Интеграция AxelNAC с коммутаторами Cisco Catalyst 2960, 2970, 3560 и 3750

В данной статье рассматривается процесс интеграции AxelNAC с коммутаторами Cisco Catalyst 2960, 2970, 3560 и 3750.

Не рекомендуется использование функционала Port-Security при активации 802.1X или MAC-аутентификации. Это может вызвать непредвиденное поведение коммутатора.

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.

При использовании 802.1X и агрегации сетевых интерфейсов на одном коммутаторе или стеке возможно использование функции **mac-move**. Когда вы аутентифицируете основное соединение группы интерфейсов, виртуальный MAC-адрес будет опубликован и авторизован на порте коммутатора. При разрыве соединения на данном интерфейсе (например, при отключении физического кабеля), драйвер группы опубликует MAC-адрес на другом интерфейсе группы, и коммутатор попытается его авторизовать. Однако, поскольку коммутатор уже имеет этот MAC-адрес в сессии на другом коммутационном порту, он переведет интерфейс в режим **err-disabled**.
Чтобы предотвратить такое поведение, необходимо разрешить коммутатору перемещение MAC-адресов между портами. Для этого используйте команду **authentication mac-move permit**.

Глобальные настройки

Шаг 1. Для первичной конфигурации выполните следующий набор команд:

```
dot1x system-auth-control
aaa new-model
aaa group server radius anac
 server name anac
aaa authentication login default local
aaa authentication dot1x default group anac
aaa authorization network default group anac
```

Шаг 2. Сконфигурируйте RADIUS-сервер:

```
radius server anac
  address ipv4 192.168.1.5 auth-port 1812 acct-port 1813
  automate-tester username dummy ignore-acct-port idle-time 3
  key 0 useStrongerSecret
radius-server vsa send authentication
```

Шаг 3. Настройте использование CoA (функционал CoA не поддерживается на коммутаторах Cisco 2960+, описание реаутентификации описано в секции ниже):

```
aaa server radius dynamic-author
 client 192.168.1.5 server-key useStrongerSecret
 port 3799
```

Шаг 4. Активируйте SNMP на коммутаторе:

```
snmp-server community public RO
```

Конфигурация коммутатора для аутентификации по стандарту 802.1X с функционалом MAB

Для настройки аутентификации по стандарту 802.1X с поддержкой MAB, выполните на каждом интерфейсе, который планируется использовать, следующий набор команд:

```
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 7200
authentication violation replace
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
```

Конфигурация коммутатора для аутентификации по стандарту 802.1X с функционалом MAB (для реализации VoIP)

Для настройки аутентификации по стандарту 802.1X с поддержкой MAB, для аутентификации VoIP-устройств, выполните на каждом интерфейсе, который планируется использовать, следующий набор команд:

```
switchport mode access
switchport voice vlan 100
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 7200
authentication violation replace
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
```

Конфигурация MAB

Для того чтобы настроить только функционал MAB, выполните на каждом интерфейсе, который планируется использовать, следующий набор команд:

```
switchport mode access
switchport voice vlan 100
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout tx-period 5
dot1x reauthentication
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 7200
authentication violation replace
mab
no snmp trap link-status
```

Процесс конфигурации MAB может отличаться для разных версий ПО коммутаторов Cisco Catalyst 2960. Обратитесь к официальной документации Cisco для актуального описания настройки.

Конфигурация веб-аутентификации

Настройка порта коммутатора для веб-аутентификации

Для того чтобы веб-аутентификация в AxelNAC стала доступной, необходимо настроить порт коммутатора. Выполните следующие действия:

Шаг 1. Подключитесь к коммутатору по протоколу SSH как администратор.

Шаг 2. Включите функцию **Change-of-Authorization (CoA)** в конфигурации коммутатора.

