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.

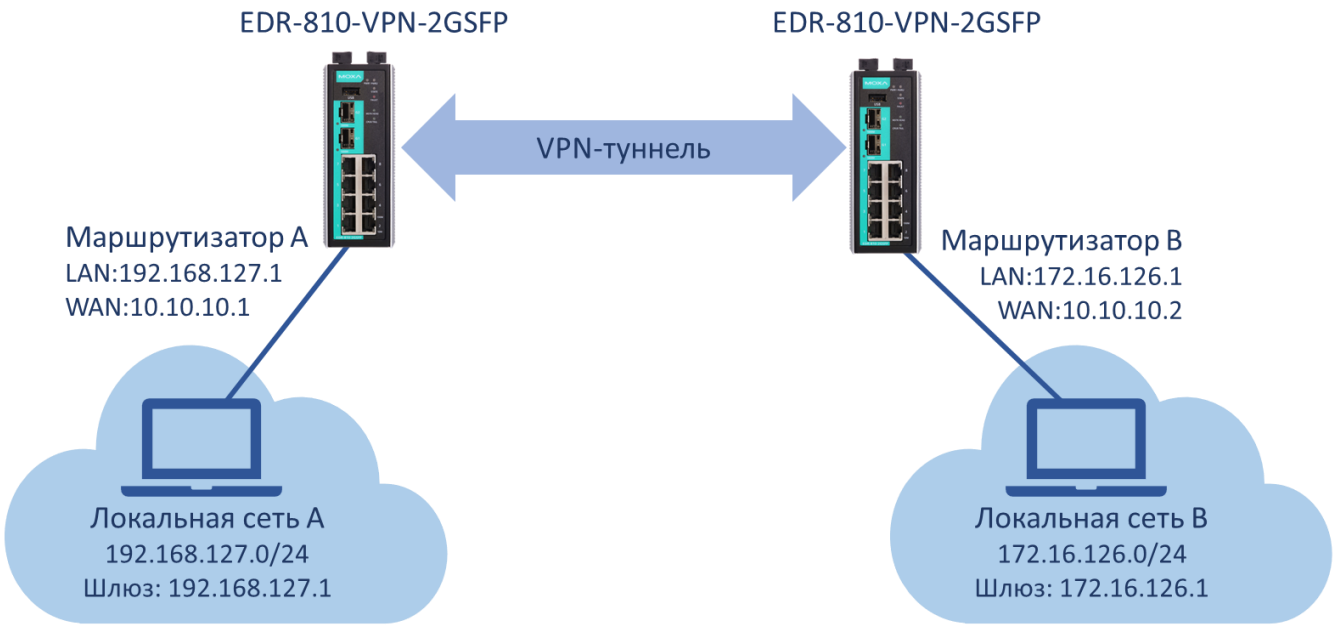


Рисунок 1 «Схема сети»

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

Таблица 1 «Адресация сети»

	IP-адрес	Маска подсети	Основной шлюз
Маршрутизатор A LAN-интерфейс	192.168.127.1	255.255.255.0	
Маршрутизатор A WAN-интерфейс	10.10.10.1	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети A	192.168.127.13	255.255.255.0	192.168.127.1
Маршрутизатор B LAN-интерфейс	172.16.126.1	255.255.255.0	
Маршрутизатор B WAN-интерфейс	10.10.10.2	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети B	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 A и B 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: moxa

