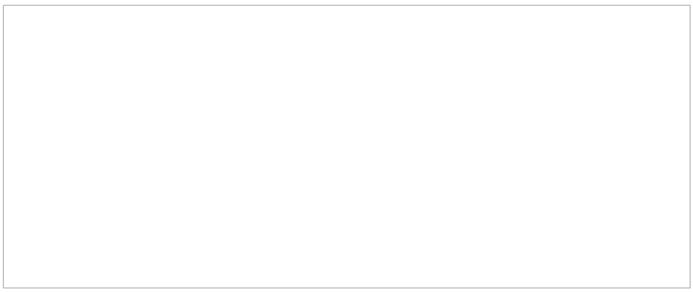
Интеграция с OpenVPN в режиме Inline

Режим Inline — это способ подключения сетевого оборудования, которое не поддерживает автоматическое назначение VLAN, ACL и т.д. к системам контроля доступа сети (NAC), что позволяет расширить базовый функционал OpenVPN.
OpenVPN с подключенным плагином для аутентификации RADIUS не позволяет реализовать все функциональные сценарии. Данная проблема решается активацией режима Inline, что также позволяет расширить функционал подключенного сетевого оборудования.

Подробнее о режиме **Inline** вы можете прочитать в статье Режим принудительного переопределения Inline.

Схема подключения сетевых устройств с использованием OpenVPN в режиме Inline:



В данном сценарии все пакеты, которые приходят с сети 31.31.210.0/24 (vpn), перенаправляются в сеть 31.31.206.200/30 (inline).
Далее по правилам IPTables все запросы перенаправляются при помощи ip_forward (настройка kernel) с Inline-интерфейса на интерфейс управления.
Это в свою очередь позволяет перехватывать DNS-запросы и менять в них ответ. За счет этого механизма клиента можно перенаправить на Captive-портал.

Установка и конфигурация OpenVPN-сервера

Пример настройки ниже описывает установку и конфигурацию OpenVPN-сервера на Debian 11. Если у вас другая операционная система — скорректируйте настройку в соответствии с ней.

Шаг 1. В ОС Debian 11 перейдите в **bash** на машине, на которой собираетесь установить OpenVPN-клиент. Выполните команду для установки инструментов настройки VPN-сервера с использованием OpenVPN и создания сертификатов для шифрования соединений:

```
apt install libgcrypt20-dev openvpn easy-rsa
```

Шаг 2. Создайте сертификаты сервера. Вы можете использовать пример ниже или воспользоваться собственным центром сертификации для генерации сертификатов:

```
mkdir -p /etc/openvpn/server/certs
cd /etc/openvpn/server/certs
openssl genrsa -out ca.key 2048
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
openssl genrsa -out vpn.key 2048
openssl req -new -key vpn.key -out vpn.csr
openssl x509 -req -in vpn.csr -out vpn.crt -CA ca.crt -CAkey ca.key -CAcreateserial -days 365
openssl dhparam -out dh2048.pem 2048
```

Шаг 3. Отредактируйте файл конфигурации сервера OpenVPN **/etc/openvpn/server.conf**:

```
port 443
proto tcp4
dev tun
server 10.11.0.0 255.255.255.0 #Пул адресов, выдаваемых клиентам
ca /etc/openvpn/server/certs/ca.crt #Сертификат удостоверяющего центра
cert /etc/openvpn/server/certs/vpn.crt #Открытый ключ
key /etc/openvpn/server/certs/vpn.key #Закрытый ключ
dh /etc/openvpn/server/certs/dh2048.pem #Ключ алгоритма Диффи-Хелмана
plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radiusplugin.cnf #Плагин для аутентификации по RADIUS
persist-key
persist-tun
keepalive 10 60
reneg-sec 0
comp-lzo
tun-mtu 1468
tun-mtu-extra 32
mssfix 1400
auth SHA1
push "persist-key"
push "persist-tun"
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
status /etc/openvpn/443.log
verb 3
verify-client-cert none
```

Шаг 4. Скачайте плагин для работы с RADIUS, реализующий поддержку аккаунтинга и аутентификации сервисом OpenVPN:

```
wget https://github.com/ValdikSS/openvpn-radiusplugin/archive/refs/heads/master.zip
unzip master.zip
cd openvpn-radiusplugin-master
```

Шаг 5. Отредактируйте плагин для OpenVPN:

```
diff -ruN openvpn-radiusplugin-master.orig/Config.cpp openvpn-radiusplugin-master/Config.cpp
--- openvpn-radiusplugin-master.orig/Config.cpp 2015-12-23 08:07:19.000000000 -0500
+++ openvpn-radiusplugin-master/Config.cpp      2021-11-09 11:17:21.759139003 -0500
@@ -240,6 +240,14 @@
                                        this->clientcertnotrequired=true;
                                }
                        }
+                       if (param == "verify-client-cert")
+                       {
+                               this->deletechars(&line);
```

```
+                                       if (line == "verify-client-certoptional" || line == "verify-client-certnone")
+                                       {
+                                             this->clientcertnotrequired=true;
+                                       }
+                                }
                                 if (param == "username-as-common-name")
                                 {
                                       this->deletechars(&line);
```

Шаг 6. Выполните компиляцию плагина:

```
make
cp radiusplugin.so /etc/openvpn/
```

Вы можете скачать предварительно подготовленный плагин по ссылке.

