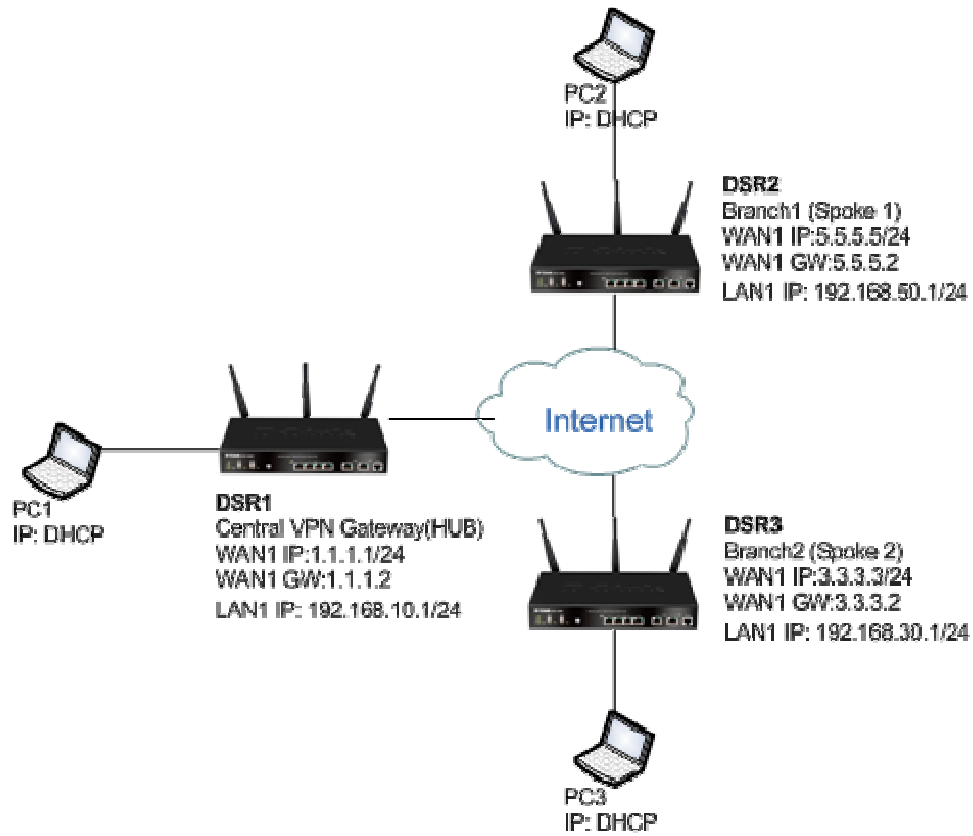


## Configuring L2TP/IPSec (PSK) Client with Android/IPHONE/IPAD/Windows device



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

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 Configuration**

Enable L2TP Server?

---

**L2TP Routing Mode**

Nat:

Classical:

---

**Enter the range of IP addresses that is allocated to L2TP Clients**

Starting IP Address:

Ending IP Address:

---

**Authentication Supported**

PAP:

CHAP:

MS-CHAP:

MS-CHAPv2:

---

**User Time-out**

Idle TimeOut:  (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"/> |
| <b>Group Configuration</b>   |                                 |  |
| <b>Group Name:</b>   | <input type="text"/>            |  |
| <b>Description:</b>  | <input type="text"/>            |  |
| <b>UserType</b>  |                                 |  |
| <b>PPTP User:</b>  | <input type="checkbox"/>        |  |
| <b>L2TP User:</b>  | <input type="checkbox"/>        |  |
| <b>Xauth User:</b>   | <input type="checkbox"/>        |  |
| <b>SSLVPN User:</b>  | <input type="checkbox"/>        |  |
| <b>Admin:</b>  | <input type="checkbox"/>        |  |
| <b>Guest User (readonly):</b>  | <input type="checkbox"/>        |  |
| <b>Captive Portal User:</b>  | <input type="checkbox"/>        |  |
| <b>Idle Timeout:</b>   | <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"/> |
| <b>Group Configuration</b>   |   |  |
| <b>Group Name:</b>   | <input type="text" value="L2TP"/>       |  |
| <b>Description:</b>  | <input type="text" value="L2TP_Group"/> |  |
| <b>UserType</b>  |   |  |
| <b>PPTP User:</b>  | <input type="checkbox"/>                |  |
| <b>L2TP User:</b>  | <input checked="" type="checkbox"/>     |  |
| <b>Xauth User:</b>   | <input type="checkbox"/>                |  |
| <b>SSLVPN User:</b>  | <input type="checkbox"/>                |  |
| <b>Admin:</b>  | <input type="checkbox"/>                |  |
| <b>Guest User (readonly):</b>  | <input type="checkbox"/>                |  |
| <b>Captive Portal User:</b>  | <input type="checkbox"/>                |  |
| <b>Idle Timeout:</b>   | <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



**UPDATE with actual Firmware 109B64 and later.**

With the latest Firmwares you need to modify the IPSEC settings according to following points to enable Client Access.

⇒ IPSEC Policy add/edit

**General Settings:**

- Name: you can choose free
- Policy Type: keep Auto Policy
- L2TP Mode: set to Gateway
- Remote Endpoint : choose FQDN (full qualified domain name)
  - add in the field "0.0.0.0"

The screenshot shows the 'General' settings for an IPSEC Policy. The fields are as follows:

|                              |  |
|------------------------------|--|
| <b>Policy Name:</b>          | ipsechub   |
| <b>Policy Type:</b>          | Auto Policy  |
| <b>IP Protocol Version:</b>  | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6   |
| <b>IKE Version:</b>          | <input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2 |
| <b>L2TP Mode:</b>            | Gateway  |
| <b>IPsec Mode:</b>           | Transport Mode   |
| <b>Select Local Gateway:</b> | Dedicated WAN  |
| <b>Remote Endpoint:</b>      | FQDN<br>0.0.0.0  |

The 'L2TP Mode' dropdown and the 'Remote Endpoint' dropdown and text input are circled in red in the original image.