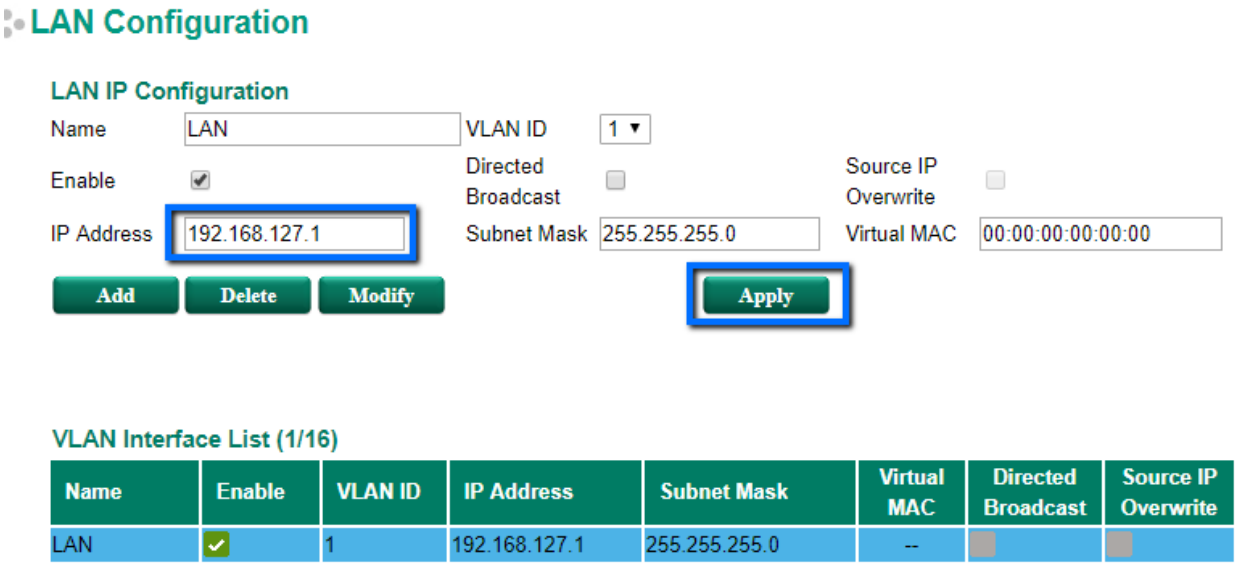
В целях безопасности рекомендуется изменить данные для входа.

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

1. Настройка Маршрутизатора A

1.1. Настройка LAN-интерфейса

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



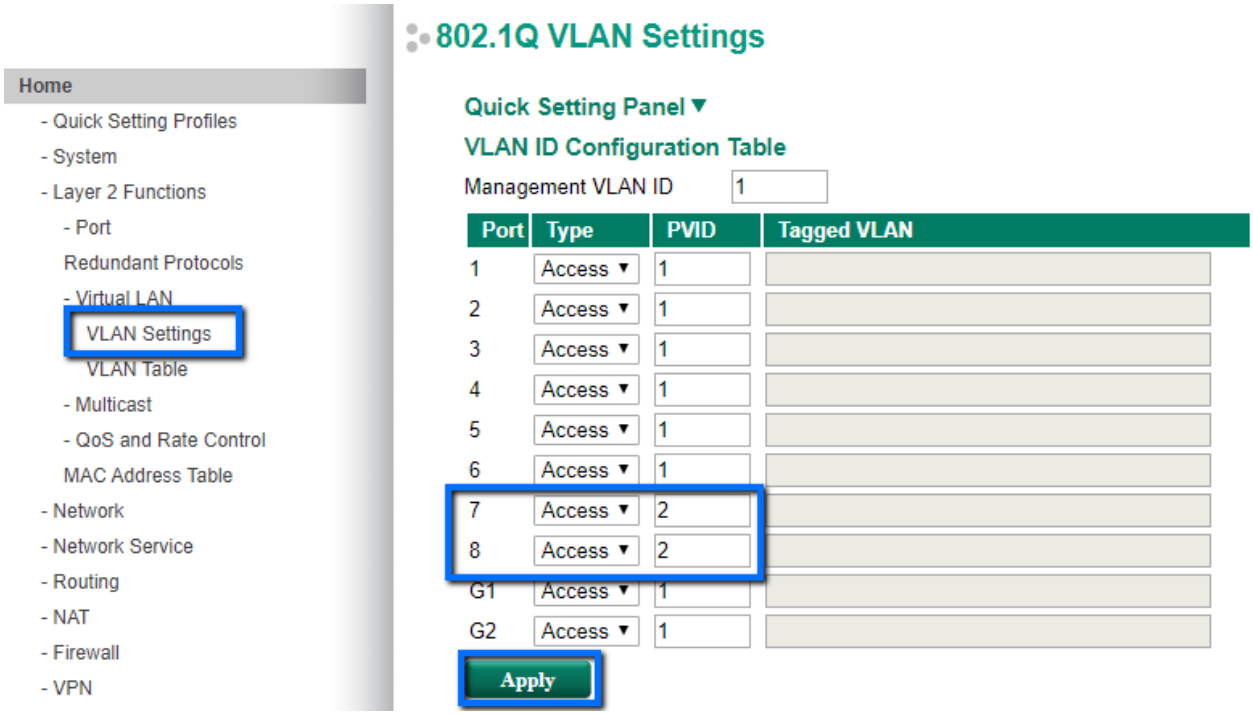
1.2. Настройка WAN-интерфейса

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***.

