

Инструкция по настройке соединения между двумя подсетями через маршрутизаторы EDR-810-VPN-2GSFP

Для организации защищенного канала связи между двумя удаленными подсетями необходимо настроить VPN-туннель.

В данной инструкции рассматривается пример построения Open VPN-туннеля между двумя маршрутизаторами [EDR-810-VPN-2GSFP](#).

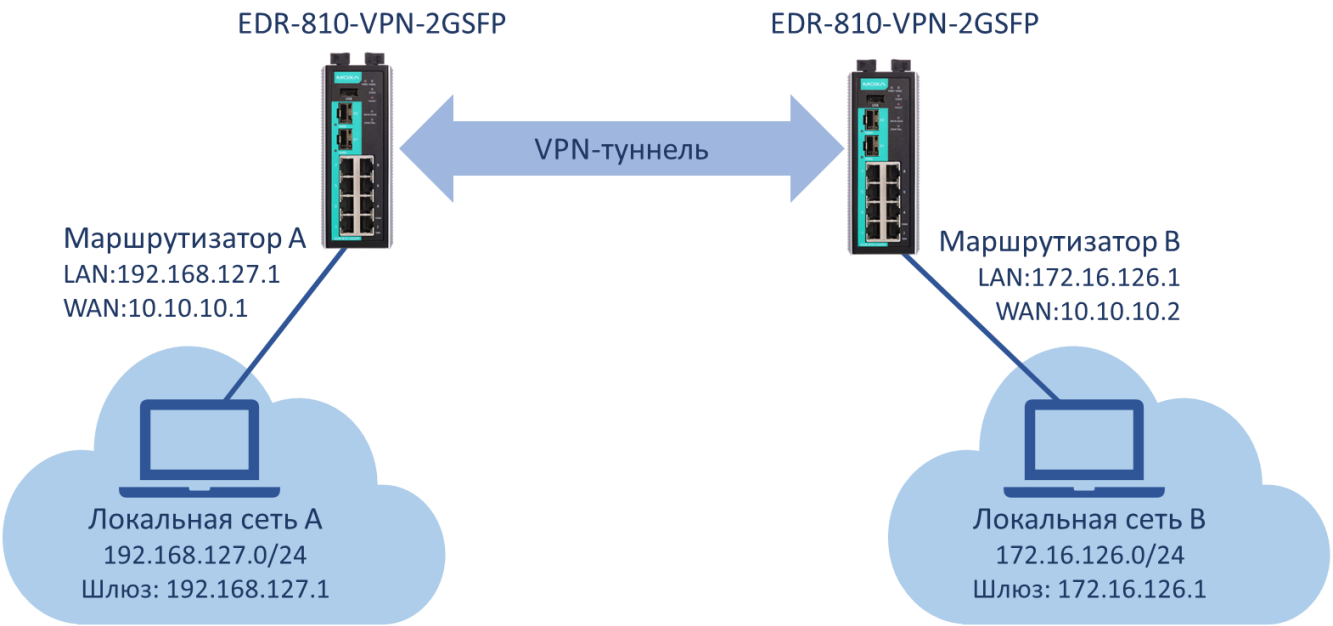


рис. 1 «Схема сети»

В таблице 1 указана адресация всей системы, согласно которой будем настраивать оборудование.

Таблица 1 «Адресация сети»

	IP-адрес	Маска подсети	Основной шлюз
Маршрутизатор А LAN-интерфейс	192.168.127.1	255.255.255.0	
Маршрутизатор А WAN-интерфейс	10.10.10.1	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети А	192.168.127.13	255.255.255.0	192.168.127.1
Маршрутизатор В LAN-интерфейс	172.16.126.1	255.255.255.0	
Маршрутизатор В WAN-интерфейс	10.10.10.2	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети В	172.16.126.13	255.255.255.0	172.16.126.1

xxx.xxx.xxx.xxx – основной шлюз WAN сети зависит от построения системы или выдается провайдером связи. В примере на рисунке 1 – соединение между маршрутизатором сети А и В прямое, поэтому шлюз указывать не нужно.

Все настройки маршрутизаторов осуществляются через web-интерфейс.

По умолчанию маршрутизаторы EDR-810-VPN-2GSFP имеют следующие параметры:

ip-адрес: 192.168.127.254

логин: admin

пароль: моха

В целях безопасности рекомендуется изменить данные для входа.

После внесения любых изменений в настройки маршрутизатора необходимо нажимать кнопку **Apply** для сохранения изменений.

