Интеграция AxelNAC с контроллерами беспроводного доступа Mikrotik

В данной статье рассматривается процесс интеграции AxelNAC с оборудованием Mikrotik.

AxelNAC поддерживает оборудование Mikrotik (RouterOS) для организации беспроводной аутентификации 802.1X (WPA2-Enterprise и MAC-аутентификация) и проводной аутентификации 802.1X (EAPoL (Extensible Authentication Protocol over LAN)).

Требования для интеграции

Данная конфигурация была протестирована на различных устройствах MikroTik, включая **RB433AH**, **hAP ac**, **hAP ac lite**, **RB1100**, **RB3011** и различные устройства **CCR**.

MikroTik поддерживает беспроводную аутентификацию RADIUS 802.1X в RouterOS 6.x и более поздних версиях. Проводная аутентификация EAPoL (802.1X) доступна с версии 6.46 (декабрь 2019), а запасной вариант MAB стабилен с версии 6.48.3. На момент написания статьи **RADIUS Disconnect** поддерживается для беспроводной аутентификации 802.1X, но для проводной аутентификации 802.1X (dot1x) данная функциональность недоступна.

Для бесплатного обновления программного обеспечения RouterOS вы можете использовать команды **/system package update install** и **/system routerboard upgrade**.

По умолчанию AxelNAC использует RADIUS для деаутентификации беспроводных устройств. Если вы предпочитаете использовать SSH как метод деаутентификации, измените строку '**my $default = $SNMP::RADIUS;**' на '**my $default = $SNMP::SSH;**'.

Если вы используете метод деаутентификации SSH, необходимо подключиться с учетной записи **axelnac** по SSH к точке доступа, для того чтобы получить SSH-ключ.

Настройка WPA2-EAP (WPA2 Enterprise) 802.1X SSID с MAC-аутентификацией на WPA2-PSK SSID

В данном примере интерфейсы с частотами 2,4 и 5 ГГц сконфигурированы для обеспечения беспроводной аутентификации 802.1X с виртуальной точкой доступа, которая добавляется для обеспечения MAC-аутентификации на WPA2-PSK SSID, где пароль указывается как часть SSID.

Несмотря на то, что Pre-Shared Key является публичным, каждое беспроводное соединение шифруется с использованием динамически сгенерированного ключа. Чтобы настроить WPA2-EAP (WPA2 Enterprise) 802.1X SSID с MAC-аутентификацией на WPA2-PSK SSID, выполните следующие действия:

Шаг 1. Создайте SSID и виртуальную точку доступа для второго SSID:

```
/interface wireless security-profiles
  add authentication-types=wpa2-eap disable-pmkid=yes interim-update=15m management-protection=allowed mode=dynamic-keys name=radius-eap \
    radius-eap-accounting=yes supplicant-identity=""
  add authentication-types=wpa2-psk disable-pmkid=yes eap-methods="" interim-update=15m management-protection=allowed mode=dynamic-keys name=\
    radius-mac radius-mac-accounting=yes radius-mac-authentication=yes supplicant-identity="" wpa2-pre-shared-key="internet"
/interface wireless
  set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20mhz country="south africa" disabled=no frequency=auto mode=ap-bridge name=\
    "wlan1 - 2.4 GHz - ACME WiFi" security-profile=radius-eap skip-dfs-channels=all ssid="ACME WiFi" station-roaming=enabled vlan-id=3999 \
    vlan-mode=use-tag wireless-protocol=802.11 wps-mode=disabled
  add disabled=no master-interface="wlan1 - 2.4 GHz - ACME WiFi" multicast-helper=full name="wlan1 - 2.4 GHz - ACME Guest" \
    security-profile=radius-mac ssid="ACME Guest (pw: internet)" station-roaming=enabled vlan-id=3999 vlan-mode=use-tag wps-mode=disabled
  set [ find default-name=wlan2 ] band=5ghz-a/n/ac channel-width=20/40/80mhz-Ceee country="south africa" disabled=no frequency=auto mode=ap-bridge \
    name="wlan2 - 5 GHz - ACME WiFi" security-profile=radius-eap skip-dfs-channels=all ssid="ACME WiFi" station-roaming=enabled vlan-id=3999 \
    vlan-mode=use-tag wireless-protocol=802.11 wps-mode=disabled
  add disabled=no master-interface="wlan2 - 5 GHz - ACME WiFi" multicast-helper=full name="wlan2 - 5 GHz - ACME Guest" \
    security-profile=radius-mac ssid="ACME Guest (pw: internet)" station-roaming=enabled vlan-id=3999 vlan-mode=use-tag wps-mode=disabled
```

VLAN 3999 используется как фиктивная и служит для блокирования доступа до момента, пока RADIUS-сервер не вернет клиенту корректную VLAN в ответе.