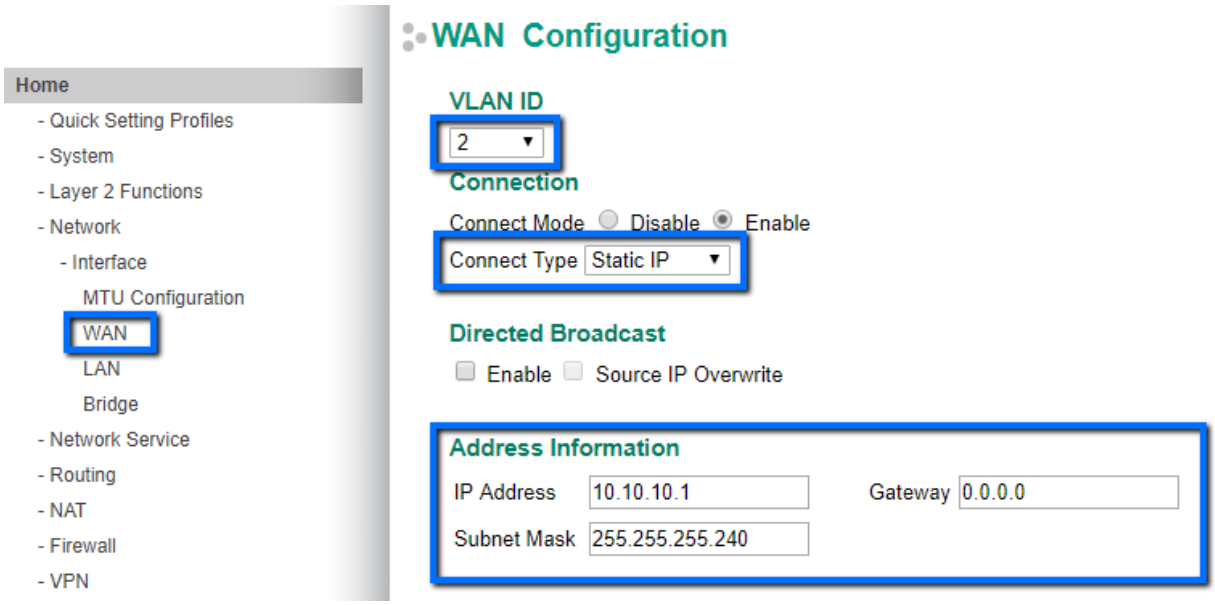
Порты 7 и 8 маршрутизатора будут относиться к WAN-интерфейсу. На этих портах указываем VLAN ID 2.



