Интеграция AxelNAC с коммутаторами Eltex MES

В данной статье рассматривается процесс интеграции AxelNAC с коммутаторами Eltex MES.

Убедитесь, что у вас настроена локальная учетная запись администратора на коммутаторе, т.к. после активации 802.1X или MAC-аутентификации коммутатор запросит учетные данные при следующем подключении.

Настройка 802.1x и MAC-авторизации через RADIUS-сервер

Конфигурация RADIUS-сервера

Шаг 1. Для первичной конфигурации необходимо активировать работу RADIUS-сервера. Для этого выполните на коммутаторе следующую команду:

radius server enable

Шаг 2. Выполните конфигурацию RADIUS-сервера и AAA с помощью следующих команд:

```
!
aaa authentication dot1x default radius none
aaa authorization dynamic radius
aaa accounting dot1x start-stop group radius
!
radius-server host 192.168.1.10 encrypted key YourSecret usage all
radius-server host source-interface vlan 999 #Если необходимо явно указать с какого интерфейса должны отправляться запросы на RADIUS-сервер#
```

Конфигурация интерфейсов

Шаг 1. Активируйте поддержку dot1x и CoA с помощью следующих команд:

```
dot1x system-auth-control
aaa authorization dynamic radius
```

Шаг 2. Выполните конфигурацию портов с помощью следующего набора команд:

```
interface gigabitethernet1/0/7 ##
dot1x port-control auto #активация поддержки 802.1x#
dot1x reauthentication #активация регулярной реаутентификации клиентов#
dot1x timeout reauth-period 300 #период реаутентификации 300 секунд#
dot1x host-mode multi-auth #поддержка нескольких одновременных сессий dot1x на одном порте#
dot1x max-hosts 2 #ограничить количество клиентов dot1x на одном порте 2 сессиями#
dot1x authentication mac 802.1x #методы аутентификации и их порядок применения#
dot1x max-login-attempts 5 #количество неуспешных попыток подключения, после которых клиент блокируется#
dot1x critical-vlan enable #поддержка "bypass vlan" в которую направляется клиент при недоступности RADIUS-серверов#
dot1x critical-vlan 100 #указание номера "bypass vlan"#
dot1x radius-attributes vlan static #активация поддержки приема номера vlan от RADIUS-сервера.#
dot1x radius-attributes vendor-specific data-filter #активация поддержки приема номера ACL от RADIUS-сервера#
exit
```

Настройка RADIUS-авторизации администраторов

Если ранее выполнялась настройка 802.1x и MAC-авторизации, пропустите шаги 1 и 2.

Для настройки разграничения доступа к сетевому оборудованию, необходимо выполнить следующие действия:

Шаг 1. Активируйте работу RADIUS-сервера с помощью следующей команды:

console(config)# radius server enable

Шаг 2. Укажите IP-адрес и секретный ключ RADIUS-сервера:

console(config)# radius-server host 192.168.1.10 encrypted key YourSecret usage login

Если вы планируете использовать dot1x, для параметра **usage** укажите значение **all**.

Шаг 3. Установите способ аутентификации для входа в систему по протоколу RADIUS:

console(config)# aaa authentication login authorization default radius local

Шаг 4. Установите способ аутентификации при повышении уровня привилегий:

console(config)# aaa authentication enable default radius enable

Шаг 5. Чтобы не потерять доступ к коммутатору (в случае недоступности RADIUS-сервера), рекомендуется создать учетную запись в локальной базе данных, и задать пароль на привилегированный режим:

```
console(config)# username tester password eltex privilege 15
console(config)# enable password eltex
```

Конфигурация разграничения доступа

Конфигурация групп и привязка к ним уровней привилегий выполняется с помощью следующего набора команд:

```
radius server group admin
vlan name test #для доступа к оборудованию с указанного vlan(опционально)
```

```
privilege-level 15
exit
!
radius server group priv1
privilege-level 1
exit
```

Настройка TACACS-авторизации администраторов

Шаг 1. Укажите IP-адрес и секретный ключ TACACS-сервера:

```
console(config)# tacacs-server host 192.168.10.5 key Secret
```

Шаг 2. Установите способ аутентификации для входа в систему по протоколу TACACS+:

```
console(config)# aaa authentication login authorization default tacacs local
```

Шаг 3. Установите способ аутентификации при повышении уровня привилегий:

```
console(config)# aaa authentication enable default tacacs enable
```

Шаг 4. Чтобы не потерять доступ к коммутатору (в случае недоступности TACACS-сервера), рекомендуется создать учетную запись в локальной базе данных, и задать пароль на привилегированный режим:

```
console(config)# username tester password eltex privilege 15
console(config)# enable password eltex
```

Шаг 5. Разрешите ведение аккаунтинга для сессий управления:

```
console(config)# aaa accounting login start-stop group tacacs+
```

Шаг 6. Активируйте ведение аккаунтинга введенных в CLI команд по протоколу TACACS+:

```
console(config)# aaa accounting commands stop-only group tacacs+
```

Шаг 7. Активируйте авторизацию вводимых команд на TACACS-сервере:

```
console(config)# aaa authorization commands default group tacacs+ local
```

После этого каждая вводимая команда будет проходить авторизацию на сервере.

ID статьи: 164
Последнее обновление: 12 нояб., 2024
Обновлено от: Егоров В.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с коммутаторами Eltex MES
https://docs.axel.pro/entry/164/