

## 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.

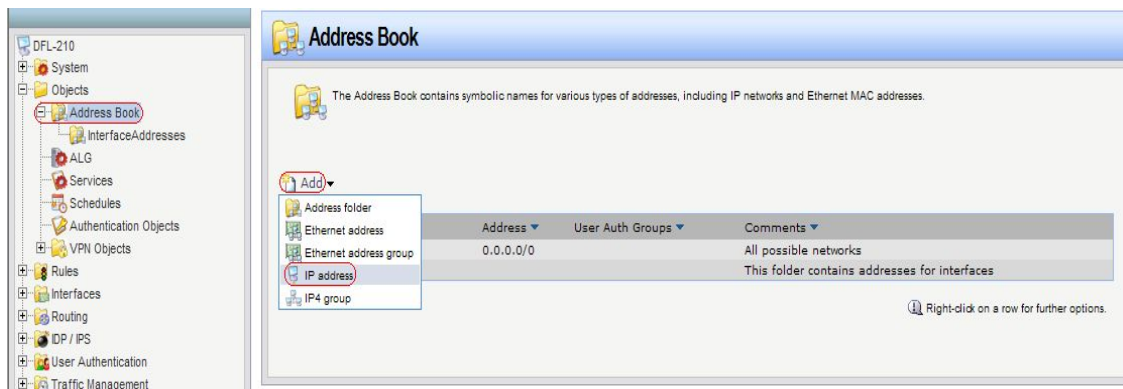
Откройте Web-браузер, введите IP-адрес межсетевого экрана в адресную строку (по умолчанию 192.168.1.1) и нажмите **Enter**. Авторизуйтесь (по умолчанию пароль и логин admin).

Далее добавляем нужные нам объекты:

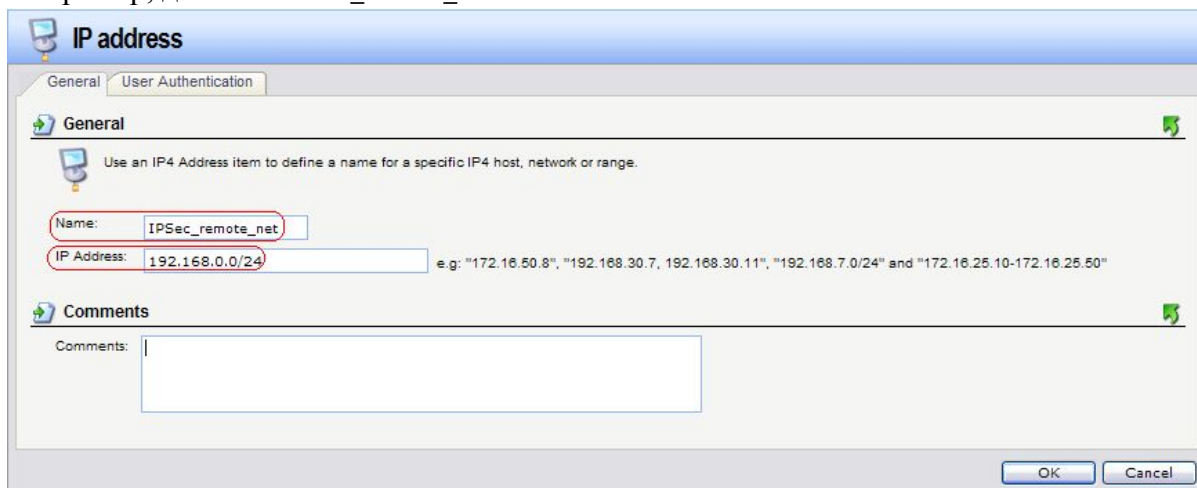
IPSec\_remote\_net: **192.168.0.0/24**

IPSec\_remote\_endpoint: **192.168.110.100**

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



Например, добавим **IPSec\_remote\_net**



**IP address**

General User Authentication

**General**

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: IPSec\_remote\_net

IP Address: 192.168.0.0/24 e.g. "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