PHASE 1 Settings:

- change Remote Identifier Type to "FQDN"
- change Remote to "0.0.0.0"
- change Encryption Algorithm to:
  - 3DES = Windows Clients/ iOS clients
  - AES128 = Android Clients

**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>                      | 192.168.10.207                      |
| <b>Remote Identifier Type:</b>                | FQDN                                |
| <b>Remote Identifier:</b>                     | 0.0.0.0                             |
| <b>Encryption Algorithm:</b>                  |                                     |
| <b>DES:</b>                                   | <input type="checkbox"/>            |
| <b>3DES:</b>                                  | <input checked="" type="checkbox"/> |
| <b>AES-128:</b>                               | <input checked="" type="checkbox"/> |

- change "Integrity Algorithm" to:
  - SHA-1 for most common clients
- change Authentication method to:
  - PSK(pre-shared key)
  - Add the Pre-shared Key you want to use for authentication

|                                    |                                     |
|------------------------------------|-------------------------------------|
| <b>AES-128:</b>                    | <input checked="" type="checkbox"/> |
| <b>AES-192:</b>                    | <input type="checkbox"/>            |
| <b>AES-256:</b>                    | <input type="checkbox"/>            |
| <b>BLOWFISH:</b>                   | <input type="checkbox"/> [ ]        |
| <b>CAST128:</b>                    | <input type="checkbox"/> [ ]        |
| <b>Integrity Algorithm:</b>        |                                     |
| <b>MD5:</b>                        | <input type="checkbox"/>            |
| <b>SHA-1:</b>                      | <input checked="" type="checkbox"/> |
| <b>SHA2-256:</b>                   | <input type="checkbox"/>            |
| <b>SHA2-384:</b>                   | <input type="checkbox"/>            |
| <b>SHA2-512:</b>                   | <input type="checkbox"/>            |
| <b>Authentication Method:</b>      | Pre-shared key                      |
| <b>Pre-shared Key:</b>             | 1234567890                          |
| <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"/>            |

PHASE 2 Settings:

- change Encryption Algorithm to:
  - 3DES = Windows Clients/ iOS clients
  - AES128 = Android Clients
- change "Integrity Algorithm" to:
  - SHA-1 for most common clients

**Phase2-(Auto Policy Parameters)**

|                              |                                     |                         |
|------------------------------|-------------------------------------|-------------------------|
| <b>SA Lifetime:</b>          | <input type="text" value="3600"/>   | seconds ▾               |
| <b>Encryption Algorithm:</b> |                                     |                         |
| DES:                         | <input type="checkbox"/>            |                         |
| NONE:                        | <input type="checkbox"/>            |                         |
| 3DES:                        | <input checked="" type="checkbox"/> |                         |
| AES-128:                     | <input checked="" type="checkbox"/> |                         |
| AES-192:                     | <input type="checkbox"/>            |                         |
| AES-256:                     | <input type="checkbox"/>            |                         |
| TWOFISH (128):               | <input type="checkbox"/>            |                         |
| TWOFISH (192):               | <input type="checkbox"/>            |                         |
| TWOFISH (256):               | <input type="checkbox"/>            |                         |
| BLOWFISH:                    | <input type="checkbox"/>            | <input type="text"/>    |
| CAST128:                     | <input type="checkbox"/>            | <input type="text"/>    |
| <b>Integrity Algorithm:</b>  |                                     |                         |
| MD5:                         | <input type="checkbox"/>            |                         |
| SHA-1:                       | <input checked="" type="checkbox"/> |                         |
| SHA2-224:                    | <input type="checkbox"/>            |                         |
| SHA2-256:                    | <input type="checkbox"/>            |                         |
| SHA2-384:                    | <input type="checkbox"/>            |                         |
| SHA2-512:                    | <input type="checkbox"/>            |                         |
| <b>PFS Key Group:</b>        | <input type="checkbox"/>            | DH Group 2 (1024 bit) ▾ |

L2TP Server Settings could look like following screenshot:

- change "Starting IP Address" to the IP Address you want
- change "Ending IP Address" to the IP Address you want
  - **the largest IP Range currently supported is .1 - .26 (as displayed in screenshot below)**
- change "Authentication Supported" to the Method your clients support
  - MS-CHAPv2 most secure and most clients support this

| L2TP Server Configuration   |  |
|---|--|
| L2TP Server Mode:   | Enable IPv4 ▾                            |
| L2TP Routing Mode   |  |
| NAT:  | <input type="radio"/>                    |
| Classical:  | <input checked="" type="radio"/>         |
| Enter the range of IP addresses that is allocated to L2TP Clients |  |
| Starting IP Address:  | <input type="text" value="20.20.30.1"/>  |
| Ending IP Address:  | <input type="text" value="20.20.30.26"/> |
| IPv6 Prefix   |  |
| IPv6 Prefix:  | <input type="text"/>                     |
| IPv6 Prefix Length:   | <input type="text"/>                     |
| Authentication Database   |  |
| Authentication:   | Local User Database ▾                    |
| Authentication Supported  |  |
| PAP:  | <input type="checkbox"/>                 |
| CHAP:   | <input type="checkbox"/>                 |
| MS-CHAP:  | <input type="checkbox"/>                 |
| MS-CHAPv2:  | <input checked="" type="checkbox"/>      |