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

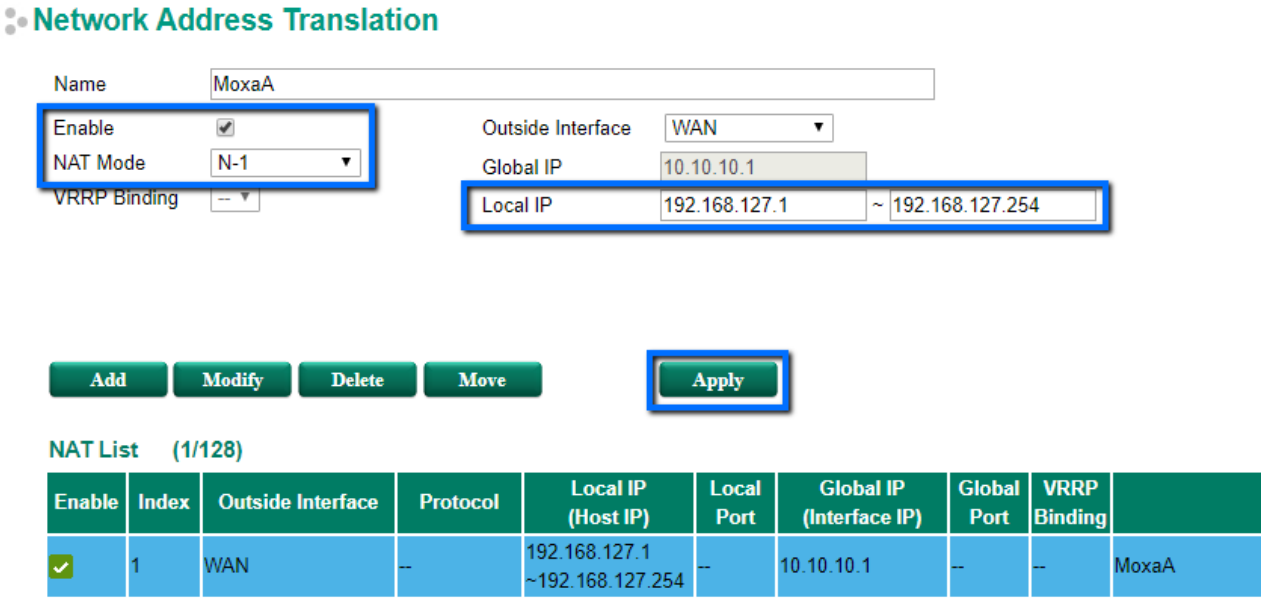
- Адресация WAN-интерфейса

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



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***

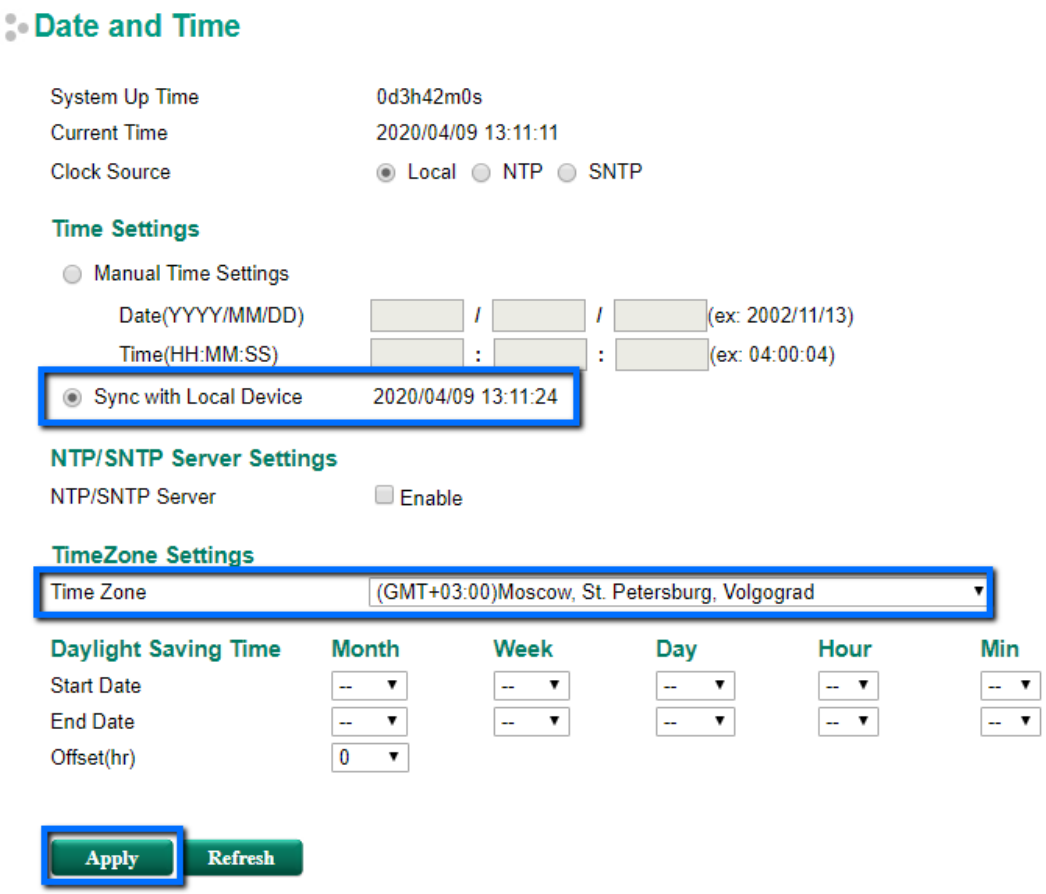


1.4. Настройка даты и времени

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.



