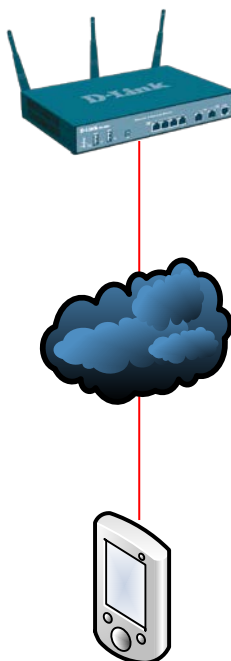


Настройка L2TP поверх IPSec для мобильных клиентов

Пример:

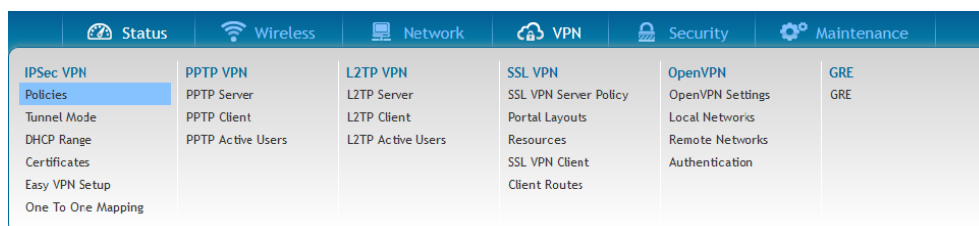
WAN 1 Static IP



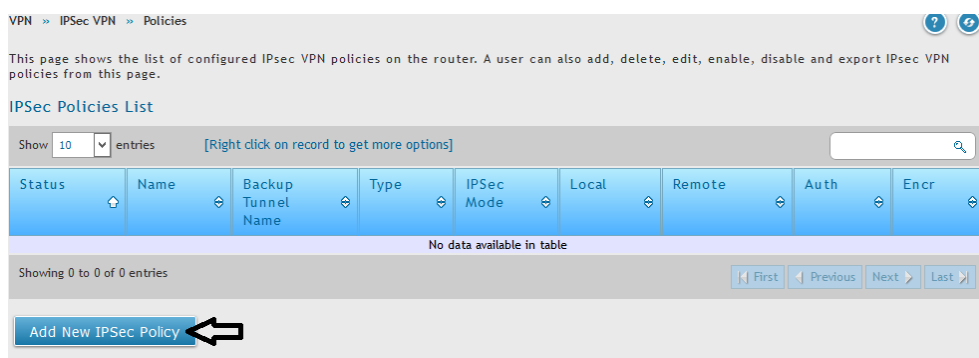
L2TP over IPSec client (ANDROID, PC Windows)

Итак приступим, вот что было проделано для создания рабочей среды:

1) Открываем пункт: VPN > IPSec VPN> Policies



2) Жмакаем: Add New IPSec Policy.



Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!

3) Выбираем значение как в таблице ниже:

GENERAL

Police Name: *Произвольное значение

L2TP Mode: Gateway

Remote Endpoint: FQDN

IP Address / FQDN: 0.0.0.0 (для подключения с любого IP адреса)

Phase1 (IKE SA Params)

Remote Endpoint: FQDN

IP Address / FQDN: 0.0.0.0 (для подключения с любого IP адреса)

Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

Authentication Method: Pre-Shared Key

Pre-Shared Key: *Произвольное значение (ключ IPSec)

Phase2 (Auto Policy Params)

Encryption Algorithm: 3DES

Integrity Algorithm: SHA1

4) Ну и жмем заветную **SAVE**

IPsec Policy Configuration

General

Policy Name	testIPSec
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	Gateway
IPsec Mode	Transport Mode
Select Local Gateway	Dedicated WAN
Remote Endpoint	FQDN
IP Address / FQDN	0.0.0.0
Enable Mode Config	OFF
Enable RollOver	OFF

Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!

