Настройка IPSec между межсетевым экраном DFL-210/800 и DI-804HV

IPSec строим исходя из данных:

DFL:

Внутренняя сеть (lannet): 192.168.1.0/24
IP на WAN (wan_ip): 192.168.110.10

DI-804HV:

Внутренняя сеть: 192.168.0.0
IP на WAN: 192.168.110.100

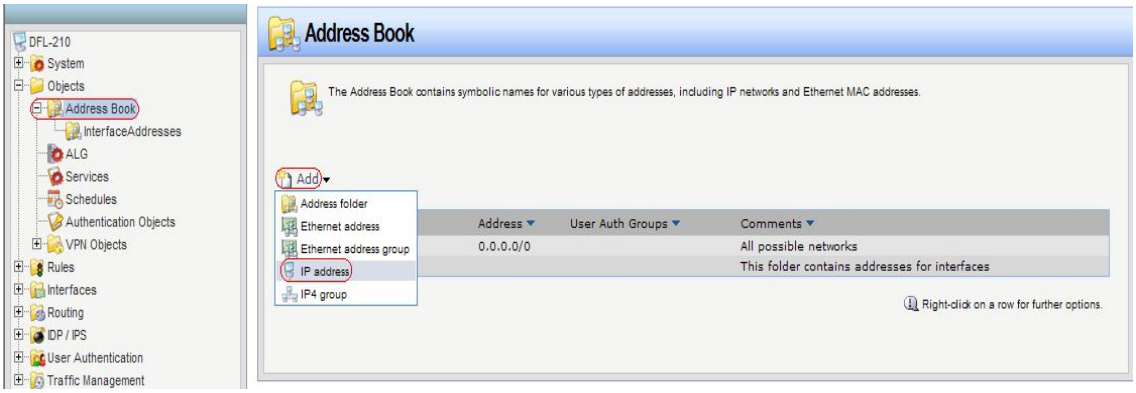
Настройка IPSec на DFL.

Откройте Web-браузер, введите IP-адрес межсетевого экрана в адресную строку (по умолчанию 192.168.1.1) и нажмите **Enter.** Авторизуйтесь (по умолчанию пароль и логин admin).

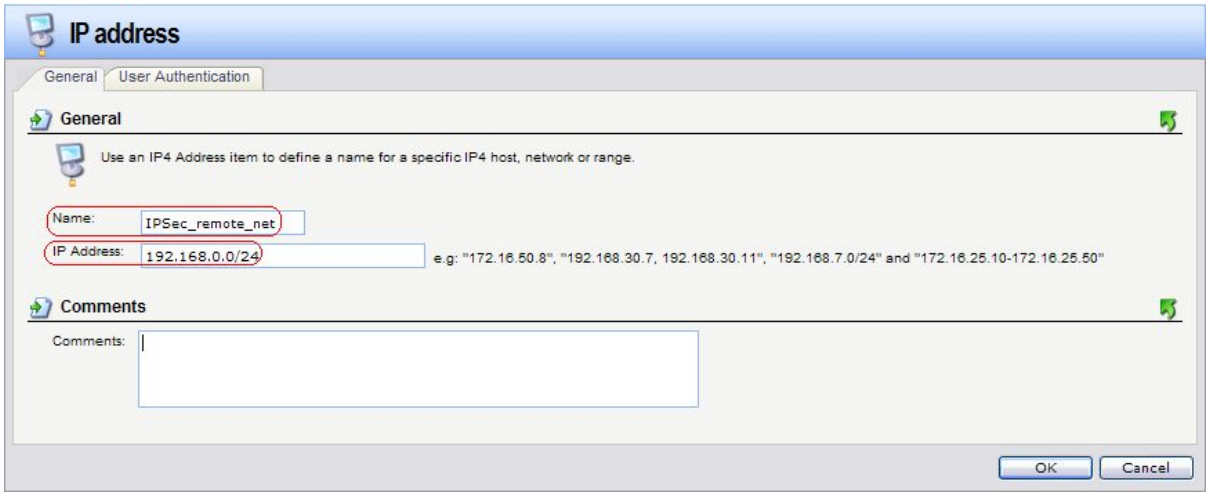
Далее добавляем нужные нам объекты:

IPSec_remote_net: **192.168.0.0/24**
IPSec_remote_endpoint: **192.168.110.100**

Кликните по знаку «+» рядом с папкой **Objects** и выберите **Address Book**, затем нажмите **Add**, из меню выберете **IP4 Host/Network.**



Например, добавим **IPSec_remote_net**



После заполнения всех полей нажимаем ОК.