2. Настройка Маршрутизатора B

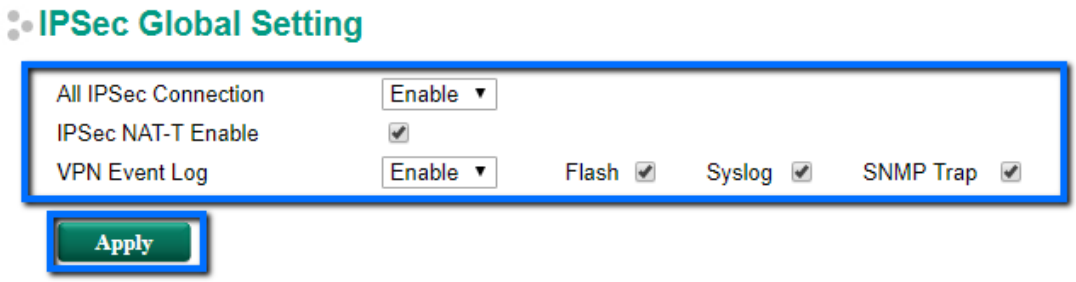
Для настройки Маршрутизатора B необходимо повторить шаги 1.1 – 1.4, указывая параметры в соответствии с Таблицей 1.

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)



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

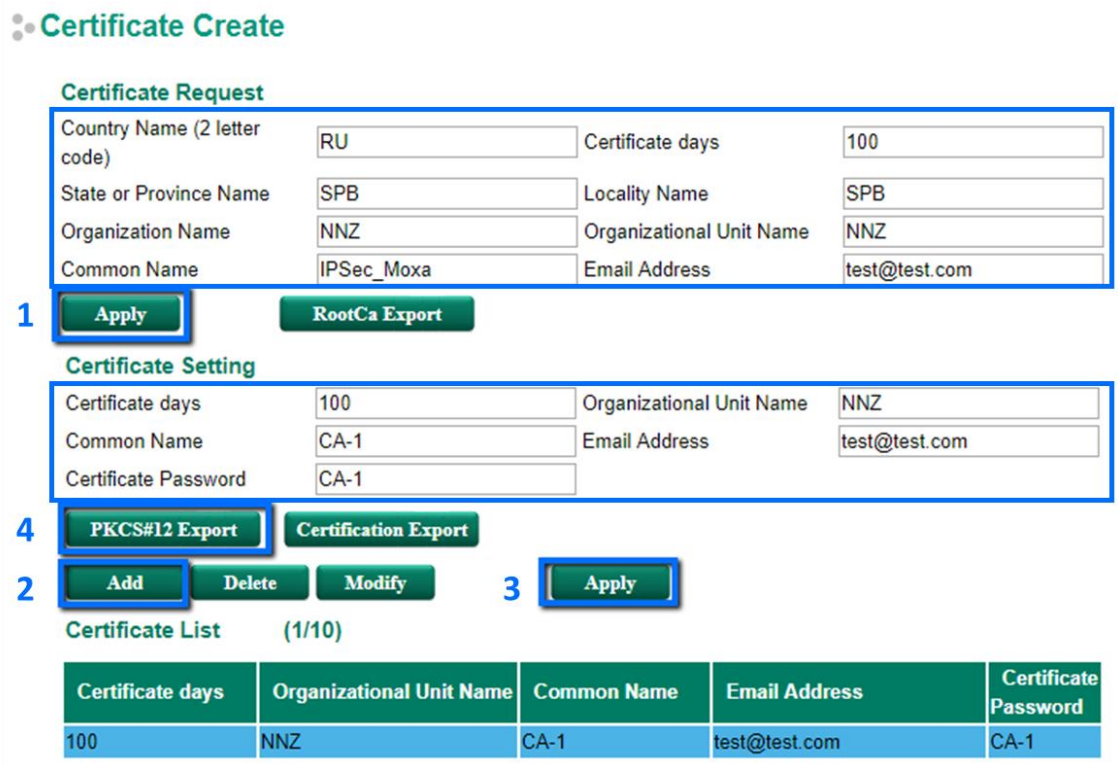
В разделе ***Certificate Management - CA Server - Certificate Create*** нужно выполнить несколько шагов:

- 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.