Protocol

Enable Keepalive ☐ OFF

Phase1(IKE SA Parameters)

Exchange Mode

Direction / Type

Nat Traversal ☒ ON

NAT Keep Alive Frequency Seconds

Local Identifier Type

Remote Identifier Type

Remote Identifier

Encryption Algorithm

DES	<input type="checkbox"/> OFF	3DES	<input checked="" type="checkbox"/> ON
AES-128	<input type="checkbox"/> OFF	AES-192	<input type="checkbox"/> OFF
AES-256	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

Authentication Algorithm

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-256	<input type="checkbox"/> OFF	SHA2-384	<input type="checkbox"/> OFF
SHA2-512	<input type="checkbox"/> OFF		

Authentication Method

Pre-Shared Key

Diffie-Hellman (DH) Group

SA-Lifetime [Default: 28800, Range: 300 - 2147483647] Seconds

Enable Dead Peer Detection ☒ ON

Detection Period [Default: 10, Range: 10 - 999]

Reconnect after Failure Count [Default: 3, Range: 3 - 99]

Extended Authentication

Phase2(Auto Policy Parameters)

SA Lifetime

Encryption Algorithm

DES	<input type="checkbox"/> OFF	NONE	<input type="checkbox"/> OFF
3DES	<input checked="" type="checkbox"/> ON	AES-128	<input type="checkbox"/> OFF
AES-192	<input type="checkbox"/> OFF	AES-256	<input type="checkbox"/> OFF
TWOFISH (128)	<input type="checkbox"/> OFF	TWOFISH (192)	<input type="checkbox"/> OFF
TWOFISH (256)	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

Integrity Algorithm

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-224	<input type="checkbox"/> OFF	SHA2-256	<input type="checkbox"/> OFF
SHA2-384	<input type="checkbox"/> OFF	SHA2-512	<input type="checkbox"/> OFF
PFS Key Group	<input type="checkbox"/> OFF		

Redundant VPN Gateway Parameters

Enable Redundant Gateway ☐ OFF

Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!

5) Следующим шагом активируем сервер: VPN > L2TP VPN> L2TP Server

IPSec VPN Policies Tunnel Mode DHCP Range Certificates Easy VPN Setup One To One Mapping	PPTP VPN PPTP Server PPTP Client PPTP Active Users	L2TP VPN L2TP Server L2TP Client L2TP Active Users	SSL VPN SSL VPN Server Policy Portal Layouts Resources SSL VPN Client Client Routes	OpenVPN OpenVPN Settings Local Networks Remote Networks Authentication	GRE GRE
---	--	---	---	---	-------------------

6) Далее следуем настройкам в таблице:

Enable L2TP Server: Enable IPv4

L2TP Routing Mode: Classical

Range of IP Addresses (Allocated to L2TP Clients) : Указываем диапазон раздаваемых клиентам IP адресов

Authentication Database: Local User Database (Здесь могут быть другие значения в зависимости от настроек базы Ваших пользователей)

Authentication Supported: MS-CHAPv2 (у меня на нем прекрасно пашет)

User Time-out: Вписываем время тайм-аута пользователя

Ну и жмакаем заветную **SAVE**

VPN » L2TP VPN » L2TP Server

L2TP allows an external user to connect to your router through the internet, forming a VPN. This section allows you to enable/disable L2TP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.).

L2TP Server

Server Setup

Enable L2TP Server: ☒ Enable IPv4

L2TP Routing Mode: ☐ Nat ☒ Classical

Range of IP Addresses (Allocated to L2TP Clients)

