

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 IPSec VPN-туннеля между двумя маршрутизаторами EDR-810-VPN-2GSFP.

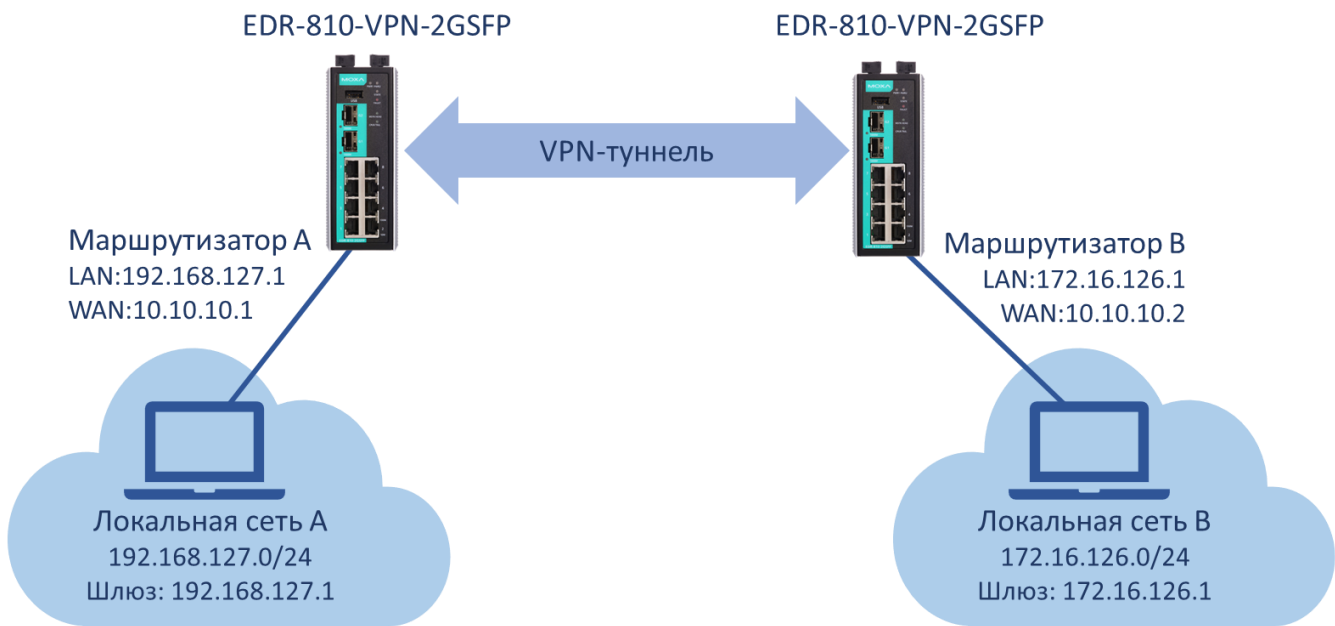


Рисунок 1 «Схема сети»

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: MoxaA

Enable: ☒ NAT Mode: N-1 VRRP Binding: --

Outside Interface: WAN Global IP: 10.10.10.1

Local IP: 192.168.127.1 ~ 192.168.127.254

Add Modify Delete Move **Apply**

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: (GMT+03:00)Moscow, St. Petersburg, Volgograd

Daylight Saving Time

Month: -- Week: -- Day: -- Hour: -- Min: --

Start Date: -- End Date: -- Offset(hr): 0

Apply

Refresh

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. Активация VPN-соединения

На каждом маршрутизаторе нужно активировать VPN-туннель в разделе **VPN – IPSec - Global Setting**.

Также в этом разделе включается NAT для данных, передаваемых в туннеле и логирование системной информации об установлении туннеля (может понадобиться для отладки VPN-соединения)

IPSec Global Setting

The screenshot shows the 'IPSec Global Setting' configuration interface. It includes the following elements:

- All IPSec Connection:** A dropdown menu set to 'Enable'.
- IPSec NAT-T Enable:** A checkbox that is checked.
- VPN Event Log:** A dropdown menu set to 'Enable'.
- Flash:** A checkbox that is checked.
- Syslog:** A checkbox that is checked.
- SNMP Trap:** A checkbox that is checked.
- Apply:** A green button at the bottom left.