Теперь добавим Pre-Shared Key

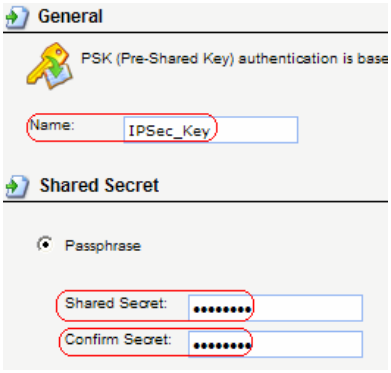
Кликните по знаку «+» рядом с папкой **Objects** и выберите **Authentication Objects**, затем нажмите **Add**, из меню выберите **Pre-Shared Key.**

Заполняем поля так:

Name: **IPSec_Key**

<u>Passphrase</u>

Shared Secret: Указываем ключ, например 1029384756
Confirm Secret: Повторяем ключ.

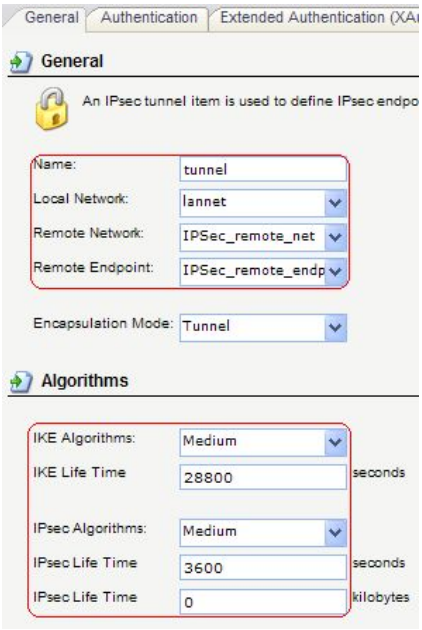


После заполнения всех полей нажимаем ОК.

Добавляем IPSec.

Кликните по знаку «+» рядом с папкой **Interfaces** и выберите **IPSec**, затем нажмите **Add**, из меню выберите **IPSec Tunnel**.

Поля заполняем так:



В **General**

Name: **Tunnel**
Local Network: **lannet**
Remote Network: **IPSec_remote_net**
Remote Endpoint: **IPSec_remote_endpoint**

Encapsulation Mode: **Tunnel**

В **Algorithms**

IKE Algorithms: **Medium**
IKE Life Time: **2880**
IPsec Algorithms: **Medium**
IPsec Life Time: **3600**

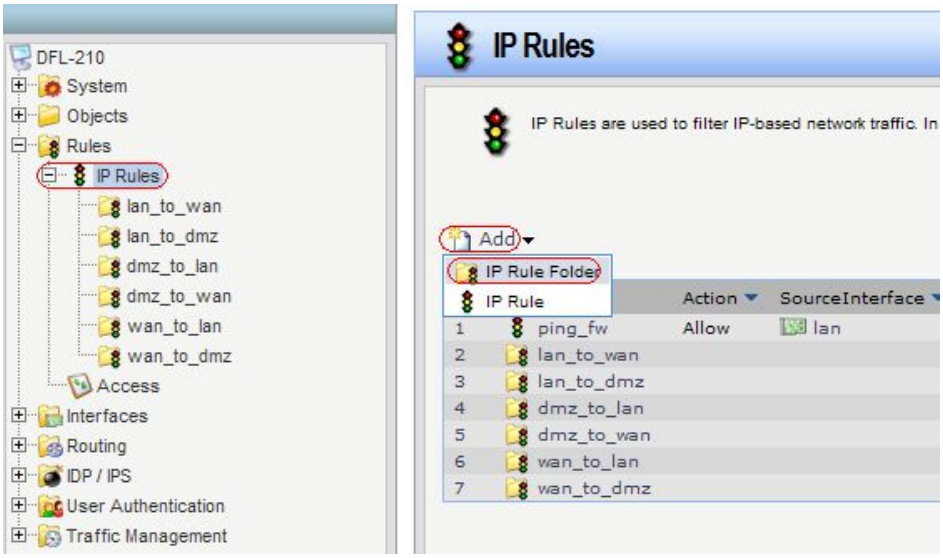
Наверху выберите вкладку **Authentication.**

Укажите в поле Pre-shared Key: **IPSec_Key.**

После заполнения всех полей нажимаем ОК.

