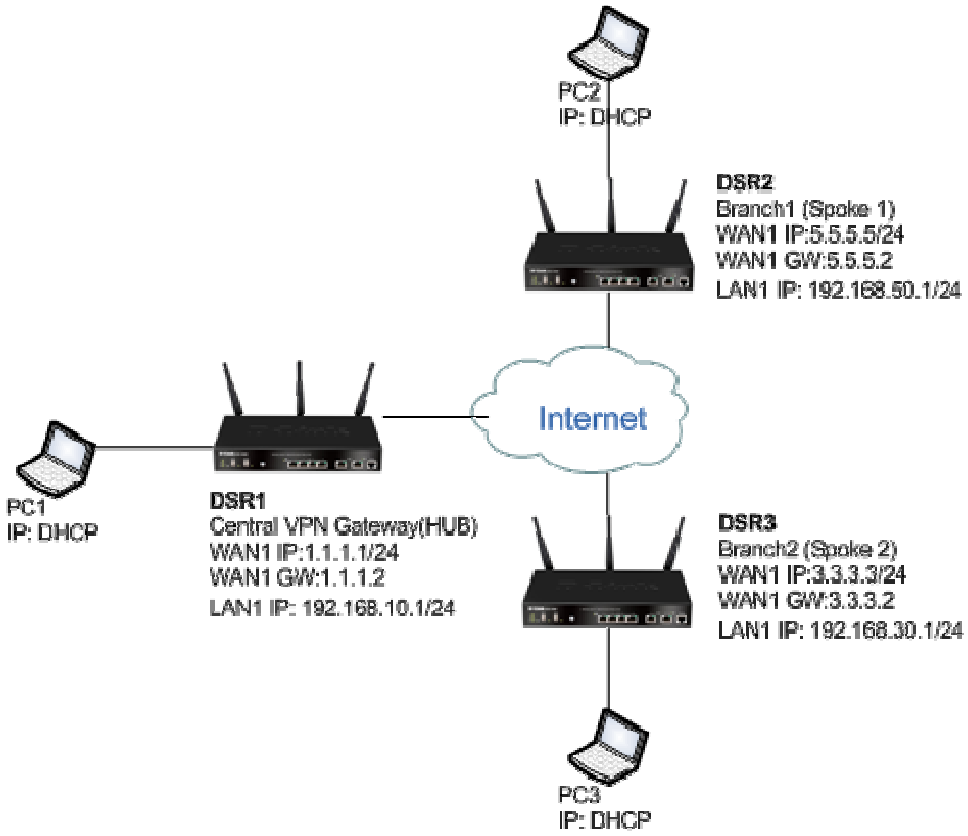
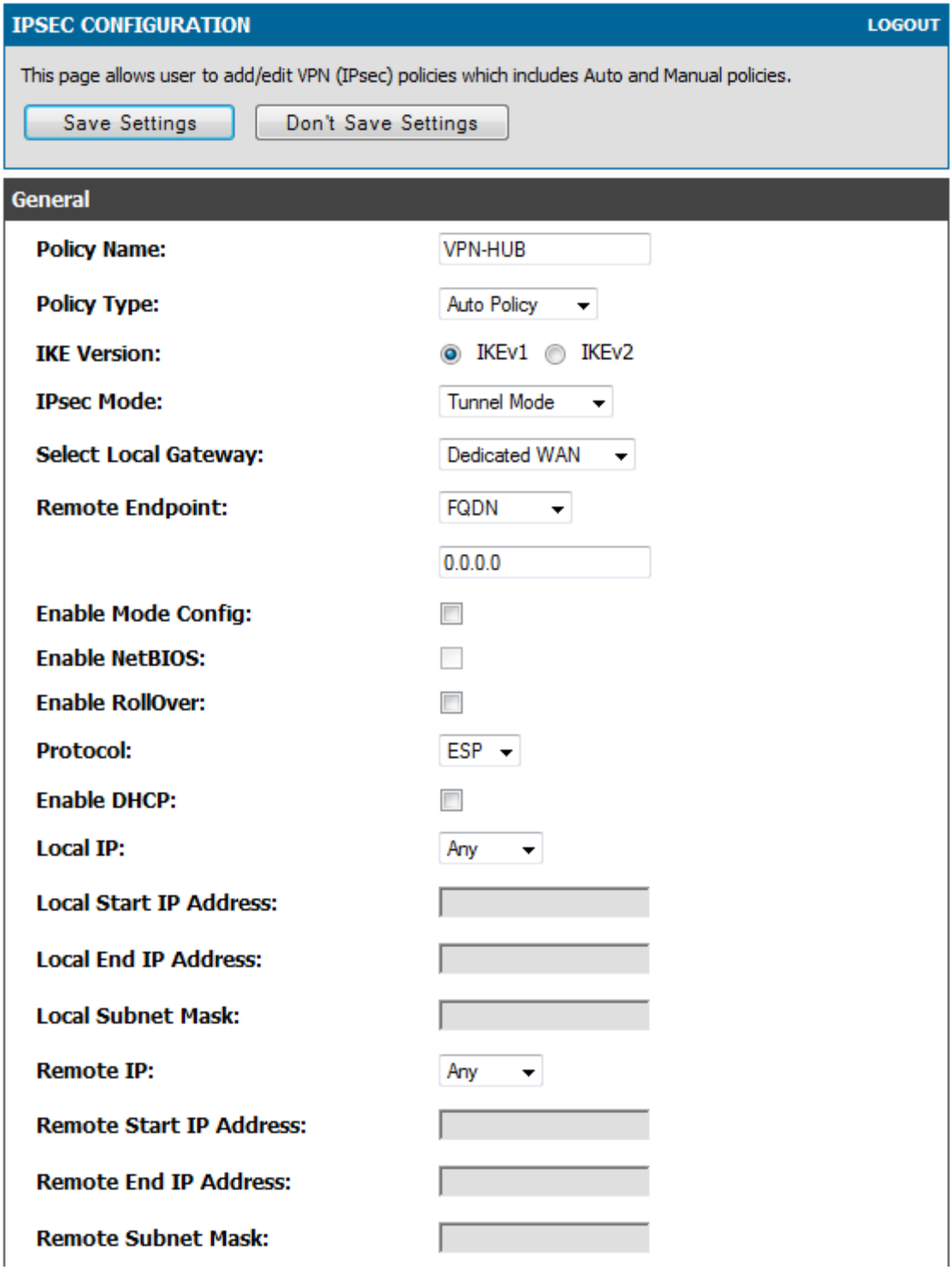