Шаг 2. Далее создайте **bridge** с фильтрацией VLAN:

```
/interface bridge
  add name=bridge vlan-filtering=yes
/interface bridge port
  add bridge=bridge interface="wlan1 - 2.4 GHz - ACME WiFi"
  add bridge=bridge interface="wlan2 - 5 GHz - ACME WiFi"
  add bridge=bridge interface="wlan1 - 2.4 GHz - ACME Guest"
  add bridge=bridge interface="wlan2 - 5 GHz - ACME Guest"
/interface bridge vlan
  add bridge=bridge tagged="bridge,wlan1 - 2.4 GHz - ACME WiFi,wlan2 - 5 GHz - ACME WiFi,wlan1 - 2.4 GHz - ACME Guest,wlan2 - 5 GHz - ACME Guest" vlan-ids=52
  add bridge=bridge tagged="bridge,wlan1 - 2.4 GHz - ACME WiFi,wlan2 - 5 GHz - ACME WiFi,wlan1 - 2.4 GHz - ACME Guest,wlan2 - 5 GHz - ACME Guest" vlan-ids=666
  add bridge=bridge tagged="bridge,wlan1 - 2.4 GHz - ACME WiFi,wlan2 - 5 GHz - ACME WiFi,wlan1 - 2.4 GHz - ACME Guest,wlan2 - 5 GHz - ACME Guest" vlan-ids=667
```

Шаг 3. Создайте VLAN и назначьте IP-адреса:

```
/interface vlan
  add comment="Guest WiFi:" interface=bridge name=vlan52 vlan-id=52
  add comment="PacketFence - Registration:" interface=bridge name=vlan666 vlan-id=666
  add comment="PacketFence - Isolation:" interface=bridge name=vlan667 vlan-id=667
/ip address
  add address=172.16.20.1/24 interface=bridge
  add address=10.239.239.1/24 interface=vlan52
  add address=192.168.10.225/28 interface=vlan666
  add address=192.168.10.241/28 interface=vlan667
```

Адрес 172.16.20.1 фактически назначен на VLAN 1 (untagged).

Шаг 4. Добавьте настройки, которые определяют AxelNAC как RADIUS-сервер и фильтруют трафик в гостевых, регистрационных и изоляционных сетях:

```
/radius
  add address=<IP-адрес AxelNAC> comment=axelnac: secret=useStrongerSecret service=wireless src-address=172.16.20.1 timeout=1s
```

```
/radius incoming
  set accept=yes
/ip dhcp-relay
  add dhcp-server=172.31.31.1 disabled=no interface=vlan666 local-address=192.168.10.225 add-relay-info=yes name="AxelNAC - Registration"
  add dhcp-server=172.31.31.129 disabled=no interface=vlan667 local-address=192.168.10.241 add-relay-info=yes name="AxelNAC - Isolation"
/ip firewall address-list
  add address=10.0.0.0/8 list=local
  add address=172.16.0.0/12 list=local
  add address=192.168.0.0/16 list=local
/ip firewall filter
  add action=reject chain=forward comment="Limit WiFi - Guest:" dst-address=!41.1.1.1 dst-address-list=local in-interface=vlan52
  add action=reject chain=forward comment="Limit AxelNAC - Registration:" dst-address=!172.31.31.1 in-interface=vlan666
  add action=reject chain=forward comment="Limit AxelNAC - Isolation:" dst-address=!172.31.31.129 in-interface=vlan667
```

Параметр '**src-address**' позволяет инициировать запросы с IP-адреса, отличного от адреса интерфейса, через который идет маршрут к AxelNAC. 172.31.31.1 — адрес маршрутизированной регистрационной сети, а 172.31.31.129 — адрес маршрутизированной изоляционной сети.