1. Настройка Маршрутизатора А

1.1. Настройка LAN-интерфейса

IP-адрес и маска подсети (согласно Таблице 1) задаются в разделе **Network – Interface - LAN**

LAN Configuration

LAN IP Configuration

Name	<input type="text" value="LAN"/>	VLAN ID	<input type="text" value="1"/>	Source IP Overwrite	<input type="checkbox"/>
Enable	<input checked="" type="checkbox"/>	Directed Broadcast	<input type="checkbox"/>	Virtual MAC	<input type="text" value="00:00:00:00:00:00"/>
IP Address	<input type="text" value="192.168.127.1"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>		
<input type="button" value="Add"/>		<input type="button" value="Delete"/>		<input type="button" value="Modify"/>	
<input type="button" value="Apply"/>					

VLAN Interface List (1/16)

Name	Enable	VLAN ID	IP Address	Subnet Mask	Virtual MAC	Directed Broadcast	Source IP Overwrite
LAN	<input checked="" type="checkbox"/>	1	192.168.127.1	255.255.255.0	--	<input type="checkbox"/>	<input type="checkbox"/>

1.2. Настройка WAN-интерфейса

Маршрутизатор EDR-810 имеет 10 портов, каждый из которых можно назначить LAN или WAN-интерфейсом. Поэтому прежде, чем задавать адресацию на WAN-интерфейсе, нужно установить порты, которые будут относиться к WAN. Для этого необходимо поместить их в отдельную VLAN.

➤ Настройка VLAN

VLAN настройки осуществляются в разделе **Layer 2 Functions - Virtual LAN - VLAN Settings**.

Порты 7 и 8 маршрутизатора будут относиться к WAN-интерфейсу. На этих портах указываем VLAN ID 2.

802.1Q VLAN Settings

Quick Setting Panel ▾

VLAN ID Configuration Table

Management VLAN ID

Port	Type	PVID	Tagged VLAN
1	Access ▾	1	
2	Access ▾	1	
3	Access ▾	1	
4	Access ▾	1	
5	Access ▾	1	
6	Access ▾	1	
7	Access ▾	2	
8	Access ▾	2	
G1	Access ▾	1	
G2	Access ▾	1	

Когда отдельная VLAN для WAN-портов создана, можно перейти к назначению адресации.

➤ Адресация WAN-интерфейса

В разделе **Network – Interface – WAN** назначается IP-адрес, маска сети и шлюз по умолчанию согласно Таблице 1.

WAN Configuration

VLAN ID

Connection

Connect Mode ☐ Disable ☒ Enable

Connect Type

Directed Broadcast

☐ Enable ☐ Source IP Overwrite

Address Information

IP Address Gateway

Subnet Mask

1.3. Настройка NAT

Для того чтобы маршрутизатор подменял адреса локальной сети на внешний адрес при передаче во внешнюю сеть, необходимо настроить NAT в разделе **NAT - NAT Setting**

Network Address Translation

Name

Enable ☒

NAT Mode

VRRP Binding

Outside Interface

Global IP

Local IP ~

NAT List (1/128)

Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	
<input checked="" type="checkbox"/>	1	WAN	--	192.168.127.1 ~192.168.127.254	--	10.10.10.1	--	--	MoxaA

1.4. Настройка даты и времени

Для выполнения корректного соединения между VPN-сервером и VPN-клиентом необходимо, чтобы маршрутизаторы были синхронизированы в настройках даты и времени.

Настройка системного времени осуществляется в разделе **System - Date and Time**.

Можно осуществить синхронизацию локальную или по протоколу SNTP.

Date and Time

System Up Time 0d3h42m0s
 Current Time 2020/04/09 13:11:11
 Clock Source ☒ Local ☐ NTP ☐ SNTP

Time Settings

☐ Manual Time Settings

Date(YYYY/MM/DD) / / (ex: 2002/11/13)

Time(HH:MM:SS) : : (ex: 04:00:04)

☒ Sync with Local Device 2020/04/09 13:11:24

NTP/SNTP Server Settings

NTP/SNTP Server ☐ Enable

TimeZone Settings

Time Zone

Daylight Saving Time

	Month	Week	Day	Hour	Min
Start Date	--	--	--	--	--
End Date	--	--	--	--	--
Offset(hr)	0				

2. Настройка Маршрутизатора В

Для настройки Маршрутизатора В необходимо повторить шаги 1.1 – 1.4, указывая параметры в соответствии с Таблицей 1.

3. Настройка VPN-туннеля

3.1. Предустановка сертификатов безопасности

Аутентификация при установке Open VPN-туннеля осуществляется с помощью сертификатов безопасности, а авторизация пользователя с помощью логина и пароля.

Сгенерировать сертификаты безопасности можно с помощью различных программ, а также можно создать их на самом маршрутизаторе.