**Comments**

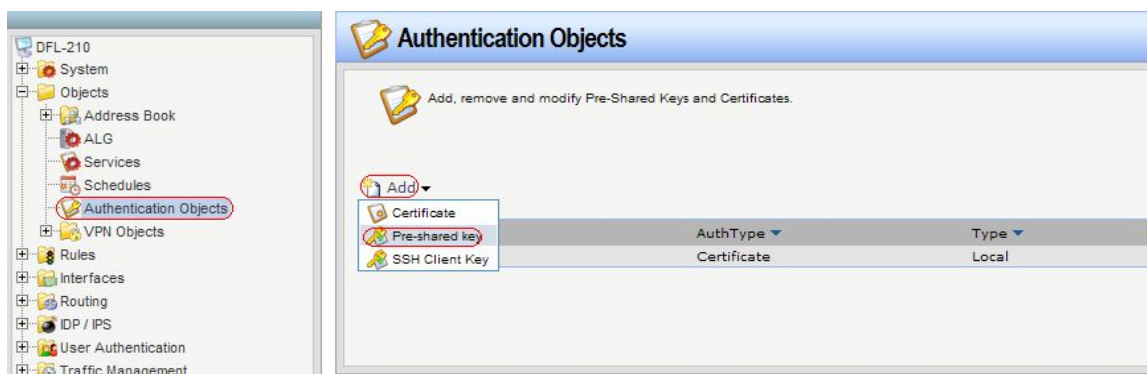
Comments:

OK Cancel

После заполнения всех полей нажимаем **OK**.

**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**.



**Authentication Objects**

Add, remove and modify Pre-Shared Keys and Certificates.

Add

	AuthType	Type
Certificate	Certificate	Local
Pre-shared key		
SSH Client Key		

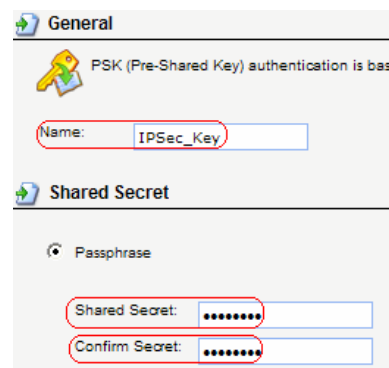
Заполняем поля так:

Name: **IPSec\_Key**

**Passphrase**

Shared Secret: Указываем ключ, например 1029384756

Confirm Secret: Повторяем ключ.



**General**

PSK (Pre-Shared Key) authentication is base

Name: IPSec\_Key

**Shared Secret**

Passphrase

Shared Secret: .....

Confirm Secret: .....

После заполнения всех полей нажимаем **OK**.

## 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**

The screenshot shows the 'General' tab of the IPsec Tunnel configuration window. The 'Name' field is set to 'tunnel'. The 'Local Network' dropdown is set to 'lannet'. The 'Remote Network' dropdown is set to 'IPSec\_remote\_net'. The 'Remote Endpoint' dropdown is set to 'IPSec\_remote\_endp'. The 'Encapsulation Mode' dropdown is set to 'Tunnel'. The 'Algorithms' section shows 'IKE Algorithms' set to 'Medium', 'IKE Life Time' set to '2880' seconds, 'IPsec Algorithms' set to 'Medium', 'IPsec Life Time' set to '3600' seconds, and 'IPsec Life Time' set to '0' kilobytes.

Наверху выберите вкладку **Authentication**.

Укажите в поле Pre-shared Key: **IPSec\_Key**.

The screenshot shows the 'Authentication' tab of the IPsec Tunnel configuration window. The 'Pre-shared Key' radio button is selected. The 'Pre-shared Key' dropdown is set to 'IPSec\_Key'. The 'X.509 Certificate' section is unselected, and the 'Root Certificate(s)' list contains 'AdminCert'. The 'Gateway Certificate' and 'Identification List' dropdowns are both set to '(None)'.

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 ОК.



