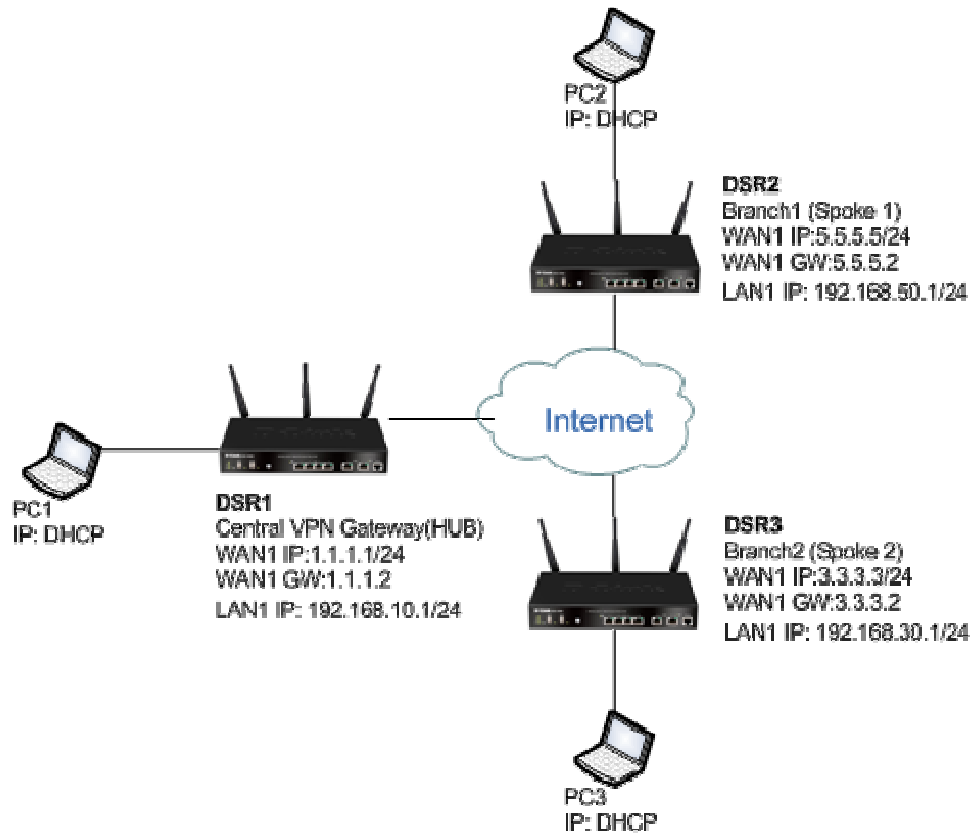


## Configuring L2TP/IPSec (PSK) Client with Android/IPHONE/IPAD/Windows device



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):

IPSEC CONFIGURATION		LOGOUT
This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.		
<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>		
<b>General</b>		
<b>Policy Name:</b>	<input type="text" value="VPN-HUB"/>	
<b>Policy Type:</b>	<input type="text" value="Auto Policy"/>	
<b>IKE Version:</b>	<input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2	
<b>IPsec Mode:</b>	<input type="text" value="Tunnel Mode"/>	
<b>Select Local Gateway:</b>	<input type="text" value="Dedicated WAN"/>	
<b>Remote Endpoint:</b>	<input type="text" value="FQDN"/>	
	<input type="text" value="0.0.0.0"/>	
<b>Enable Mode Config:</b>	<input type="checkbox"/>	
<b>Enable NetBIOS:</b>	<input type="checkbox"/>	
<b>Enable RollOver:</b>	<input type="checkbox"/>	
<b>Protocol:</b>	<input type="text" value="ESP"/>	
<b>Enable DHCP:</b>	<input type="checkbox"/>	
<b>Local IP:</b>	<input type="text" value="Any"/>	
<b>Local Start IP Address:</b>	<input type="text"/>	
<b>Local End IP Address:</b>	<input type="text"/>	
<b>Local Subnet Mask:</b>	<input type="text"/>	
<b>Remote IP:</b>	<input type="text" value="Any"/>	
<b>Remote Start IP Address:</b>	<input type="text"/>	
<b>Remote End IP Address:</b>	<input type="text"/>	
<b>Remote Subnet Mask:</b>	<input type="text"/>	

**Phase1(IKE SA Parameters)**

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

Phase2-(Manual Policy Parameters)	
SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key Length:	<input type="text" value="0"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

Phase2-(Auto Policy Parameters)	
SA Lifetime:	<input type="text" value="3600"/> <input type="text" value="Seconds"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key Length:	<input type="text" value="0"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
PFS Key Group:	<input type="checkbox"/> <input type="text" value="DH Group 2 (1024 bit)"/>

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*

L2TP SERVER		LOGOUT
<p>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.)</p>		
<input type="button" value="Save Settings"/>		<input type="button" value="Don't Save Settings"/>
L2TP Server Configuration		
Enable L2TP Server?	<input checked="" type="checkbox"/>	
L2TP Routing Mode		
Nat:	<input checked="" type="radio"/>	
Classical:	<input type="radio"/>	
Enter the range of IP addresses that is allocated to L2TP Clients		
Starting IP Address:	<input type="text" value="192.168.3.10"/>	
Ending IP Address:	<input type="text" value="192.168.3.20"/>	
Authentication Supported		
PAP:	<input type="checkbox"/>	
CHAP:	<input type="checkbox"/>	
MS-CHAP:	<input checked="" type="checkbox"/>	
MS-CHAPv2:	<input checked="" type="checkbox"/>	
User Time-out		
Idle TimeOut:	<input type="text" value="300"/>	(Seconds)

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

GROUP CONFIGURATION		LOGOUT
This page allows user to add a new user group. Once this group is added, a user can then add system users to it.		
<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>		
Group Configuration		
Group Name:	<input type="text"/>	
Description:	<input type="text"/>	
UserType		
PPTP User:	<input type="checkbox"/>	
L2TP User:	<input type="checkbox"/>	
Xauth User:	<input type="checkbox"/>	
SSLVPN User:	<input type="checkbox"/>	
Admin:	<input type="checkbox"/>	
Guest User (readonly):	<input type="checkbox"/>	
Captive Portal User:	<input type="checkbox"/>	
Idle Timeout:	<input type="text" value="10"/>	(Seconds)

There you create a new “L2TP” user group:

GROUP CONFIGURATION		LOGOUT
This page allows user to add a new user group. Once this group is added, a user can then add system users to it.		
<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>		
Group Configuration		
Group Name:	<input type="text" value="L2TP"/>	
Description:	<input type="text" value="L2TP_Group"/>	
UserType		
PPTP User:	<input type="checkbox"/>	
L2TP User:	<input checked="" type="checkbox"/>	
Xauth User:	<input type="checkbox"/>	
SSLVPN User:	<input type="checkbox"/>	
Admin:	<input type="checkbox"/>	
Guest User (readonly):	<input type="checkbox"/>	
Captive Portal User:	<input type="checkbox"/>	
Idle Timeout:	<input type="text" value="300"/>	(Seconds)

Click "Save Settings" to save your configuration.

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

There you click "ADD" to add a new User

**USERS CONFIGURATION** LOGOUT

This page allows a user to add new system users.

---

**Users Configuration**

**User Name:**

**First Name:**

**Last Name:**

**Select Group:**  ▾

**Password:**

**Confirm Password:**

**Idle Timeout:**  (Minutes)

Define the "Username" (f.e. L2TP) and the "Password" (f.e. L2TP), also you need to define the "Idle Timeout" (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