- Создание сертификатов безопасности

В разделе **Certificate Management - CA Server - Certificate Create** нужно выполнить несколько шагов:

- Заполнить таблицу **Certificate Request**, нажать кнопку **Apply**
- Заполнить таблицу **Certificate Setting**, нажать кнопку **Add** и затем **Apply**
- Выгрузить сертификат **RootCA** с помощью кнопки **RootCA Export**
- Сгенерировать сертификат с помощью кнопки **PKCS#12 Export**

(необходимо время на создание файлов с сертификатами, нужно немного подождать и повторно нажать на кнопки **Export**)

Нужно создать сертификаты на одном маршрутизаторе и загрузить их на два маршрутизатора (на VPN-сервер и VPN-клиент).

Certificate Create

Certificate Request

Country Name (2 letter code)	RU	Certificate days	100
State or Province Name	SPB	Locality Name	TEST
Organization Name	TEST	Organizational Unit Name	TEST
Common Name	TEST	Email Address	test@test.com

1 **Apply** 4 **RootCa Export**

Certificate Setting

Certificate days	100	Organizational Unit Name	TEST
Common Name	TEST	Email Address	test@test.com
Certificate Password	TEST		

5 **PKCS#12 Export** **Certification Export**

2 **Add** **Delete** **Modify** 3 **Apply**

Certificate List (1/10)

Certificate days	Organizational Unit Name	Common Name	Email Address	Certificate Password
100	TEST	TEST	test@test.com	TEST

➤ Загрузка сертификатов на маршрутизаторы

Оба сертификата нужно загрузить на каждый маршрутизатор в раздел **Certificate Management**, но в разные подразделы в соответствии с таблицей 2.

Таблица 2 «Сертификаты безопасности»

Место загрузки	Тип сертификата	Название сертификата
Trusted CA Certificate	RootCA	Cacert.crt
Local Certificate	PKCS	TEST.p12

В раздел **Certificate Management - Local Certificate** загружается PKCS сертификат

Local Certificate

Import Identity Certificate
Label

Certificate From PKCS#12 ▾

Import Password
Certificate From PKCS#12

TEST

Выберите файл TEST.p12

Import

Delete

Apply

Certificate List

All	Label	Issued To	Issued By	Expired Date
<input type="checkbox"/>	TEST.p12	/C=RU/ST=SPB/O=TEST/OU=TEST/CN=TEST/emailAddress=test@test.com	/C=RU/ST=SPB/O=TEST/OU=TEST/CN=TEST/emailAddress=test@test.com	notBefore=Apr 10 12:59:39 2020 GMT,notAfter=Jul 19 12:59:39 2020 GMT

В раздел **Certificate Management - Trusted CA Certificate** загружается Root сертификат

Trusted CA Certificate

Name

CA Certificate Upload

Выберите файл cacert.crt

Import

Delete

Certificate List

Name	Subject
cacert.crt	/C=RU/ST=SPB/O=TEST/OU=TEST/CN=TEST/emailAddress=test@test.com

3.2. Настройка Open VPN-сервера

Маршрутизатор А будет выступать в качестве Open VPN-сервера, то есть будет ожидать подключения от удаленной подсети.

Настройки Open VPN Сервера осуществляются в разделе нужно активировать VPN-туннель в разделе **VPN – OpenVPN**.

- Активация Open VPN-сервера

В разделе **VPN – OpenVPN - OpenVPN Server - Server Setting** активируется VPN туннель. В качестве **Push Network** указывается локальная сеть Сервера, а **Network** – любая незадействованная виртуальная подсеть.

OpenVPN Server Setting

Enable ☒

Server ID 1

Interface Type TUN(Router)

Network 10.8.0.0 Netmask 255.255.255.0

Push Network 192.168.127.0 Netmask 255.255.255.0

Protocol UDP

Port 1194

Encryption Algorithm BlowFish CBC

Hash Algorithm SHA-1

LZO Compression ☐ Disable ☒ Enable

CA Certificate cacert.crt

Certificate TEST.p12

User Authentication Password

Keepalive ☐ Disable ☒ Enable

Redirect Default Gateway ☒ Disable ☐ Enable

Allow Client to Client ☒ Disable ☐ Enable

Allow Duplicate User Name ☒ Disable ☐ Enable

Modify Apply

OpenVPN Server

Enable	Server ID	Interface Type	Protocol	Port	Encryption	Hash	LZO Compression
<input checked="" type="checkbox"/>	1	TUN(Router)	UDP	1194	BlowFish CBC	SHA-1	<input checked="" type="checkbox"/>

Сертификаты безопасности автоматически будут установлены те, что были загружены в соответствующие разделы. Для авторизации пользователей выбирается вариант - **password**.

- Создание таблицы пользователей

В разделе **VPN – OpenVPN - OpenVPN Server - User Management** нужно указать локальную подсеть удаленного Open VPN-клиента и придумать логин и пароль для пользователей.