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:

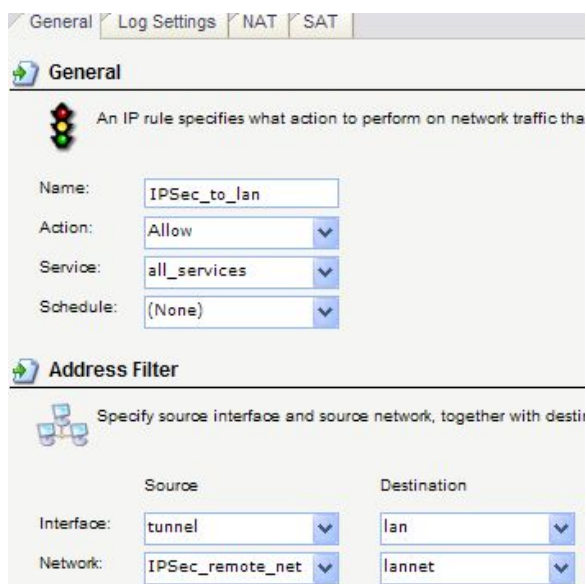
Interface: **tunnel**

Network: **IPSec\_remote\_net**

Destination:

Interface: **lan**

Network: **lannet**



Нажмите ОК.

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**

General | Log Settings | NAT | SAT

**General**

An IP rule specifies what action to perform on network traffic that

Name:

Action:

Service:

Schedule:

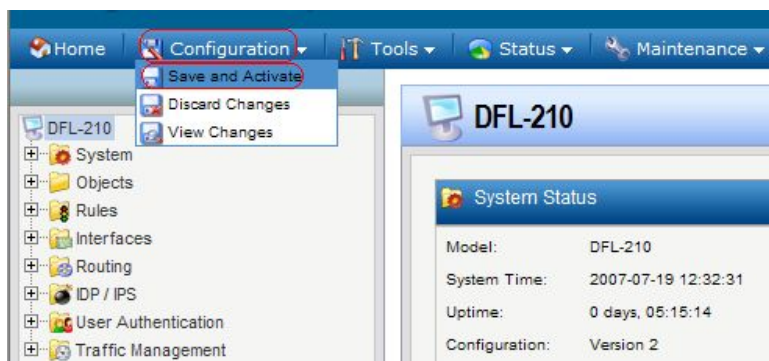
**Address Filter**

Specify source interface and source network, together with destination

	Source	Destination
Interface:	<input type="text" value="lan"/>	<input type="text" value="tunnel"/>
Network:	<input type="text" value="lannet"/>	<input type="text" value="IPSec_remote_net"/>

Нажмите **OK**.

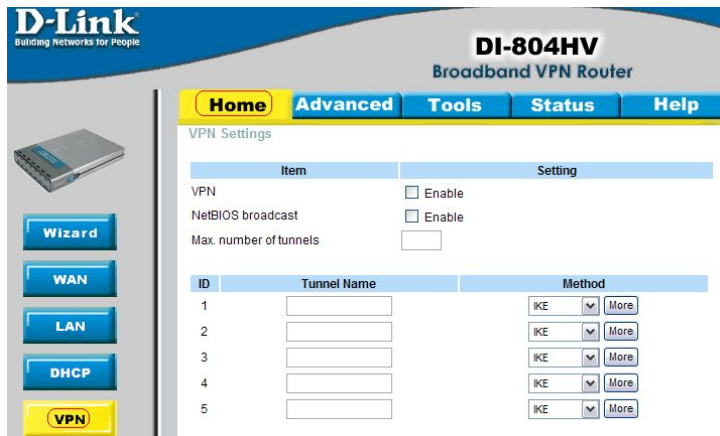
Теперь примените настройки. Вверху меню **Configuration** выберите **Save and Activate**, нажмите **OK** и дождитесь применения настроек.