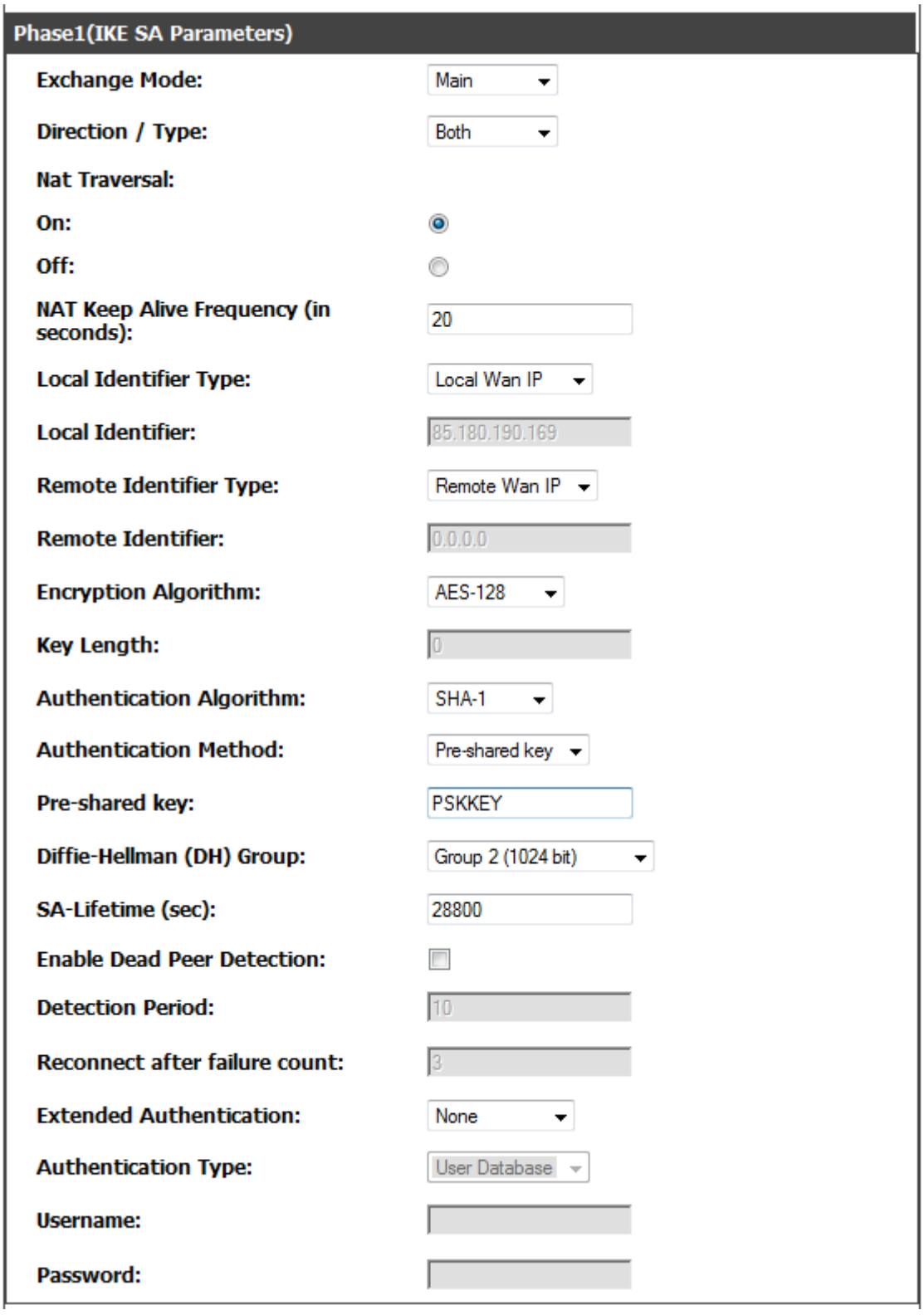
Configuring L2TP/IPSec (PSK) Client with Android/IPHONE/IPAD/Windows device