OpenVPN User Management

OpenVPN Server:

User Name:

New Password:

Confirm Password:

Remote Network: Netmask:

OpenVPN User

User Name	Remote Network	Netmask
TEST	172.16.126.0	255.255.255.0

3.3. Настройка Open VPN-клиента

В разделе **VPN – OpenVPN - OpenVPN Client - Client Setting** выполняются настройки Open VPN-клиента.

OpenVPN Client Setting

☒ Enable

Client ID:

Interface Type:

Bridge with LAN:

Remote Server IP:

Port:

Protocol:

LZO Compression: ☐ Disable ☒ Enable

Encryption Cipher:

Hash Algorithm:

CA Certificate:

Certificate:

Authentication Method:

User Name: Password:

OpenVPN Client

Enable	Client ID	Interface Type	Remote Server	Protocol	Encryption Cipher	LZO Compression	Authentication Mode
<input checked="" type="checkbox"/>	1	TUN	10.10.10.1/1194	UDP	BlowFish CBC	<input checked="" type="checkbox"/>	Password
<input type="checkbox"/>	2	TUN	0.0.0.0/1194	UDP	BlowFish CBC	<input checked="" type="checkbox"/>	Certificate

В качестве **Remote Server** нужно указать WAN ip-адрес Маршрутизатора А и выбрать такие же сертификаты, как установлены на VPN-сервере.

User Name и **Password** должны соответствовать данным, указанным в настройках пользователей на VPN-сервере.

3.4. Настройка устройств в локальных сетях

На устройствах в локальных сетях необходимо указать основной шлюз – LAN адрес маршрутизатора в соответствии с Таблицей 1.

Для локальной сети А: 192.168.127.1

Для локальной сети В: 172.16.126.1

Свойства: IP версии 4 (TCP/IPv4)

Общие

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

☐ Получить IP-адрес автоматически

☒ Использовать следующий IP-адрес:

IP-адрес: 192 . 168 . 127 . 13

Маска подсети: 255 . 255 . 255 . 0

Основной шлюз: 192 . 168 . 127 . 1

☐ Получить адрес DNS-сервера автоматически

☒ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер: . . .

Альтернативный DNS-сервер: . . .

☐ Подтвердить параметры при выходе

Дополнительно...

OK Отмена

Свойства: IP версии 4 (TCP/IPv4)

Общие

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

☐ Получить IP-адрес автоматически

☒ Использовать следующий IP-адрес:

IP-адрес: 172 . 16 . 126 . 27

Маска подсети: 255 . 255 . 255 . 0

Основной шлюз: 172 . 16 . 126 . 1

☐ Получить адрес DNS-сервера автоматически

☒ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер: . . .

Альтернативный DNS-сервер: . . .

☐ Подтвердить параметры при выходе

Дополнительно...

OK Отмена

3.5. Диагностика VPN-соединения

После выполнения вышеуказанных настроек на двух маршрутизаторах будет установлено VPN-соединение.

На VPN-сервере в разделе **VPN – OpenVPN – OpenVPN Server – OpenVPN Server Status** появится запись об установленном VPN-соединении с определенным клиентом и добавится маршрут для доступа в новую подсеть.

OpenVPN Server Status

```
Server 1:
-----
OpenVPN CLIENT LIST
Updated, Mon Apr 13 14:10:19 2020
[Common Name] , [Real Address] , [Bytes Received] , [Bytes Sent], [Connected Since]
TEST , 10.10.10.2:55752 , 13318, 13945, Mon Apr 13 13:19:10 2020
-----
ROUTING TABLE
[Virtual Address] , [Common Name] , [Real Address] , [Last Ref]
10.8.0.6 , TEST , 10.10.10.2:55752, Mon Apr 13 13:19:11 2020
172.16.126.0/24 , TEST , 10.10.10.2:55752, Mon Apr 13 13:19:11 2020
```

На VPN-клиенте в разделе **VPN – OpenVPN – OpenVPN Client – OpenVPN Client Status** появится информация об успешном соединении.

Open VPN-туннель на маршрутизаторах Moxa

OpenVPN Client Status

```
Client 1:  
State: Connected  
OpenVPN STATISTICS  
Updated, Mon Apr 13 15:06:37 2020  
TUN/TAP read bytes, 0  
TUN/TAP write bytes, 0  
TCP/UDP read bytes, 4407  
TCP/UDP write bytes, 3082  
Auth read bytes, 832  
pre-compress bytes, 0  
post-compress bytes, 0  
pre-decompress bytes, 0  
post-decompress bytes, 0  
END
```

```
Client 2:  
client is not enabled
```



Кроме того, при успешном установлении VPN-туннеля на маршрутизаторах загорится индикатор VPN.