## 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**.



D-Link Building Networks for People

**DI-804HV**  
Broadband VPN Router

Home Advanced Tools Status Help

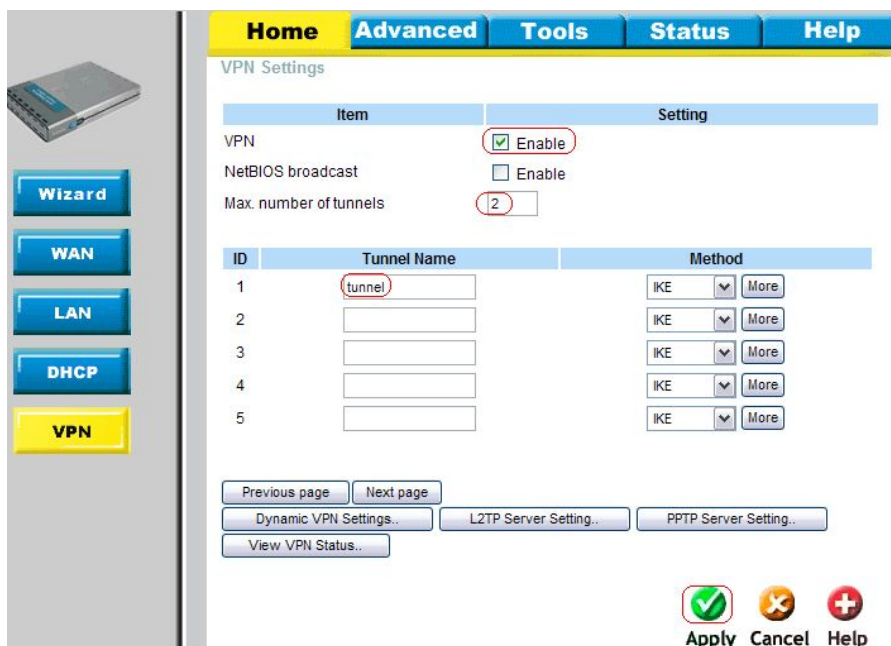
VPN Settings

Item	Setting
VPN	<input type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	<input type="text"/>

ID	Tunnel Name	Method
1	<input type="text"/>	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>

Wizard  
WAN  
LAN  
DHCP  
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**.



Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	<input type="text" value="2"/>

ID	Tunnel Name	Method
1	tunnel	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>

Previous page Next page

Dynamic VPN Settings.. L2TP Server Setting.. PPTP Server Setting..

View VPN Status..

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 настройке DFL например 1029384756

Item	Setting
Tunnel Name	tunnel
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.110.10
IKE Keep Alive (Ping IP Address)	
Preshare Key	*****

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

### Настраиваем IKE Proposal.

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

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	tunnel	Group 2	3DES	MD5	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Proposal ID: 1 Add to Proposal index

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:

The screenshot shows the 'VPN Settings - Tunnel 1 - Set IPSEC Proposal' configuration page. The page has a navigation bar with 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. Below the navigation bar is a table with 'Item' and 'Setting' columns. The 'Item' column contains 'IPSec Proposal index' and a dropdown menu showing 'tunnel'. The 'Setting' column contains a 'Remove' button. Below the table is a list of proposals with columns: ID, Proposal Name, DH Group, Encap protocol, Encrypt algorithm, Auth algorithm, Life Time, and Life Time Unit. The first proposal (ID 1) is highlighted with red circles and numbers 1-4 indicating the configuration steps: 1. Proposal Name: Tunnel, 2. DH Group: None, 3. Auth algorithm: MD5, 4. Life Time: 3600. At the bottom, there is a 'Proposals' section with a dropdown menu showing '1' and an 'Add to' button, with red numbers 5 and 6 indicating the steps: 5. Proposal ID: 1, 6. Add to.

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	Tunnel	None	ESP	3DES	MD5	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

Proposals: Proposal ID: 1 Add to Proposal index

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**.