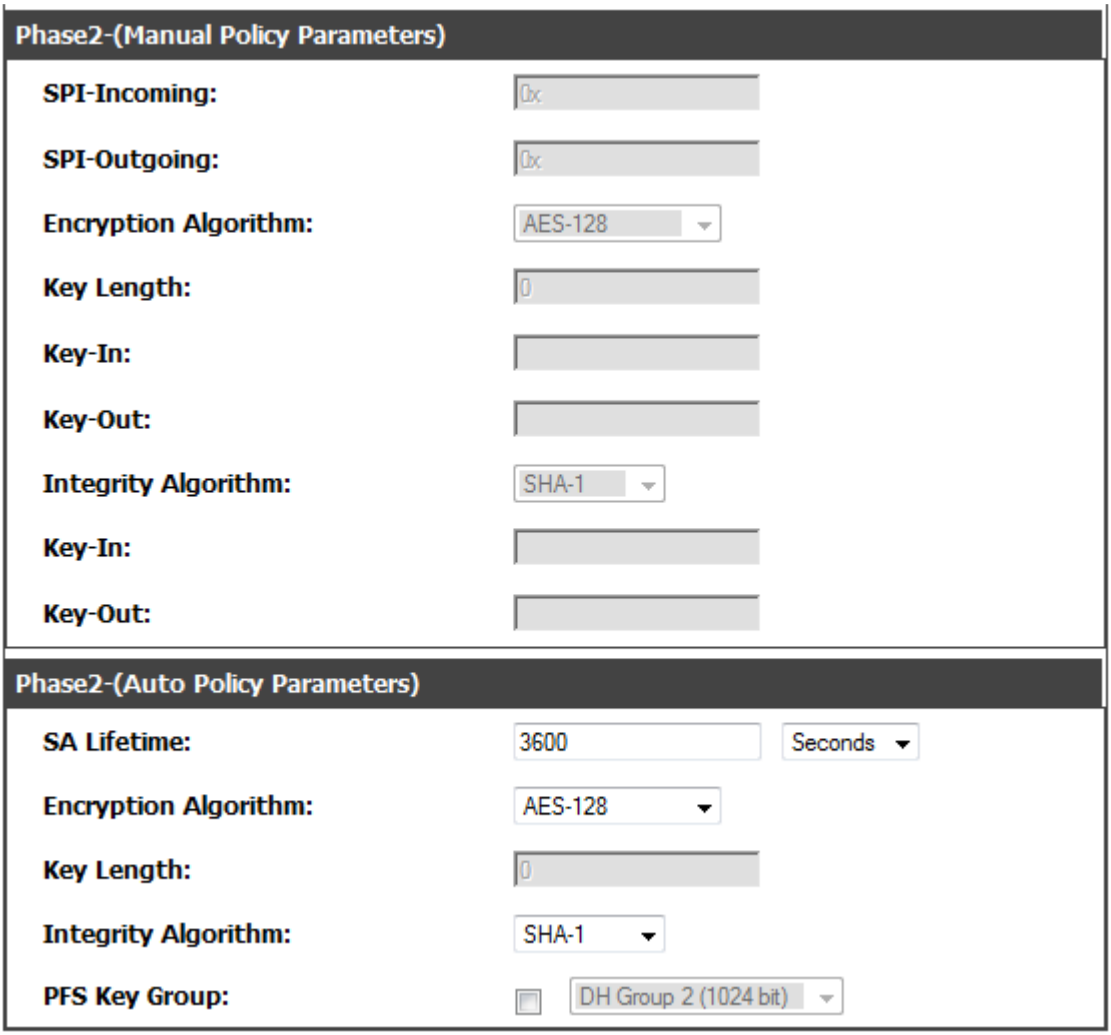


In this scenario we already have an IPSEC VPN (HUB) configured as we already use the HUB-SPOKE VPN connections.

A. IPSEV VPN Rule (for HUB only):




Phase1(IKE SA Parameters)
Exchange Mode:
Main
Direction / Type:
Both
Nat Traversal:
On:
Off:
NAT Keep Alive Frequency (in seconds):
20
Local Identifier Type:
Local Wan IP
Local Identifier:
85.180.190.169
Remote Identifier Type:
Remote Wan IP
Remote Identifier:
0.0.0.0
Encryption Algorithm:
AES-128
Key Length:
0
Authentication Algorithm:
SHA-1
Authentication Method:
Pre-shared key
Pre-shared key:
PSKKEY
Diffie-Hellman (DH) Group:
Group 2 (1024 bit)
SA-Lifetime (sec):
28800
Enable Dead Peer Detection:
Detection Period:
10
Reconnect after failure count:
3
Extended Authentication:
None
Authentication Type:
User Database
Username:
Password:

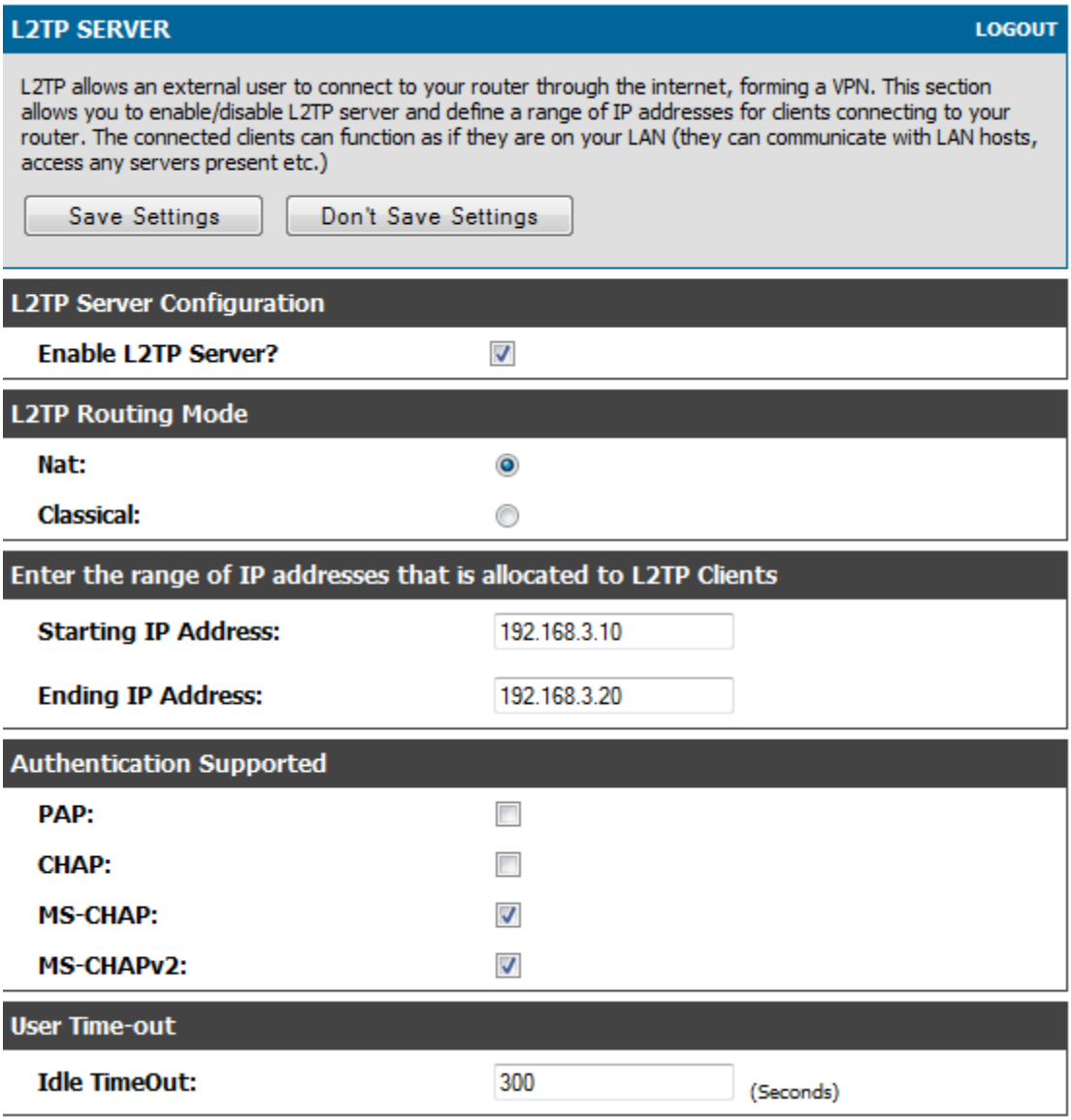


Click "Save Settings" to save your configuration.

If you want to use an IPHONE/IPAD or Windows client to connect via the L2TP/IPSEC you HAVE to change the Encryption Algorithm to 3DES.