Создаем разрешающие правила для доступа из IPSec в lan и наоборот.

Кликните по знаку «+» рядом с папкой **Rules,** далее по знаку «+» рядом с папкой **IP Rules** и выберите эту папку, нажмите кнопку **Add**, укажите **IP Rule Folder**, поле Name укажите **IPSec** и нажмите OK.



Нажмите кнопку **Add**, укажите **IP Rule**.

Заполните поля как показано на рисунке:

В **General**

Name: **IPSec_to_lan**
Action: **Allow**
Service: **all_services**

В **Address Filter**

Source:
Interface: **tunnel**
Network: **IPSec_remote_net**

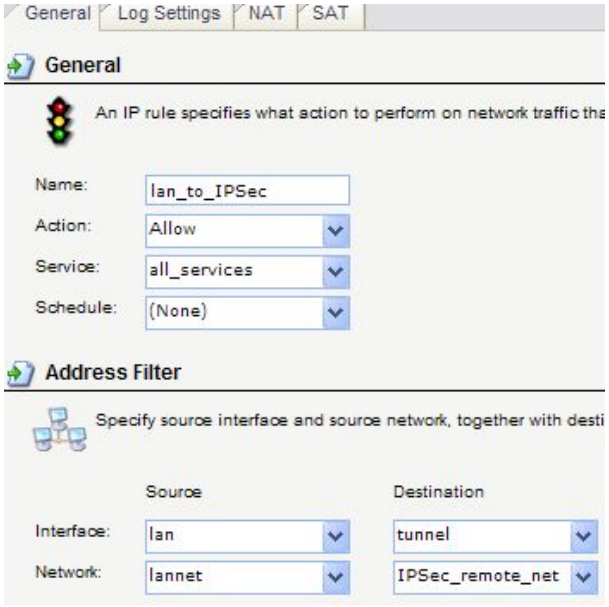
Destination:
Interface: **lan**
Network: **lannet**

Нажмите OK.

Создаем второе правило.

Нажмите кнопку **Add**, укажите **IP Rule**.

Заполните поля как показано на рисунке:



В **General**

Name: **lan_to_IPSec**
Action: **Allow**
Service: **all_services**

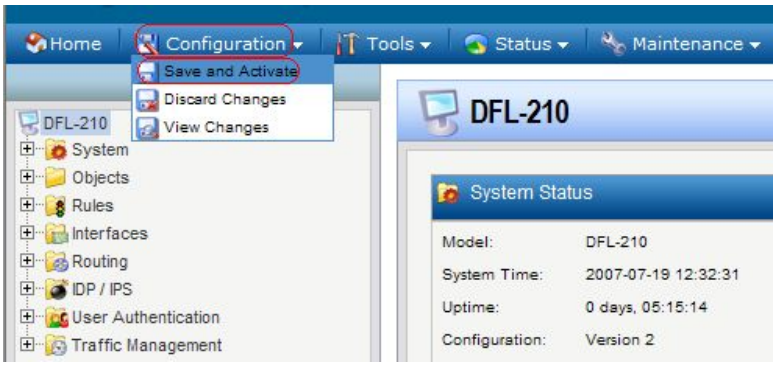
В **Address Filter**

Source:
Interface: **lan**
Network: **lannet**

Destination:
Interface: **tunnel**
Network: **IPSec_remote_net**

Нажмите ОК.

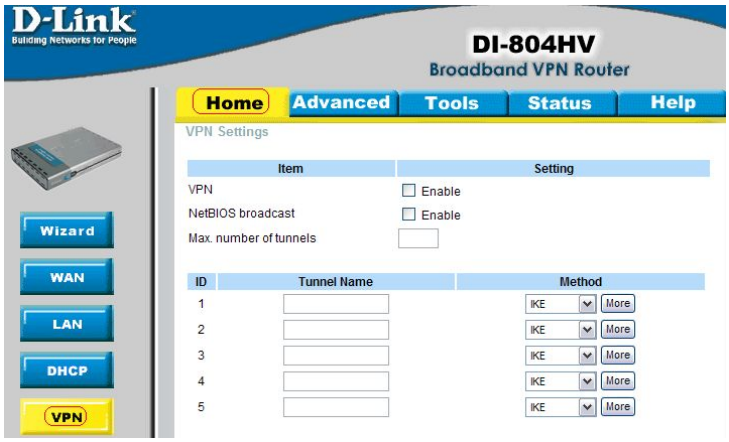
Теперь примените настройки. Наверху меню **Configuration** выберите **Save and Activate,** нажмите ОК и дождитесь применения настроек.