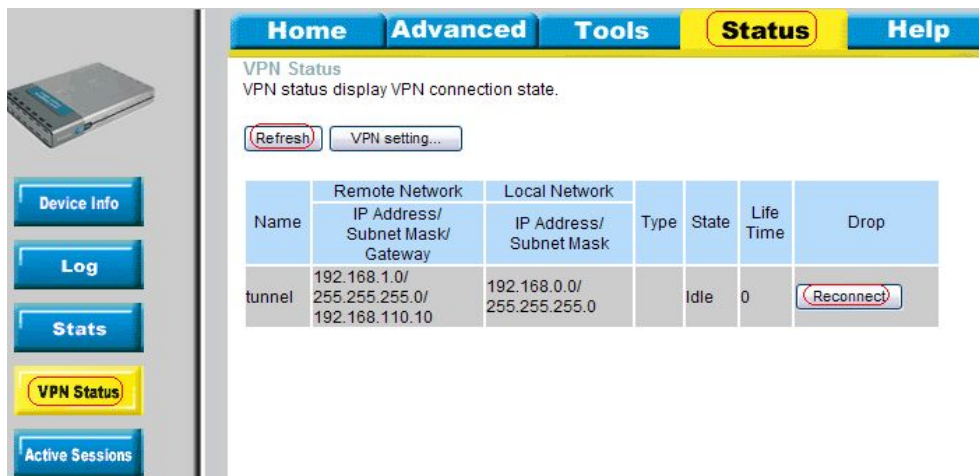
Шаг 4: В поле **Life Time** укажите **3600**.

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.

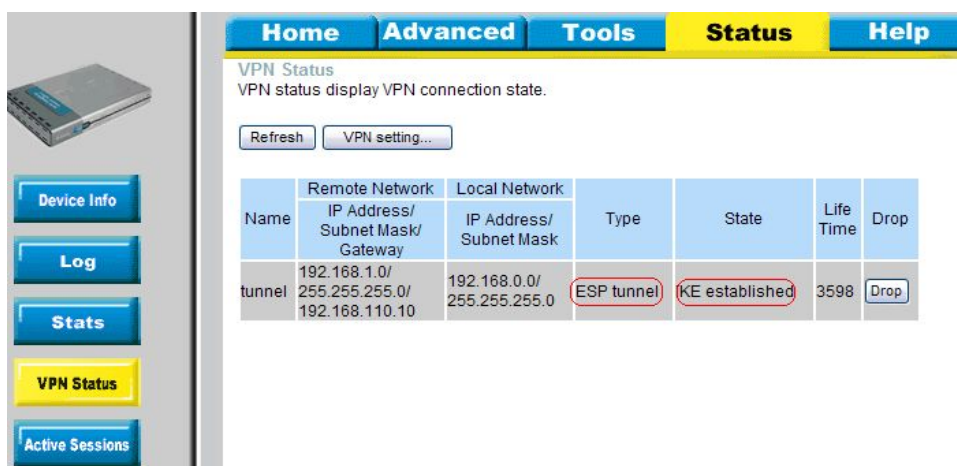
Кликните сверху на вкладке **Status**, выберите внизу слева **VPN Status**, нажмите кнопку reconnect, затем нажмите кнопку refresh.



The screenshot shows the 'VPN Status' page with the 'Status' tab selected. The page title is 'VPN Status' and the subtitle is 'VPN status display VPN connection state.' There are two buttons: 'Refresh' and 'VPN setting...'. Below is a table with the following data:

Name	Remote Network	Local Network	Type	State	Life Time	Drop
	IP Address/ Subnet Mask/ Gateway	IP Address/ Subnet Mask				
tunnel	192.168.1.0/ 255.255.255.0/ 192.168.110.10	192.168.0.0/ 255.255.255.0		Idle	0	Reconnect

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



The screenshot shows the 'VPN Status' page with the 'Status' tab selected. The page title is 'VPN Status' and the subtitle is 'VPN status display VPN connection state.' There are two buttons: 'Refresh' and 'VPN setting...'. Below is a table with the following data:

Name	Remote Network	Local Network	Type	State	Life Time	Drop
	IP Address/ Subnet Mask/ Gateway	IP Address/ Subnet Mask				
tunnel	192.168.1.0/ 255.255.255.0/ 192.168.110.10	192.168.0.0/ 255.255.255.0	ESP tunnel	KE established	3598	Drop