3.2. Предустановка сертификатов безопасности

Аутентификация при установке IPSec VPN-туннеля может осуществляться с помощью ключа безопасности (пароля), но это не самый безопасный вариант. Рекомендуем использовать сертификаты безопасности для аутентификации.

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

➤ Создание сертификата 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**
- Сгенерировать сертификат с помощью кнопки **PKCS#12 Export** (необходимо время на создание файла с сертификатом, затем нужно будет повторно нажать кнопку **PKCS#12 Export**)

Нужно создать сертификаты на каждом маршрутизаторе в соответствии с таблицей 2.

Таблица 2 «Сертификаты безопасности»

	Тип сертификата	Название сертификата
Маршрутизатор А	PKCS	CA-1
Маршрутизатор В	PKCS	CA-2

Certificate Create

Certificate Request

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

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

Certificate Setting

Certificate days	100	Organizational Unit Name	NNZ
Common Name	CA-1	Email Address	test@test.com
Certificate Password	CA-1		

4 **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	NNZ	CA-1	test@test.com	CA-1

➤ Загрузка сертификаты на маршрутизатор

Оба сертификата нужно загрузить на каждый маршрутизатор в раздел **Certificate Management - Local Certificate**

Local Certificate

Import Identity Certificate

Label

Import Password

Certificate From PKCS#12

CA-1.p12 **Import**

Delete **Apply**

Certificate List

All	Label	Issued To	Issued By	Expired Date
<input checked="" type="checkbox"/>	CA-1.p12	/C=RU/ST=SPB/O=NNZ/OU=NNZ/CN=CA-1/emailAddress=test@test.com	/C=RU/ST=SPB/O=NNZ/OU=NNZ/CN=IPSec_Moxa/emailAddress=test@test.com	notBefore=Apr 9 13:05:34 2020 GMT,notAfter=Jul 18 13:05:34 2020 GMT
<input type="checkbox"/>	CA-2.p12	/C=RU/ST=SPB/O=NNZ/OU=NNZ/CN=CA-2/emailAddress=test@test.com	/C=RU/ST=SPB/O=NNZ/OU=NNZ/CN=CA-2/emailAddress=test@test.com	notBefore=Mar 18 03:25:21 2020 GMT,notAfter=Jun 26 03:25:21 2020 GMT

3.3. Настройка параметров VPN-соединения

В разделе **VPN – IPSec - IPSec Setting** нужно осуществить расширенные настройки (**Advanced Setting**).

➤ Маршрутизатор А – VPN-клиент.

Маршрутизатор А будет инициировать VPN-соединение. То есть режим работы устанавливается как **Start in initial**.

IPSec Setting

Setting Quick Setting **Advanced Setting**

Tunnel Setting

Enable ☒ Name L2TP tunnel ☐

VPN Connection Type Remote VPN Gateway

Startup Mode

Local Network

Remote Network

Identity Type Local ID Remote ID

Даже если аутентификация осуществляется с помощью сертификатов безопасности, нужно сначала установить пароль для предустановленного ключа (**Pre-shared Key**).

Затем нужно выбрать режим аутентификации X.509 и два загруженных сертификата.

На маршрутизаторе А локальным сертификатом будет сертификат CA-1, а удаленным – CA-2

Key Exchange (Phase 1)

IKE Mode

1 **Authentication Mode**

Encryption Algorithm Hash Algorithm

DH Group

Negotiation Times (0:forever) IKE Life Time hour.