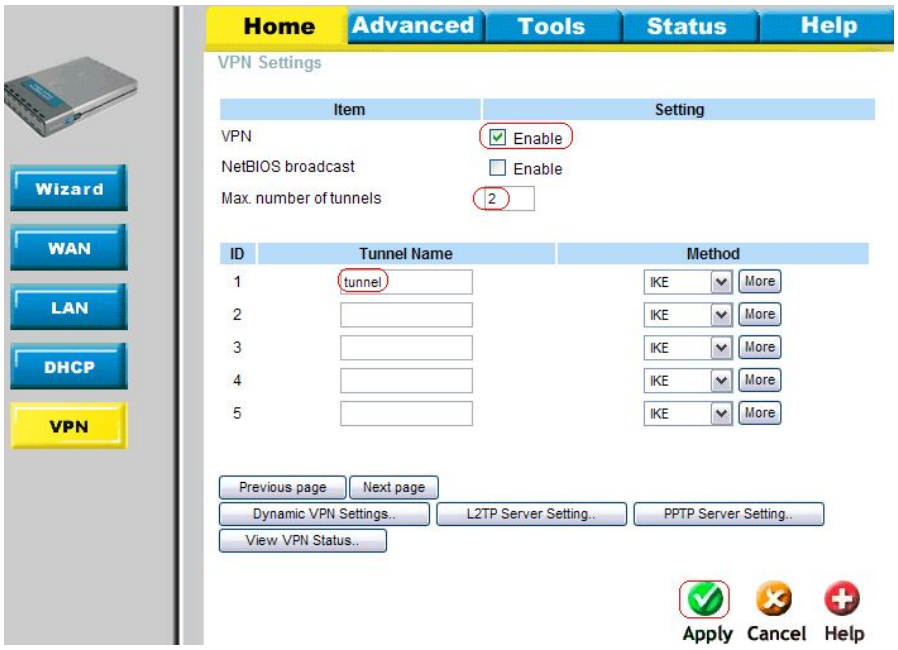
Настройка IPSec на DI-804HV.

Откройте Web-браузер и введите IP-адрес DI-824HV в адресную строку (по умолчанию 192.168.0.1) и нажмите **Enter.** Авторизуйтесь.

Кликните с верху на вкладке **Home**, выберите внизу слева **VPN**.

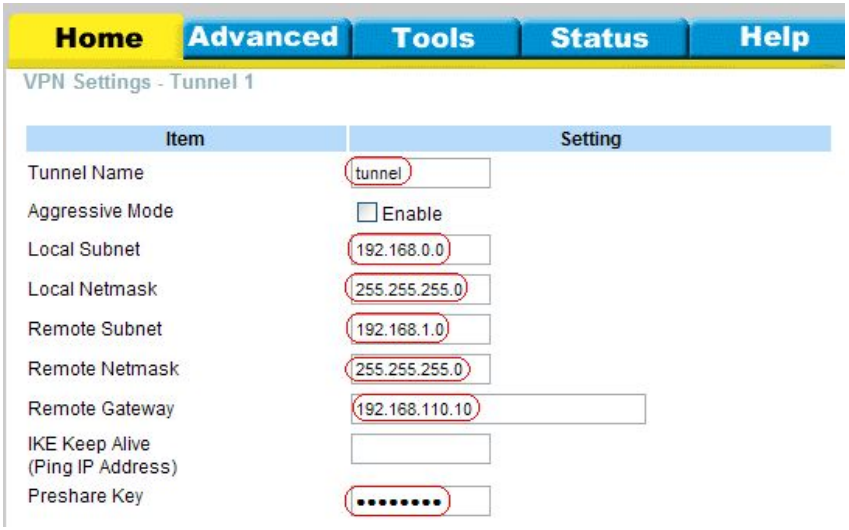


Поставьте галочку в поле **VPN** на Enable, в поле **Max number of tunnels** поставьте 2, далее занесите в поле **Tunnel Name** с **ID 1** tunnel и нажмите apply, дождитесь применения настроек и нажмите **continue.**



