделе **Конфигурация → Политики и контроль доступа → Сетевые устройства** .

Предварительно убедитесь, что роли определены в сетевых устройствах.

Интеграция VoIP с CDP, LLDP и LLDP-MED

Для целей определения абонентских устройств IP-телефонии система AxelNAC использует данные, получаемые по двум протоколам: CDP и LLDP.

Cisco Discovery Protocol (CDP) — это проприетарный протокол обнаружения устройств, поддерживаемый на всем оборудовании Cisco, включая маршрутизаторы, серверы доступа, мосты и коммутаторы. С помощью CDP устройство может объявить о своем существовании другим устройствам и получить информацию о других устройствах в той же локальной сети или на удаленной стороне глобальной сети.

CDP может определить, является ли подключаемое устройство IP-телефоном, и дать ему указание маркировать кадры Ethernet с помощью настроенной голосовой VLAN на коммутационном порту.

Многие производители поддерживают LLDP или LLDP-MED. Link Layer Discovery Protocol (LLDP) — это открытый протокол канального уровня из набора интернет протоколов, используемый сетевыми устройствами для оповещения о своей идентичности, возможностях и соседях. Как и CDP, LLDP может указывать IP-телефону, какой VLAN ID является голосовым.

Поддержка данных протоколов реализована в рамках двух сценариев взаимодействия:

- **Активный опрос (Polling)** — система AxelNAC инициирует активный сбор информации при подключении устройства к сети, осуществляя запросы к сетевым коммутаторам по протоколу SNMP. В ходе опроса запрашиваются данные, полученные коммутаторами от конечных устройств через протоколы LLDP и CDP;
- **Пассивный прием уведомлений (SNMP-Trap)** — сетевое оборудование активно направляет в сторону системы AxelNAC асинхронные уведомления по протоколу SNMP-Trap. Данные уведомления генерируются при обнаружении коммутаторами LLDP-фреймов или CDP-фреймов от абонентских устройств и передаются для обработки в реальном времени.

Таким образом, комбинация активного опроса и пассивного приема SNMP-trap обеспечивает комплексный и оперативный сбор необходимой информации для точной идентификации IP-телефонов.

VoIP и назначение VLAN

В AxelNAC поддержаны различные методы назначения VLAN, такие как port-security, MAC-аутентификация и 802.1X.

Port-security

При использовании port-security VoIP-устройство на основе CDP/LLDP маркирует Ethernet-кадры, используя настроенную голосовую VLAN на порту коммутатора. После этого из голосовой VLAN посылается port-security trap, чтобы AxelNAC мог авторизовать MAC-адрес порта. Когда устройство подключается, еще один port-security trap отправляется из VLAN данных. Таким образом, один MAC-адрес авторизуется в голосовой VLAN, а один — во VLAN доступа.

VoIP с помощью функции port-security поддерживается не всеми вендорами.

MAC-аутентификация и 802.1X

Коммутаторы Cisco поддерживают многодоменную конфигурацию с использованием атрибутов конкретного поставщика (Vendor-Specific Attributes, VSA), что позволяет использовать одно устройство в домене VOICE и одно устройство в домене DATA.

Когда телефон подключается к порту коммутатора, AxelNAC отвечает только правильными VSA, без туннельных атрибутов RADIUS. Затем CDP дает телефону указание помечать Ethernet-кадры, используя настроенную голосовую VLAN на порту коммутатора.

Когда подключается персональный компьютер, сервер RADIUS возвращает туннелированные атрибуты, и коммутатор помещает порт в предоставленную VLAN доступа.

На оборудовании других производителей VoIP работает с использованием RADIUS VSA. Когда IP-телефон подключается к порту коммутатора, возвращается соответствующий VSA, чтобы проинструктировать коммутатор разрешить ли прием тегированных кадров от этого устройства. При подключении ПК AxelNAC возвращает коммутатору стандартные атрибуты туннеля RADIUS для нетегированной VLAN.

Алгоритм действий при отсутствии поддержки CDP/LLDP

Если IP-телефон не поддерживает CDP или LLDP, то для предоставления устройству голосовой VLAN можно использовать DHCP.

Для некоторых моделей требуется определенная опция DHCP, чтобы DHCP-сервер предоставил устройству идентификатор голосовой VLAN. После

перезагрузки Ethernet-кадры маркируются с использованием предоставленного тега VLAN.

Чтобы этот сценарий работал: регистрационный и продуктивный DHCP-серверы должны быть настроены на предоставление опции DHCP; на порту настроена голосовая VLAN, а IP-телефоны должны автоматически регистрироваться (при первом подключении телефон назначается на регистрационную VLAN).

ID статьи: 624
Последнее обновление: 3 февр., 2025
Обновлено от: Михалева А.
Ревизия: 5
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Расширенная конфигурация сети -> Определение сетевых устройств
https://docs.axel.pro/entry/624/