Rekey Expire Time min. Rekey Fuzz Percent %

Data Exchange (Phase 2)

SA Life Time min. Perfect Forward Secrecy ☐

Encryption Algorithm Hash Algorithm

Dead Peer Detection

Action Retry Interval seconds Confidence Interval seconds

2 **Authentication Mode** Local Remote

Encryption Algorithm Hash Algorithm

3 **Add** **Delete** **Modify** 4 **Apply**

IPSec Connection (1/10)

Enable	Name	Remote VPN Gateway	Local Subnet	Remote Subnet
<input checked="" type="checkbox"/>	IPSec	10.10.10.2	192.168.127.0/24	172.16.126.0/24

➤ Маршрутизатор В – VPN-сервер.

VPN-сервером будет Маршрутизатор В, поэтому он будет ожидать подключения. Устанавливается режим работы **Wait connecting**.

IPSec Setting

Setting Quick Setting **Advanced Setting**

Tunnel Setting

Enable ☒ Name L2TP tunnel ☐

VPN Connection Type Remote VPN Gateway

Startup Mode

Local Network

Remote Network

Identity Type Local ID Remote ID

На маршрутизаторе В локальным сертификатом будет сертификат CA-2, а удаленным – CA-1

Key Exchange (Phase 1)

IKE Mode

1 Authentication Mode

Encryption Algorithm Hash Algorithm

DH Group

Negotiation Times (0:forever) IKE Life Time hour.

Rekey Expire Time min. Rekey Fuzz Percent %

Data Exchange (Phase 2)

SA Life Time min. Perfect Forward Secrecy ☐

Encryption Algorithm Hash Algorithm

Dead Peer Detection

Action Retry Interval seconds Confidence Interval seconds

2 **3** **4**

IKE Mode

Authentication Mode Local Remote

Encryption Algorithm Hash Algorithm

Add **Delete** **Modify** **Apply**

IPSec Connection (1/10)

Enable	Name	Remote VPN Gateway	Local Subnet	Remote Subnet
<input checked="" type="checkbox"/>	IPSec	10.10.10.1	172.16.126.0/24	192.168.127.0/24

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. В разделе **VPN – IPSec - IPSec Status** появится запись об установленном VPN-туннеле.

IPSec Status

Name	Local Subnet	Local Gateway	Remote Gateway	Remote Subnet	Key Exchange (Phase 1)	Data Exchange (Phase 2)	Time
IPSec	192.168.127.0/24	10.10.10.1	10.10.10.2	172.16.126.0/2	established	established	0h:0m:23s



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

Если соединение не устанавливается, то необходимо проверить корректность установки в разделе **Monitor - Event Log**

Event Log Table

IPSec <= <7> Debug Page 1/3

Index	Date	Time	Functions	Severity	Event
1	2020/04/09	17:10:31	IPSec	<5> Notice	[IPSec/1x1] VPN connection established
2	2020/04/09	17:10:31	IPSec	<5> Notice	[IPSec/1x1] Phase 2 Start
3	2020/04/09	17:10:30	IPSec	<5> Notice	[IPSec/1x1] Initiating VPN connection
4	2020/04/09	17:10:20	IPSec	<5> Notice	[IPSec/1x1] Disconnection request from remote peer
5	2020/04/09	17:08:06	IPSec	<5> Notice	[IPSec/1x1] VPN connection established
6	2020/04/09	17:08:03	IPSec	<5> Notice	[IPSec/1x1] Disconnection request from remote peer
7	2020/04/09	17:06:20	IPSec	<5> Notice	[IPSec/1x1] VPN connection established
8	2020/04/09	17:06:18	IPSec	<5> Notice	[IPSec/1x1] Phase 2 Start
9	2020/04/09	17:06:17	IPSec	<5> Notice	[IPSec/1x1] Initiating VPN connection
10	2020/04/09	17:06:09	IPSec	<5> Notice	[IPSec/1x1] Finish VPN connection (VPN configuration was removed)
11	2020/04/09	17:05:32	IPSec	<5> Notice	[IPSec/1x1] Remote certificate mismatch to local certificate
12	2020/04/09	17:05:32	IPSec	<5> Notice	[IPSec/1x1] Initiating VPN connection

Refresh Export Clear