## 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/TLSсоединения.

Контроллер БОРЕЙ с установленным плагином «VPNклиент» 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 «VPNклиент»
- Настройка плагина и запуск сервиса VPN
  - Загрузка
  - профиля
- Включение \
  Как узнать новый IP-адрес
- контроллера? • Ошибки подключения
- Взаимодействие у

## Подготовка к работе

Со стороны сервера Платформы НЕЙРОСС

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

При настройке используйте интерфейс ТАР.

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].

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.

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

#### Откроется окно конфигурирования плагина.

НЕЙРОСС   Плагин VPN-клиент   Рабочий стол	🕢 root   Bt
Профиль VPN-клиента : загружен Просмотреть 上 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.

Профиль VPN-клиента Х					
🗄 Сохранить на локальный компьютер					
client					
dev tap					
proto udp					
remote 10.1.31.141 1194					
resolv-retry infinite					
nobind					
persist-key					
persist-tun					
remote-cert-tls server					
auth SHA512					
cipher AES-256-CBC					
ignore-unknown-option block-outside-dns					
block-outside-dns					
verb 3					
<ca></ca>					
BEGIN CERTIFICATE					
MIIDSzCCAjOgAwIBAgIUGgGcCjkCtX+sN2ANvsjRMrvfeBcwDQYJKoZIhvcNAQEL					
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjIwODE3MDkwMzMzWhcNMzIw					
ODE0MDkwMzMzWjAWMRQwEgYDVQQDDAtFYXN5LVJTQSBDQTCCASIwDQYJKoZIhvcN					
AQEBBQADggEPADCCAQoCggEBALgGjyR9cKtZakk3ow1Z0oZNT7SY7RCpRwZZMDVC					
Lt8SOONO7ezWwcp3sSY+Jb0AZ5MaWChXiKdmENDwKPmfYf6MAxeEHW5H+z72Dyep					
mzWyQtySP4EFTztt0eUzngmigbXHa3kUcmtjgykpveQWX6I9tLP//zAMdJddGFTZ					
dXWEx83vK4Z59xezjYzvTTV2Xy6b+GKA3hasK/b6KKuBhMIxtKb5gg2vpaq/AjHa					

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 OBКЛючено.

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

Сетевые параметры						
Основные	Маршруты Дополнительно					
Сетевой адапт	Сетевой адаптер: tap0					
Использоваты	Да 🚺					
МАС-адрес:	fe:c1:7b:ee:48:a7					
MTU:	1500					
IP-адрес Маска подсети						
Сохранить	Сохранить					

Нужно включить интерфейс. Для этого:

- 1. Включите интерфейс ТАР. 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» ETHинтерфейсу, а также по новому TAP-интерфейсу [Как узнать новый IPадрес 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 ІР-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. ин	формация(10.8	.0.2)		За
Узел	Безопасность	Подписки	Дополнительно	
Тип:			ONVIF, НЕЙР	200
URL ce	рвисов:		<ul><li>http://10.8</li><li>http://10.0</li></ul>	0.2:80/onvif/device_service 29.3:80/onvif/device_service
Возмо	кности:		{	
			"events	
			"XA	ddr": "http://10.8.0.2/event/NotificationProducer/",
			"WS	PullPointSupport": true,
			"WS	SubscriptionPolicySupport": true
			},	
			"device	": {
			"XA	ddr": "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.
- На узле Платформа НЕЙРОСС средствами раздела Сеть добавить вручную узлы БОРЕЙ по IP-адресу интерфейса ТАР, 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.