Нажмите на кнопку **More** напротив заполненного поля tunnel и заполните поля следующим образом:

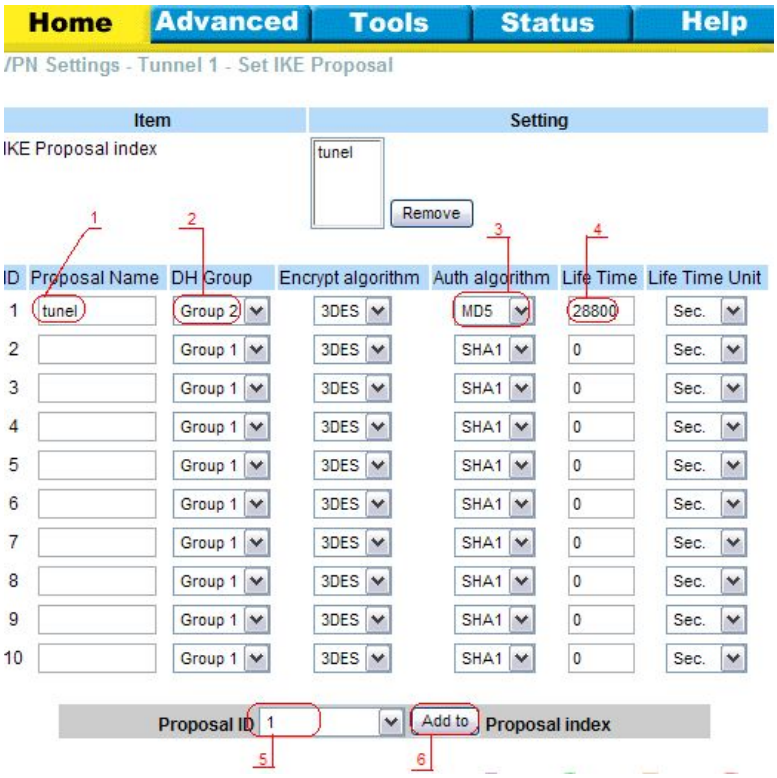
Tunnel Name: **Tunnel**
Local Subnet: **192.168.0.0**
Local Mask: **255.255.255.0**
Remote Subnet: **192.168.1.0**
Remote Mask: **255.255.255.0**
Remote Gateway: **192.168.110.10**
Preshare Key: Введите ключ такой же как ввели при настройки DFL например 1029384756



Нажмите **Apply**, дождитесь применения настроек и нажмите **continue.**

Настраиваем IKE Proposal.

Нажмите кнопку **Select IKE Proposal** и заполните поля как показано на рисунке:

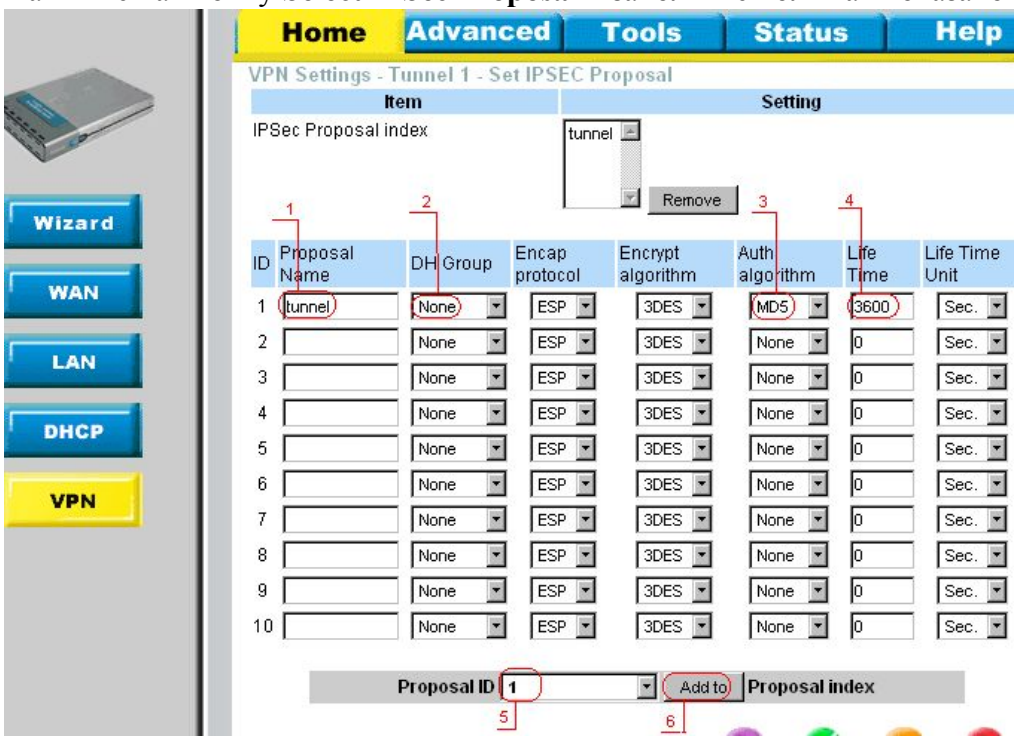


Шаг 1: В поле **Proposal Name** укажите **Tunnel**.
Шаг 2: В поле **DH Group** из выпадающего меню выберите **Group 2**.
Шаг 3: В поле **Auth algorithm** из выпадающего меню выберите **MD5**.
Шаг 4: В поле **Life Time** укажите **28800**.
Шаг 5 и 6: В поле **Proposal ID** из выпадающего меню выберите **1** и нажмите кнопку **Add to**.

После заполнения всех полей нажмите **Apply**, дождитесь применения настроек и нажмите **continue**. Далее нажмите кнопку **Back**.

Настраиваем IPSec Proposal.

Нажмите на кнопку **Select IPSec Proposal** и заполните поля как показано на рисунке:

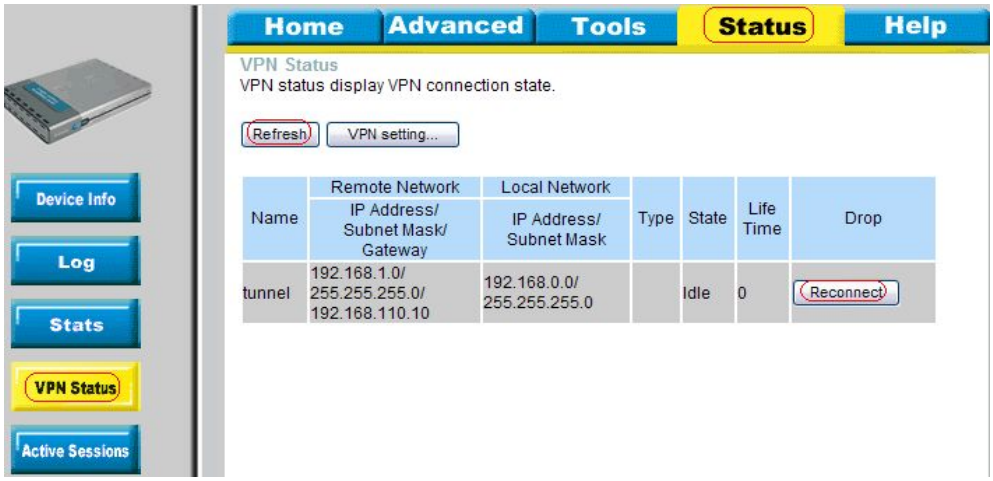


Шаг 1: В поле **Proposal Name** укажите **Tunnel**.
Шаг 2: В поле **DH Group** из выпадающего меню выберите **None**.
Шаг 3: В поле **Auth algorithm** из выпадающего меню выберите **MD5**.
Шаг 4: В поле **Life Time** укажите **3600**.
Шаг 5 и 6: В поле **Proposal ID** из выпадающего меню выберите **1** и нажмите кнопку **Add to**.

После заполнения всех полей нажмите **Apply**, дождитесь применения настроек и нажмите **continue**.

Проверяем тоннель IPSec.

Кликните сверху на вкладке **Status**, выберите внизу слева **VPN Status**, нажмите кнопку reconnect, затем нажмите кнопку refresh.



Смотрим поля **Type** и **State**, если они соответствуют тому, что приведено на рисунке ниже, то тоннель установлен.