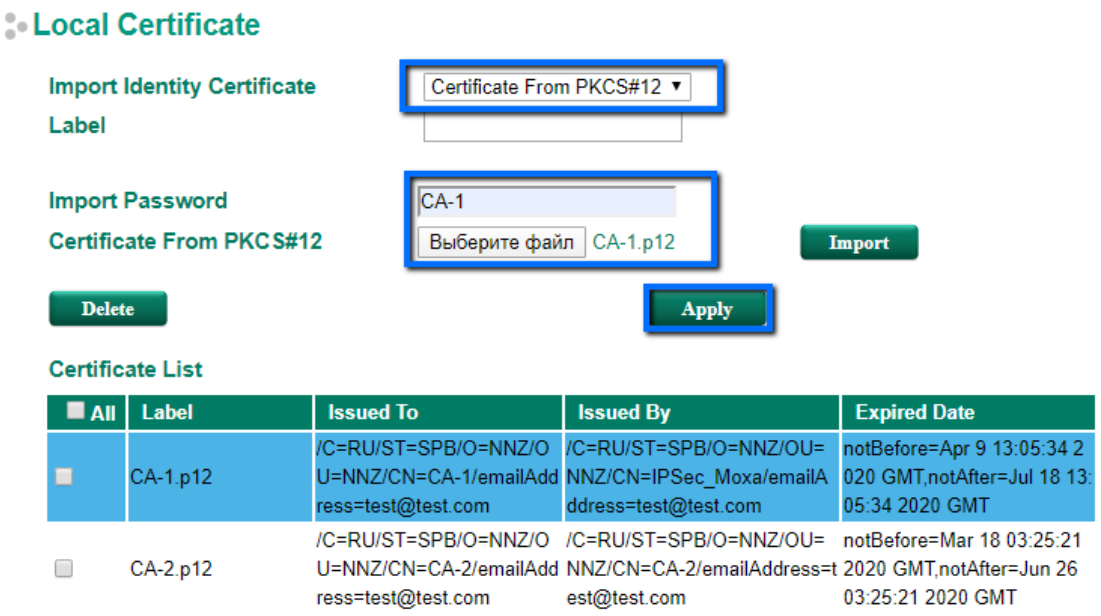
Таблица 2 «Сертификаты безопасности»

	Тип сертификата	Название сертификата
Маршрутизатор A	PKCS	CA-1
Маршрутизатор B	PKCS	CA-2



- Загрузка сертификаты на маршрутизатор

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

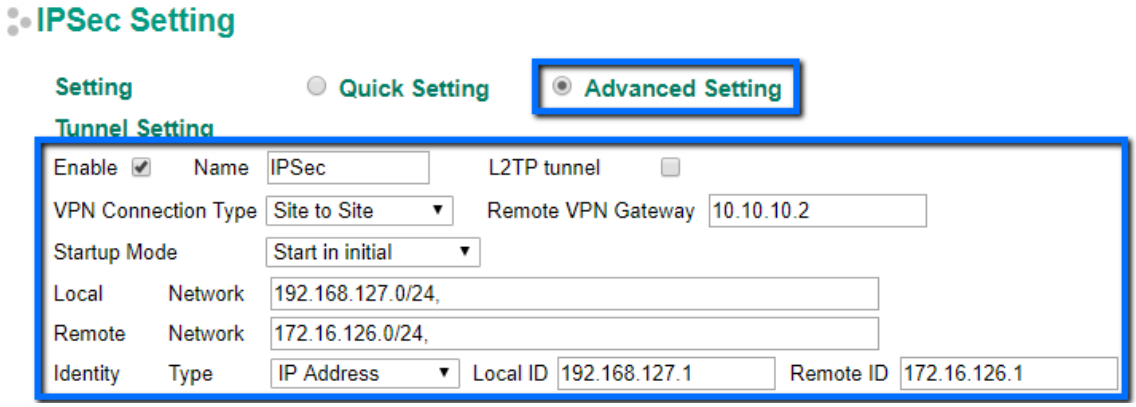


3.3. Настройка параметров VPN-соединения

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

- Маршрутизатор А – VPN-клиент.