Starting IP Address: 192.168.11.1

Ending IP Address: 192.168.11.10

Authentication Database

Authentication: Local User Database

Authentication Supported

PAP: ☐ OFF

CHAP: ☐ OFF

MS-CHAP: ☐ OFF

MS-CHAPv2: ☒ ON

Encryption

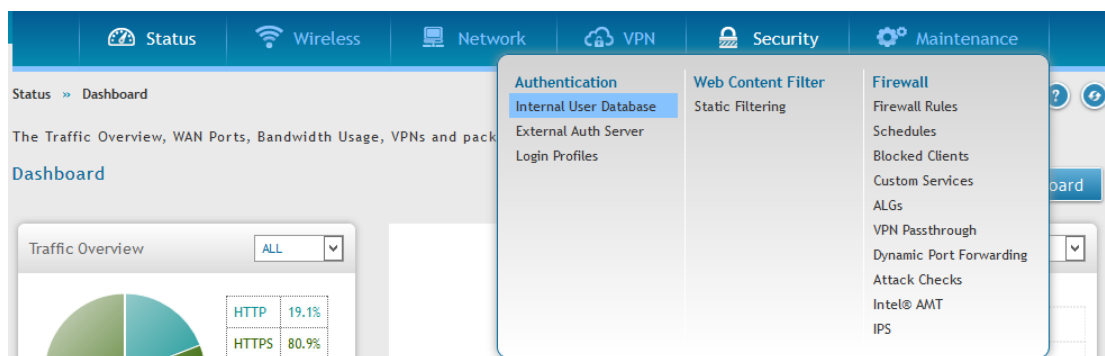
Secret Key: ☐ OFF

User Time-out

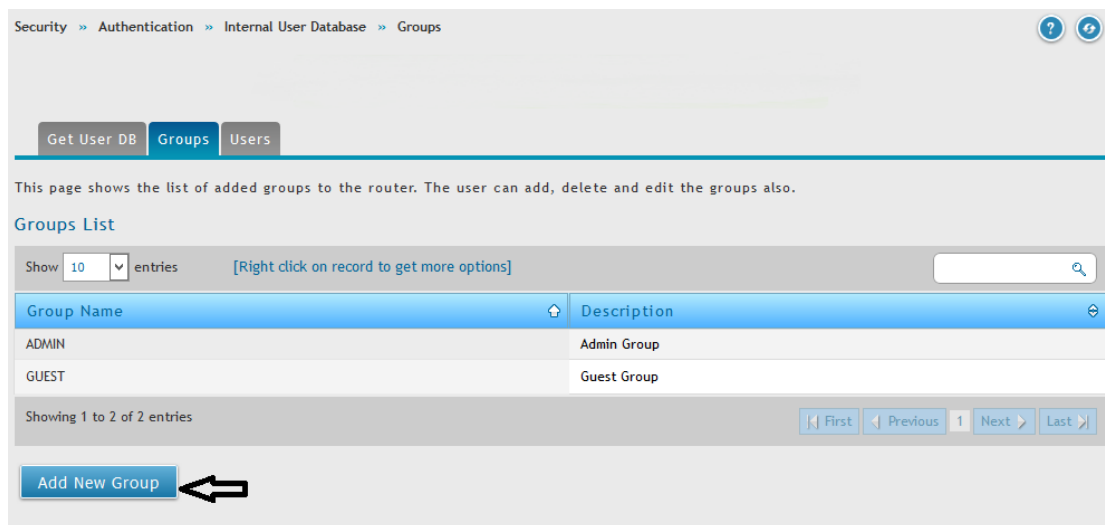
Idle TimeOut: 300 [Range: 300 - 1800] Seconds

7) Переходим с созданию пользователей для нашего сервера: Security> Internal User Database

Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!



8) Создаем сначала группу пользователей для нашего сервера: Groups> Add New Group



9) Заполняем таблицу:

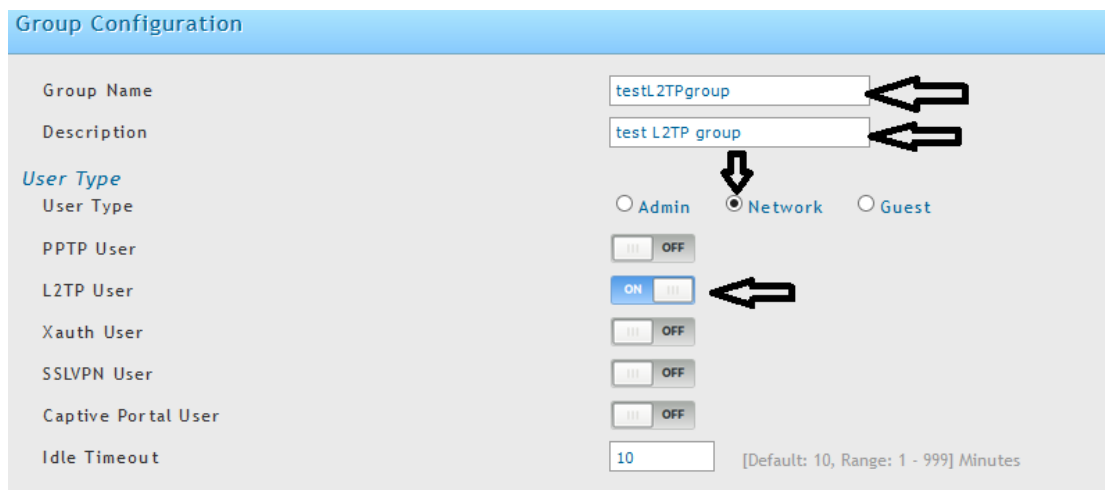
Group Name: *Произвольное значение (testL2TPgroup)

Description: *Произвольное значение (test L2TP group)

User Type: Network

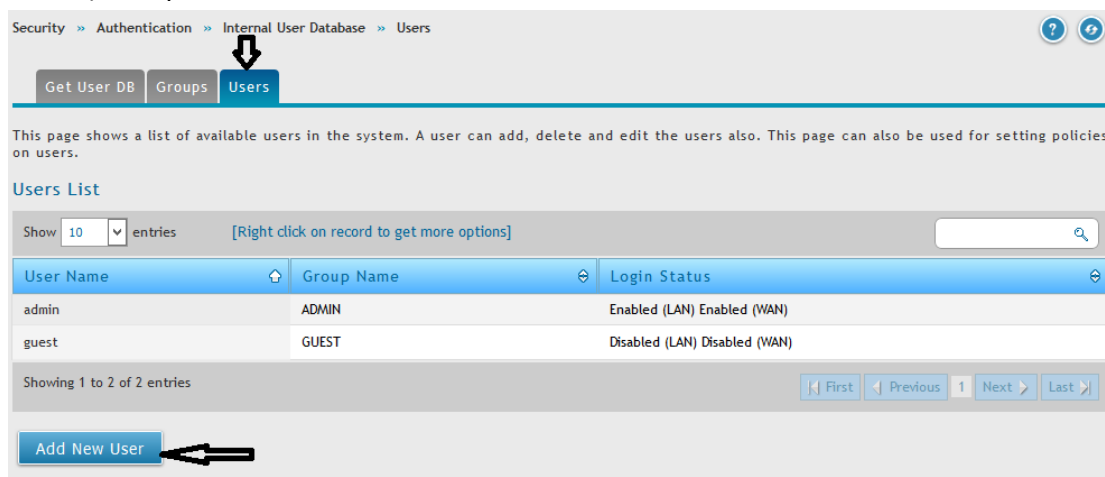
L2TP User: ON

SAVE



Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!

10) Теперь создаем пользователей: Users> Add New User



11) Заполняем таблицу:

User Name: *Произвольное значение (testL2TPuser)

First Name: *Произвольное значение (User)

Last Name: *Произвольное значение (L2TPtest)

Select Group: Выбираем группу созданную в пункте 9

Заполняем поля с паролем

Заветная **SAVE**



12) С настройкой сервера закончено, настраиваем клиентов, в нашем случае это Android/Windows, проверяем подключение пользователей и радуемся жизни: VPN> L2TP VPN> L2TP Active Users



Внимание! Настройки производились на прошивке с индексом WW, для пользователей с индексом RU некоторые пункты в настройке будут недоступны, т.к. урезан функционал по шифрованию!!!