Шаг 7. Отредактируйте конфигурационный файл **/etc/openvpn/radiusplugin.cnf**:

```
NAS-Identifier=OpenVpn
Service-Type=5
Framed-Protocol=1
NAS-Port-Type=5
NAS-IP-Address=192.168.0.6 #IP-адрес на интерфейсе сервера OpenVPN
OpenVPNConfig=/etc/openvpn/server.conf
overwriteccfiles=true
useauthcontrolfile=true
useclientconnectdeferfile=true
nonfatalaccounting=false
defacctinteriminterval=0server
{
        acctport=1813
         authport=1815
         name=192.168.0.5 #VIP-адрес AxelNAC
         retry=1
         wait=30
         sharedsecret=useStrongerSecret #Укажите секретную фразу, которую вы настроили на коммутаторе. В нашем примере секретная фраза — useStrongerSecret
}
```

Шаг 8. На сервере OpenVPN добавьте в конфигурационный файл **/etc/sysctl.conf** строку **"net.ipv4.ip_forward=1"** .

Шаг 9. Перезапустите сервер.

Конфигурация соединения в AxelNAC

Шаг 1. В веб-интерфейсе AxelNAC перейдите на вкладку **Конфигурация → Политики и контроль доступа → Сетевые устройства** и нажмите **Новое сетевое устройство**. Из выпадающего списка выберите группу. Откроется окно **Новое сетевое устройство** и раздел **Определение**.

Шаг 2. В строке **IP-адрес/MAC-адрес/диапазон (CIDR)** укажите адрес **31.31.205.13**.

Шаг 3. В строке **Описание** укажите название соединения, например **openvpn_inline_test.**

Шаг 4. В строке **Тип** выберите из выпадающего списка **OpenVPN**.

Шаг 5. В строке **Метод реаутентификации** выберите из выпадающего списка **RADIUS**.

Шаг 6. Перейдите на вкладку **Режим Inline**.

Шаг 7. Нажмите на кнопку **Добавить условие**.

Шаг 8. Выберите опцию **Всегда**.

Шаг 9. Перейдите на вкладку **RADIUS**.

Шаг 10. В строке **Секретная фраза** укажите секретную фразу, которую вы настроили на коммутаторе. В нашем примере секретная фраза — **useStrongerSecret**.

Шаг 11. Активируйте параметр **Доступ к CLI/VPN разрешён**.

Шаг 12. Нажмите **Создать**.

Шаг 13. Перейдите в раздел **Статус → Службы**.

Шаг 14. Нажмите на кнопку **Перезапустить всё**.

Шаг 15. Аутентифицируйтесь в OpenVPN-клиенте с использованием логина и пароля. OpenVPN-сервер перенаправит данные в сторону AxelNAC для валидации данных пользователя. В случае успешной валидации AxelNAC отправит сообщение RADIUS Access-Accept и OpenVPN выполнит подключение клиента.

Конфигурация интерфейсов

Шаг 1. В веб-интерфейсе AxelNAC перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** .

Шаг 2. В таблице **Интерфейсы и сети** выберите строку с интерфейсом, через который выполняете соединение. Откроется окно конфигурации интерфейса.

Шаг 3. В строке **IPv4-адрес** укажите адрес **31.31.206.201**.

Шаг 4. В строке **Маска сети** укажите маску **255.255.255.252**.

Шаг 5. В строке **Тип** выберите из выпадающего списка **Транзитный L2**.

Не забудьте включить ip_forward в вашей операционной системе, чтобы режим Inline работал.

Шаг 6. В строке **DNS** укажите адрес **31.31.205.4**.

С момента отключения NAT AxelNAC будет настраивать iptables для маршрутизации трафика без использования NAT. Убедитесь, что в систему добавлены маршруты.

Шаг 7. Активируйте параметр **DNS прокси**.

Шаг 8. Активируйте параметр **Активировать CoA**.

Шаг 9. В веб-интерфейсе AxelNAC перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** .

Шаг 10. В таблице **Сети с маршрутизацией** нажмите на строку с сетью, которая используется для соединения клиента и сервера OpenVPN. Откроется окно **Сеть с маршрутизацией** и раздел **Основное**.

Шаг 11. В строке **Маска сети** укажите маску **255.255.255.0**.

Шаг 12. В строке **Тип** выберите из выпадающего списка **Транзитный L3**.

Шаг 13. Активируйте параметр **Ложный MAC-адрес**.

Шаг 14. Активируйте параметр **Активировать CoA**, если это необходимо.

Шаг 15. Перейдите в раздел **DHCP**.

Шаг 16. Активируйте **DHCP-сервер**.

Шаг 17. В строке **DNS-сервер** укажите IP-адрес DNS-сервера.

Шаг 18. Деактивируйте **DHCP-сервер**.

Шаг 19. Перейдите в раздел **Маршрутизация**.

Шаг 20. В строке **IP маршрутизатора** укажите IP-адрес маршрутизатора.

Шаг 21. Нажмите **Сохранить**.

ID статьи: 592
Последнее обновление: 6 февр., 2025
Обновлено от: Ильина В.
Ревизия: 12
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Интеграция с VPN-сервисами -> Интеграция с OpenVPN -> Интеграция с OpenVPN в режиме Inline
https://docs.axel.pro/entry/592/