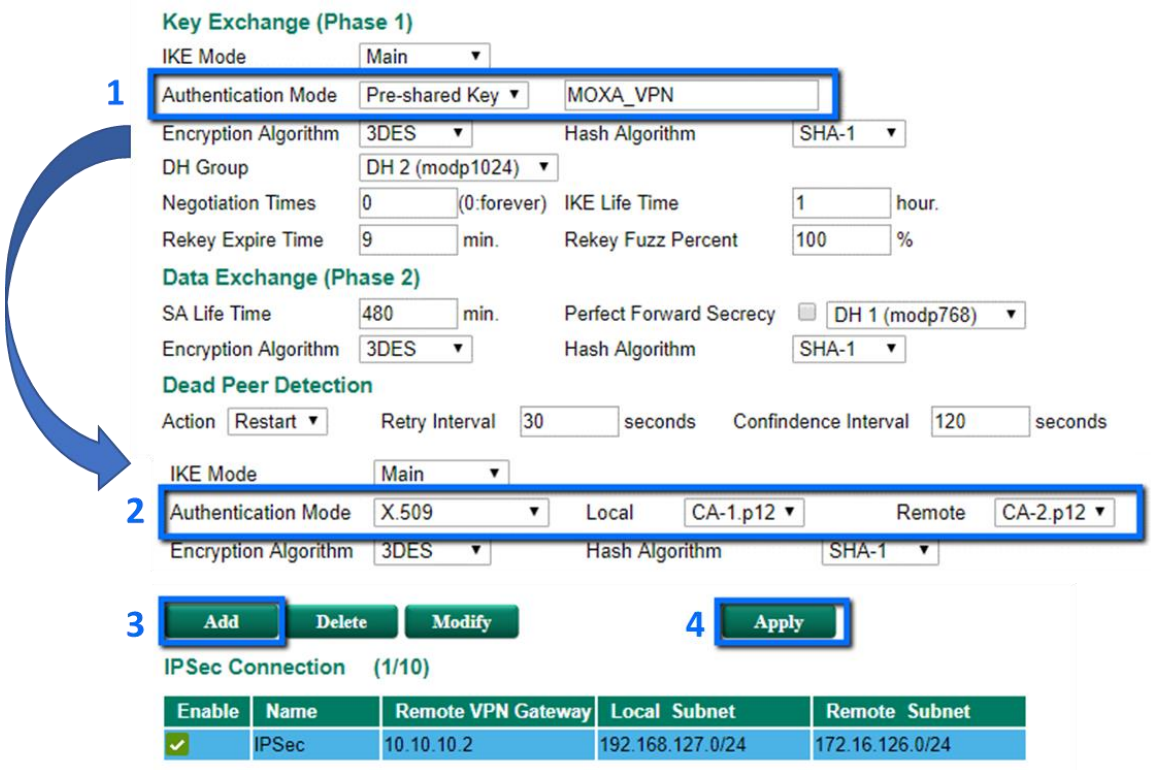
Маршрутизатор A будет инициировать VPN-соединение. То есть режим работы устанавливается как ***Start in initial***.



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

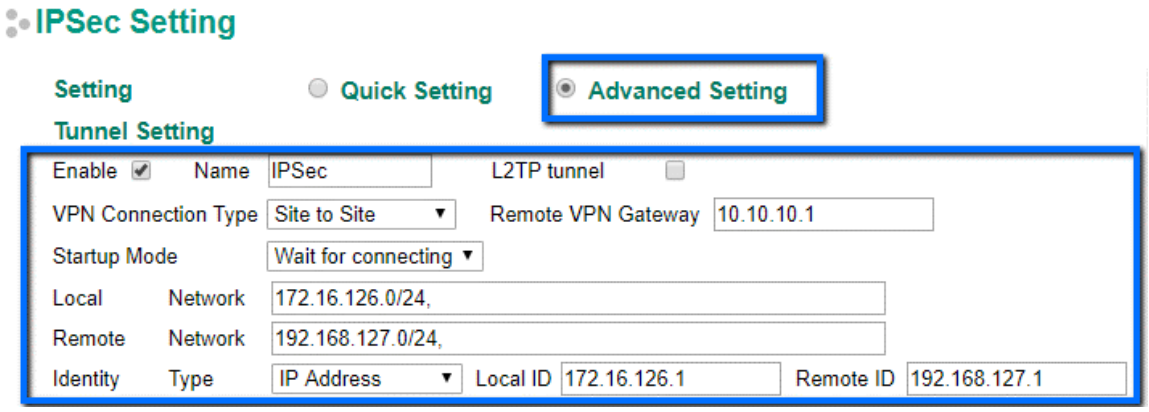
Затем нужно выбрать режим аутентификации X.509 и два загруженных сертификата.