B. Configuration to be done in DUT to support L2TP/IPSec Client:

Go to setup--> vpn settings-->L2TP server

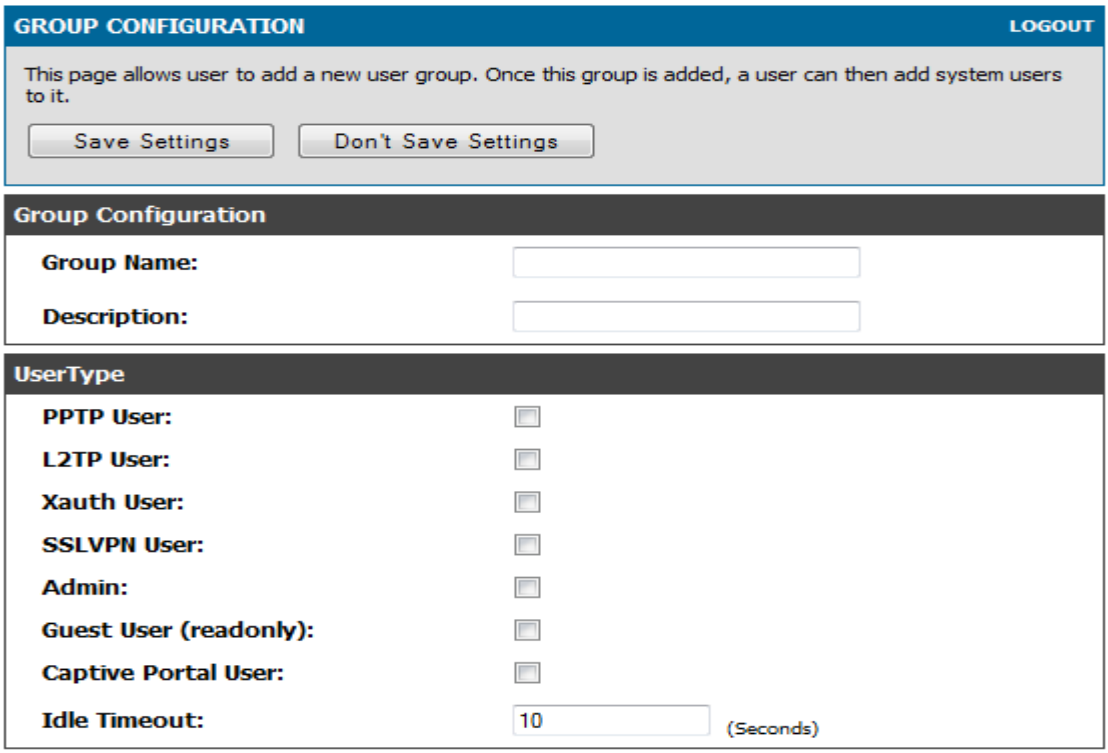


Enabled the server and configured the IP range, e.g.192.168.3.10-20 and choose the Type of routing (standard is NAT). Also choose the available Authentication Method and the user timeout. Click "Save Settings" to save your configuration.

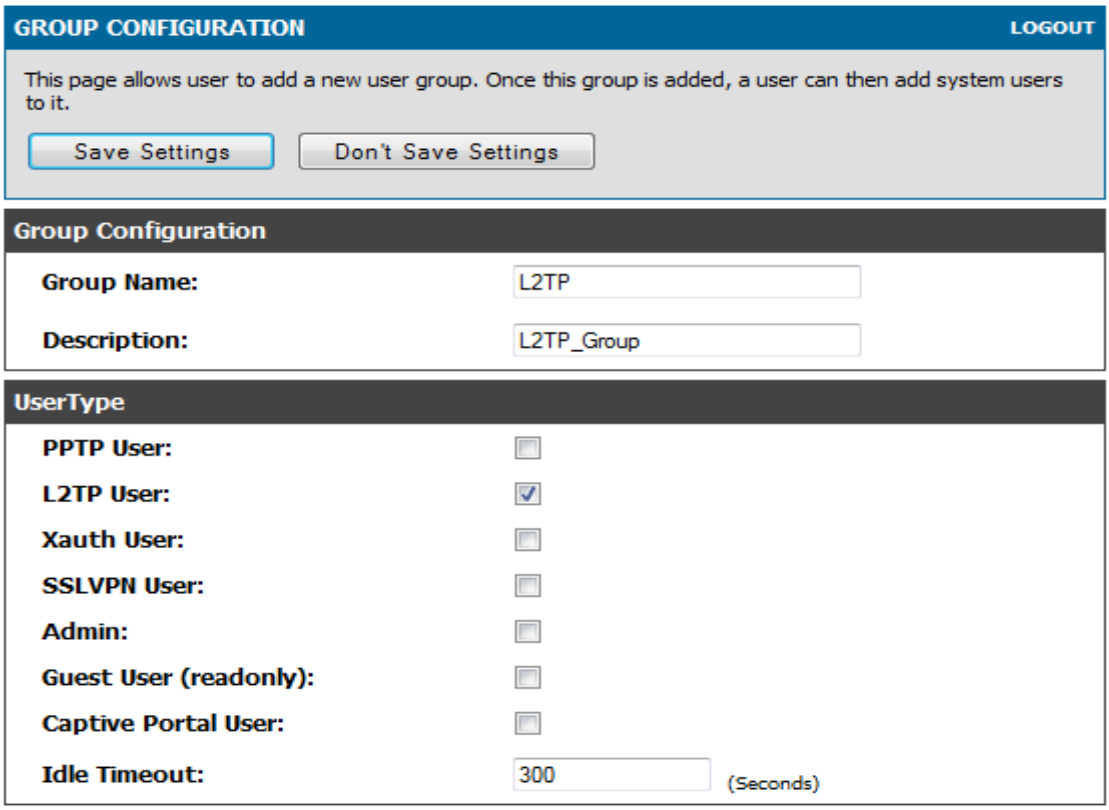
C. Creating L2TP user:

1. Go to Advanced--> Users --> Groups

There you click “ADD” to add a new User Group



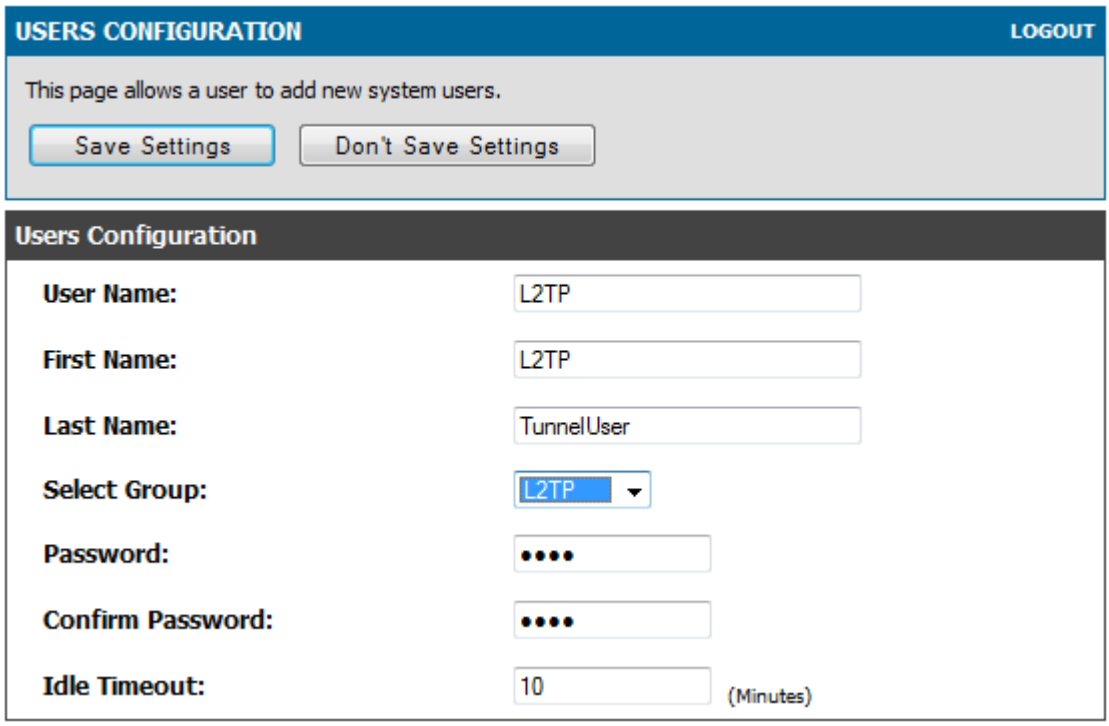
There you create a new “L2TP” user group:



Click "Save Settings" to save your configuration.

2. Go to Advanced--> Users --> Users

There you click "ADD" to add a new User



Define the "Username" *(f.e. L2TP)* and the "Password" *(f.e. L2TP)*, also you need to define the "Idle Timout" *(f.e. 10 minutes)* and which Group his user belongs to (Group means Service, *f.e. L2TP*).

Also you must define the real users First and Family name.

Click "Save Settings" to save your configuration.

D. Now go to Android device and create a L2TP/IPSec PSK-VPN adapter and configure it

1. VPN-Name: Any name
2. VPN-Server: router wan ip (if you're using dyndns you also can type the dyndns address)
3. IPsec Pre-shared key: pre-shared key as configure in client policy in DSR (f.e. PSKKEY)
4. L2TP-Secret activate : uncheck

Save your configuration

5. username: username of l2tp user as configure in DSR device.
6. password: password of l2tp user as configure in DSR device.

E. Now go to IPHONE device and create a L2TP/IPSec PSK-VPN adapter and configure it

1. VPN-Name: Any name
2. VPN-Server: router wan ip (if you're using dyndns you also can type the dyndns address)
3. Account: username of l2tp user as configure in DSR device.
4. RSA-SecureID: OFF
5. Password: password of l2tp user as configure in DSR device
5. Shared Secret: pre-shared key as configure in client policy in DSR (f.e. PSKKEY)
4. All Data : ON

Save your configuration

F. Now go to Windows device and create a L2TP/IPSec PSK-VPN adapter and configure it

1. VPN-Name: Any name
2. VPN-Server: router wan ip (if you're using dyndns you also can type the dyndns address)
3. Account: username of l2tp user as configure in DSR device.
4. Password: password of l2tp user as configure in DSR device
5. VPN-Type: choose L2TP/IPSEC
6. Advanced settings: Shared Secret, pre-shared key as configure in client policy in DSR (f.e. PSKKEY)

Save your configuration