

Защищённый канал связи с узлами НЕЙРОСС | VPN

На предприятиях с разветвлённой структурой и территориальной удалённостью подразделений, вынужденных использовать незащищенные сети (в том числе Интернет), часто возникает необходимость в организации защищённого канала связи между различными узлами НЕЙРОСС, в частности, — между Платформой НЕЙРОСС и контроллерами БОРЕЙ. Решением является объединение узлов в закрытую VPN-сеть с использованием шифрованного-SSL/TLS-соединения.

Контроллер БОРЕЙ с установленным плагином «VPN-клиент» является клиентом VPN, обеспечивает защищённое подключение к серверу VPN, развёрнутому на сервере Платформы НЕЙРОСС (или на другом сервере в подсети Платформы). Плагин осуществляет аудит процесса подключения и возможность управления профилем.

☰ Содержание:

- [Подготовка к работе](#)
- [Установка плагина «VPN-клиент»](#)
- [Настройка плагина и запуск сервиса VPN](#)
 - [Загрузка профиля](#)
 - [Включение VPN](#)
- [Как узнать новый IP-адрес контроллера?](#)
- [Ошибки подключения](#)
- [Взаимодействие у](#)

Подготовка к работе

Со стороны сервера Платформы НЕЙРОСС

1. В подсети или напрямую на сервере Платформы НЕЙРОСС разверните VPN-сервер согласно инструкции компании-производителя. Выбор сервера VPN не ограничивается, основное требование — поддержка формата OVPN.

⚠ При настройке используйте интерфейс **TAP**.

2. Подготовьте файл конфигурации в формате **OVPN** (профиль), который будет загружаться на клиентские узлы для подключения к серверу VPN.

Установка плагина «VPN-клиент»

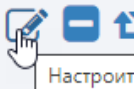
Сервис подключения по защищённому каналу связи поставляется в виде [плагина интеграции](#) — это независимого программного модуля, предназначенный для расширения функционала. Как правило, поставляется в составе продукта, но может быть загружен и установлен впоследствии. Установка плагина является стандартной процедурой и не зависит от предоставляемых функций. Перечень разработанных плагинов и порядок их установки приведён в разделе [\[Плагины и скрипты\]](#).

ℹ Требуется активация плагина.

Настройка плагина и запуск сервиса VPN

Войдите в веб-интерфейс контроллера [[Рабочий стол НЕЙРОСС](#)].

Перейдите к разделу [Конфигурация узлов > Плагины и скрипты](#). Найдите в списке установленных плагинов «VPN-клиент» и нажмите на кнопку **Настроить**. Откроется окно конфигурирования плагина.

Список плагинов			
Плагин	Версия	Разработчик	
VPN-клиент Плагин обеспечивает коммуникацию контроллера по защищенному каналу с установлением VPN-соединения	12769	ИТРИУМ СПб	 Настроить

Откроется окно конфигурирования плагина.

НЕЙРОСС | Плагин VPN-клиент | Рабочий стол ✓ root | В

Профиль VPN-клиента: загружен [Просмотреть](#) [⬇ Выбрать новый файл](#) [Удалить файл](#)

VPN-клиент включен: ☒

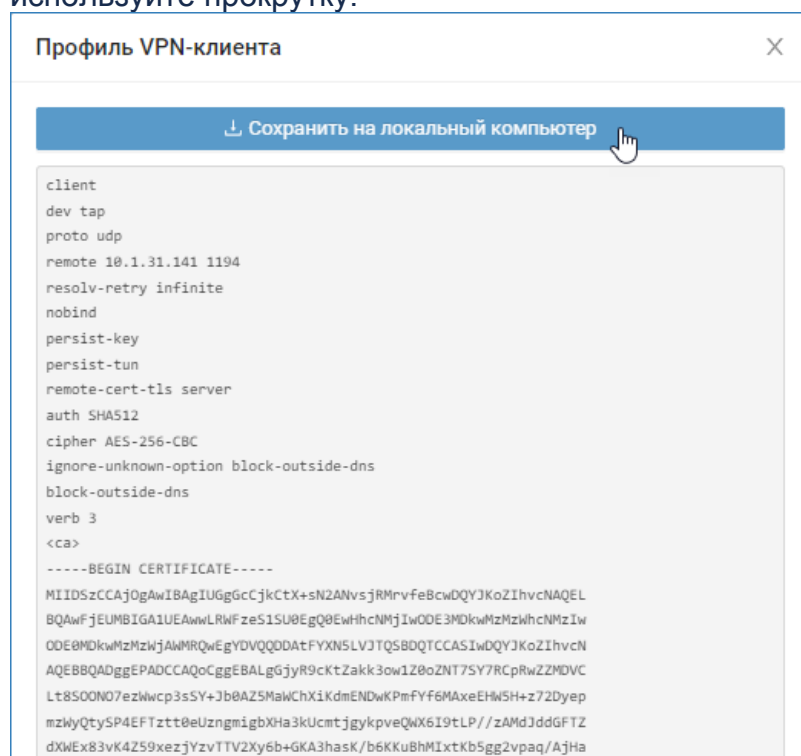
Журнал аудита (для отладки): [открыть в новой вкладке](#)

Загрузка профиля

В поле **Профиль VPN-клиента** укажите путь к файлу конфигурации в формате **OVPN** и выполните загрузку.