Шаг 5. Выполните конфигурацию AxelNAC:

```
/usr/local/pf/conf/switches.conf
  [default]
  guestVlan=52
  registrationVlan=666
  isolationVlan=667
  always_trigger=1

  _
  [group MikroTik]
  description=Default MikroTik Settings
  deauthMethod=RADIUS
  type=Mikrotik
  uplink_dynamic=0
  useCoA=N

  _
  [100.127.255.10]
  description=ACME - Home Office - Bar
  group=MikroTik
  radiusSecret=useStrongerSecret
```

Настройка проводной аутентификации 802.1X с MAB (MAC authentication bypass)

Для настройки требуется **bridge** с включенной фильтрацией VLAN и активным **Spanning Tree Protocol**. Новые **bridge** по умолчанию используют **RSTP (Rapid Spanning Tree Protocol)**, поэтому для настройки можно применять те же шаги, что и для беспроводной аутентификации 802.1X.

Для настройки проводной аутентификации 802.1X с MAB (MAC authentication bypass) выполните следующие действия:

Шаг 1. Настройте AxelNAC RADIUS-сервер для dot1x:

```
/radius
  add address=<IP-адрес AxelNAC> comment=axelnac: secret=useStrongerSecret service=dot1x src-address=172.16.20.1 timeout=1s
```

Шаг 2. Добавьте Ethernet-порты к **bridge**:

```
/interface bridge port
  add bridge=bridge interface=ether2
  add bridge=bridge interface=ether3
  add bridge=bridge interface=ether4
  add bridge=bridge interface=ether5
```

Интерфейс **ether1** используется как **uplink**, поэтому не используется в **bridge**.

Шаг 3. Включите 802.1X для интерфейсов с MAB Fallback:

```
/interface dot1x server
  add auth-types=dot1x,mac-auth interface=ether2 interim-update=15m
  add auth-types=dot1x,mac-auth interface=ether3 interim-update=15m
  add auth-types=dot1x,mac-auth interface=ether4 interim-update=15m
  add auth-types=dot1x,mac-auth interface=ether5 interim-update=15m
```

Настройка открытого SSID

Для настройки выполните следующие действия:

Шаг 1. Настройте точку доступа с помощью следующей конфигурации:

```
/interface wireless
# managed by CAPsMAN
# channel: 5180/20-Ce/an(17dBm), SSID: OPEN, local forwarding
set [ find default-name=wlan1 ] band=5ghz-a/n channel-width=20/40mhz-Ce disabled=no l2mtu=1600 mode=ap-bridge ssid=MikroTik-05A64D
/interface ethernet
set [ find default-name=ether1 ] name=ether1-gateway
set [ find default-name=ether2 ] name=ether2-master-local
set [ find default-name=ether3 ] master-port=ether2-master-local name=ether3-slave-local
set [ find default-name=ether4 ] master-port=ether2-master-local name=ether4-slave-local
set [ find default-name=ether5 ] name=ether5-master-local
/interface vlan
add interface=BR-CAPS l2mtu=1594 name=default vlan-id=1
add interface=BR-CAPS l2mtu=1594 name=isolation vlan-id=3
add interface=BR-CAPS l2mtu=1594 name=registration vlan-id=2
/caps-man datapath
add bridge=BR-CAPS client-to-client-forwarding=yes local-forwarding=yes name=datapath1
/caps-man interface
#
```

```
add arp=enabled configuration.mode=ap configuration.ssid=OPEN datapath=datapath1 disabled=no l2mtu=1600 mac-address=\
    D4:CA:6D:05:A6:4D master-interface=none mtu=1500 name=cap1 radio-mac=D4:CA:6D:05:A6:4D
/caps-man aaa
set interim-update=5m
/caps-man access-list
add action=query-radius interface=cap1 radius-accounting=yes signal-range=-120..120 time=0s-1d,sun,mon,tue,wed,thu,fri,sat
/caps-man manager
set enabled=yes
/interface bridge port
add bridge=bridge-local interface=ether2-master-local
add bridge=bridge-local interface=ether1-gateway
add bridge=BR-CAPS interface=ether5-master-local
/interface wireless cap
set bridge=BR-CAPS discovery-interfaces=BR-CAPS enabled=yes interfaces=wlan1
/ip accounting
set enabled=yes
/radius
add address=<IP-адрес вашего Captive-портала AxelNAC> secret=useStrongerSecret service=wireless
/radius incoming
set accept=yes
```

В этой конфигурации интерфейс **ether5** используется как **trunk** для **bridge**, а **ether1** — как интерфейс управления.