Шаг 3. Разрешите серверу AxelNAC (172.20.100.2) посылать CoA-запросы на коммутатор:

```
aaa server radius dynamic-author
client 172.20.100.2 server-key useStrongerSecre
port 3799
```

Шаг 4. Включите веб-аутентификацию в глобальной конфигурации коммутатора. Для этого добавьте следующую конфигурацию в глобальную секцию:

```
ip device tracking
ip http server
ip http secure-server
```

Шаг 5. Добавьте ACL, который будет перенаправлять трафик на портал AxelNAC:

```
ip access-list extended registration
deny ip any host 172.20.100.2
permit tcp any any eq www
permit tcp any any eq 443
```

Настройка конфигурации коммутатора в AxelNAC

После того, как порт коммутатора настроен для веб-аутентификации, необходимо сообщить AxelNAC, что она будет использоваться на данном коммутаторе. Для этого выполните следующие действия

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Сетевые устройства** .

Шаг 2. Кликните по IP-адресу коммутатора, чтобы открыть параметры его конфигурации.

Шаг 3. На вкладке **Определение** активируйте параметр **Обеспечение работы внешнего портала**.

Шаг 4. Переключитесь на вкладку **RADIUS** и активируйте параметр **Использовать CoA**, а также установите значение параметра **CoA-порт** равным **3799**.

Шаг 5. На вкладке **Роли** внесите следующие изменения:

- в блоке **Назначение VLAN ID** установите для регистрационной и гостевой VLAN значение 20. Это позволит незарегистрированным клиентам изначально попадать в VLAN 20 и избежать смены VLAN после успешной аутентификации через Captive-портал;
- в блоке **Назначение Local ACL** активируйте параметр **Назначать Local ACL** и установите для роли регистрации значение registration (имя ACL на коммутаторе, созданное в шаге 5 предыдущей секции). Это обеспечит перенаправление веб-трафика пользователя на Captive-портал AxelNAC.
- в блоке **Назначение URL веб-аутентификации** активируйте параметр **Назначать URL веб-аутентификации** и установите URL регистрации http://172.20.100.2/Cisco::Catalyst_2960/.

Шаг 6. Сохраните все изменения конфигурации, нажав **Сохранить**.

Активация назначения Local ACL и Downloadable ACL из AxelNAC

Общие настройки

Коммутаторы Cisco поддерживают RADIUS pushed ACLs, что означает, что вы можете назначать ACL напрямую из AxelNAC, не настраивая их в своих коммутаторах, и их правила будут применяться к коммутатору во время аутентификации. Эти ACL определяются по ролям, как и VLAN, что означает, что вы можете определить различные ACL для регистрационной VLAN, продуктивной VLAN, гостевой VLAN и т. д.

Для активации данного функционала выполните следующую команду:

```
ip device tracking
```

Cisco IOS 12

Для реализации работы функционала прямого назначения ACL в коммутаторах Cisco, управляемых программным обеспечением Cisco IOS 12.2 и старше, необходимо выполнить следующие действия:

Шаг 1. Создайте специальный ACL для работы портов до аутентификации:

```
ip access-list extended Auth-Default-ACL
 permit udp any range bootps 65347 any range bootpc 65348
 permit udp any any range bootps 65347
 permit udp any any eq domain
 deny   ip any any
```

Шаг 2. Назначьте данный ACL интерфейсу порта коммутатора:

```
interface GigabitEthernetx/y/z
 ...
 ip access-group Auth-Default-ACL in
 ...
```

Конфигурация реаутентификации на коммутаторах Cisco Catalyst 2960+

Коммутаторы Cisco Catalyst 2960+ не поддерживают функционал CoA. Для реализации реаутентификации выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Сетевые устройства** , и выберите коммутатор, в который вы хотите внести изменения.

Шаг 2. На вкладке **Определение** активируйте параметр **Реаутентификация на предыдущем сетевом устройстве**. В качестве метода реаутентификации выберите протокол **SSH**.

Шаг 3. Перейдите на вкладку **CLI** и выберите **SSH** в качестве транспортного протокола.

Коммутаторы Cisco Catalyst 2960+, в зависимости от конфигурации, поддерживают не более 15 одновременных SSH-соединений. Не допускайте большего количества одновременных реаутентификаций, т.к. остальные соединения не будут обработаны из-за блокировки сокета.

ID статьи: 1045
Последнее обновление: 25 июл., 2025
Обновлено от: Михалева А.
Ревизия: 7
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с коммутаторами Cisco Catalyst 2960, 2970, 3560 и 3750
https://docs.axel.pro/entry/1045/