Чтобы **просмотреть содержимое профиля** нажмите на кнопку **Просмотреть**.

Файл профиля будет открыт в новом окне. Для просмотра всего содержимого используйте прокрутку.



Чтобы скачать файл профиля в папку загрузок браузера нажмите на кнопку **Сохранить на локальный компьютер**.

Чтобы **изменить файл конфигурации** просто укажите путь к новому файлу и дождитесь сообщения «Файл профиля успешно обновлён».

Включение VPN

Для включения VPN в поле **VPN-клиент включен** установите переключатель в положение  **Включено**.

При успешном подключении в разделе [[Сетевые параметры](#)] узла БОРЕЙ отобразится новый интерфейс подключения (**TAP**).

Сетевые параметры

Основные
Маршруты
Дополнительно

Сетевой адаптер: tap0

Использовать: ☒ Да ?

MAC-адрес:

MTU:

IP-адрес

Маска подсети

Сохранить

Нужно включить интерфейс. Для этого:

1. Включите интерфейс TAP. Для этого в блоке **Сетевой адаптер: tap** установите переключатель в положение **Да**.
2. Сохраните изменения. Будет выполнен перезапуск контроллера.

! После перезапуска контроллер будет доступен и по «старому» ETH-интерфейсу, а также по новому TAP-интерфейсу [[Как узнать новый IP-адрес контроллера?](#)]. Для доступа к веб-интерфейсу контроллера по новому IP-адресу и из новой подсети необходимо, чтобы компьютер, с которого производится подключение, находился в диапазоне адресов этой подсети. При необходимости, настройте сетевое подключение компьютера или планшета для работы в диапазоне IP-адресов и подсети узла.

Если блока **Сетевой адаптер: tap** нет, подключение по VPN не было осуществлено. Необходимо найти причину проблемы [[Ошибки подключения](#)].

Как узнать новый IP-адрес контроллера?

В разделе [[Сеть](#)] в списке узлов найдите хостовый узел (узел, с IP-адреса которого выполнен вход в интерфейс, выделен жирным) и нажмите на кнопку ? **Дополнительно**.

В отобразившемся окне перейдите к вкладке **Дополнительно**.

Доп. информация(10.8.0.2)3

УзелБезопасностьПодпискиДополнительно

Тип:

ONVIF, НЕЙРОСС

URL сервисов:

- http://10.8.0.2:80/onvif/device_service
- http://10.0.29.3:80/onvif/device_service

Возможности:


```
{  "events": {    "XAddr": "http://10.8.0.2/event/NotificationProducer/",    "WSPullPointSupport": true,    "WSSubscriptionPolicySupport": true  },  "device": {    "XAddr": "http://10.8.0.2/onvif/device_service",
```

Все текущие адреса будут указаны в блоке **URL сервисов**.


Ошибки подключения

Если в разделе **Сетевые параметры** нет блока **Сетевой адаптер: tap**, подключение по VPN не было осуществлено. Для решения проблемы:

В окне конфигурации плагина в поле **VPN-клиент включен** установите переключатель в положение  **Выключено**. Дождитесь выполнения процедуры выключения (~ 1 мин).


Нажмите **Открыть в новой вкладке**, чтобы открыть Журнал аудита. Повторно установите переключатель в положение  **Включено** и просмотрите записи журнала аудита.

Взаимодействие узлов НЕЙРОСС посредством VPN

 Взаимодействие нескольких узлов НЕЙРОСС между собой может быть осуществлено по мультикаст, также узлы могут быть «связаны» вручную. Подробная информация приведена в разделах [[Что такое Сеть НЕЙРОСС, узел НЕЙРОСС?](#)].

При организации связи Платформы НЕЙРОСС с несколькими узлами БОРЕЙ посредством VPN необходимо:

1. На каждом узле БОРЕЙ установить и настроить плагин «VPN-клиент», включить VPN-соединение и интерфейс TAP.
2. На узле Платформа НЕЙРОСС средствами раздела **Сеть** добавить вручную узлы БОРЕЙ по IP-адресу интерфейса TAP, включить «связь» в обе стороны. Инструкция по добавлению узла приведена в разделе [[Сеть > Добавление узлов](#)].

 Узлы должны принадлежать одному домену НЕЙРОСС, мультикаст на всех узлах должен быть выключен [[Сетевые параметры](#)].

При организации связи с одним «удалённым» узлом БОРЕЙ, достаточно включить интерфейс ТАР, проверить, что контроллер принадлежит требуемому домену и включён мультикаст. В этом случае контроллер будет «вычитан» узлом Платформа НЕЙРОСС автоматически.