Настройка веб-аутентификации

Вы можете использовать веб-аутентификацию на точках доступа Mikrotik. Для этого необходимо активировать **hotspot** в конфигурации точки доступа и изменить шаблон перенаправления так, чтобы он указывал на AxelNAC. Выполните следующие действия:

Шаг 1. Установите FTP-соединение с вашей точкой доступа в файле **hotspot/login.html**:

```
<html>
<head><title>...</title></head>
<body>
$(if chap-id)
<noscript>
<center><b>JavaScript required. Enable JavaScript to continue.</b></center>
</noscript>
$(endif)
<center>If you are not redirected in a few seconds, click 'continue' below<br>
<form name="redirect" action="http://<IP-адрес вашего Captive-портала AxelNAC>/Mikrotik" method="get">
  <input type="hidden" name="mac" value="$(mac)">
  <input type="hidden" name="ip" value="$(ip)">
  <input type="hidden" name="username" value="$(username)">
  <input type="hidden" name="link-login" value="$(link-login)">
  <input type="hidden" name="link-orig" value="$(link-orig)">
  <input type="hidden" name="error" value="$(error)">
  <input type="hidden" name="chap-id" value="$(chap-id)">
  <input type="hidden" name="chap-challenge" value="$(chap-challenge)">
  <input type="hidden" name="link-login-only" value="$(link-login-only)">
  <input type="hidden" name="link-orig-esc" value="$(link-orig-esc)">
  <input type="hidden" name="mac-esc" value="$(mac-esc)">
  <input type="hidden" name="ap-id" value="IP-адрес вашей точки доступа">
  <input type="submit" value="continue">
</form>
<script language="JavaScript">
<!--
   document.redirect.submit();
//-->
</script></center>
</body>
</html>
```

Шаг 2. Настройте **hotspot** на вашей точке доступа. Эта конфигурация сделана поверх существующего SSID, который вы уже настроили на интерфейсе:

```
/ip hotspot
setup
```

В процессе настройки укажите следующие параметры:

```
hotspot interface: wlan1
local address of network: 10.5.50.1/24
masquerade network: yes
```

Скорректируйте имя интерфейса **wlan1** при необходимости.

Шаг 3. Настройте диапазон адресов **hotspot**:

```
address pool of network: 10.5.50.2-10.5.50.254
```

Шаг 4. Выберите SSL-сертификат **hotspot**:

```
select certificate: none
```

Шаг 5. Выберите SMTP-сервер:

```
ip address of smtp server: 0.0.0.0
```

Шаг 6. Настройте конфигурацию DNS:

```
dns servers: 8.8.8.8
```

Шаг 7. Выберите имя DNS локального сервера **hotspot**:

```
dns name: myhotspot
```

Шаг 8. Создайте локального пользователя **hotspot**:

name of local hotspot user: admin
password for the user:

Шаг 9. Разрешите доступ к порталу AxelNAC в списке доступа **hotspot**:

/ip hotspot walled-garden
add dst-host=<IP-адрес вашего Captive-портала AxelNAC>
add src-address=<IP-адрес вашего Captive-портала AxelNAC>

/ip hotspot walled-garden ip
add action=accept disabled=no dst-host=<IP-адрес вашего Captive-портала AxelNAC>
add action=accept disabled=no src-address=<IP-адрес вашего Captive-портала AxelNAC>

Шаг 10. Укажите AxelNAC в качестве RADIUS-сервера для **hotspot**:

/radius
add address=<IP-адрес вашего Captive-портала AxelNAC> secret=useStrongerSecret service=hotspot

/ip hotspot profile
add hotspot-address=10.5.50.1 name=hsprof1 use-radius=yes

Шаг 11. Настройте AxelNAC так, чтобы он использовал веб-аутентификацию для данной точки доступа, используя следующую конфигурацию:

[IP-адрес вашей точки доступа]
VlanMap=Y
RoleMap=N
mode=production
ExternalPortalEnforcement=Y
type=Mikrotik
radiusSecret=useStrongerSecret
registrationVlan=-1

ID статьи: 1458
Последнее обновление: 3 мар., 2026
Обновлено от: Михалева А.
Ревизия: 6
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с контроллерами беспроводного доступа Mikrotik
https://docs.axel.pro/entry/1458/