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

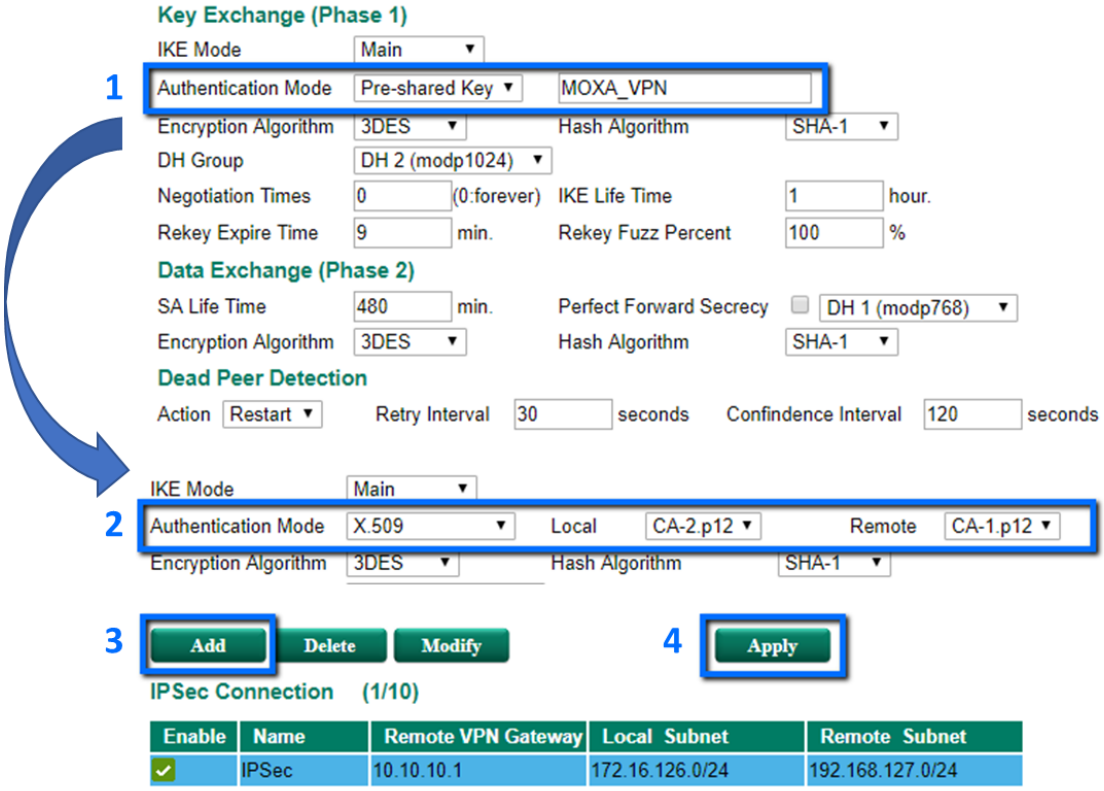


- Маршрутизатор B – VPN-сервер.

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



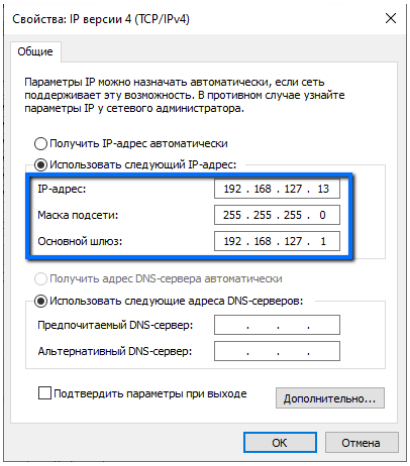
На маршрутизаторе В локальным сертификатом будет сертификат CA-2, а удаленным – CA-1

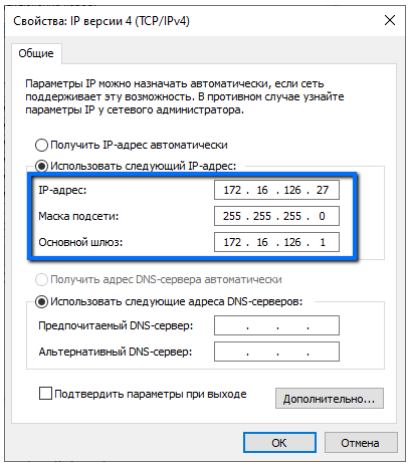


3.4. Настройка устройств в локальных сетях

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

Для локальной сети A: 192.168.127.1
Для локальной сети B: 172.16.126.1





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 cerificate mismatch to local certificate
12	2020/04/09	17:05:32	IPSec	<5> Notice	[IPSec/1x1] Initiating VPN connection

Refresh | Export | Clear