

# Setting up L2TP Over IPSec Server for remote access to LAN

Remote clients: Android 5.0, iOS v10.3, Mac OS v10.12.2 and Windows 7.

**Step 1.** Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is “admin” and password is “admin”.

**Step 2.** Set your firewall’s WAN settings as per Internet provider requirements.

In our example WAN is set to PPPoE.

**Step 3.** Add a new object into the Address Book: “L2TP\_Over\_IPSec\_Pool”.

Specify the range of IP addresses which will be assigned to the clients connecting via L2TP.

These addresses should be from the IP subnet used on your LAN. Make sure this range does not conflict with the range used by the DHCP Server on your LAN.

The screenshot shows the configuration page for the object "L2TP\_Over\_IPSec\_Pool". The breadcrumb trail is "Objects » General » Address Book » InterfaceAddresses » L2TP\_Over\_IPSec\_Pool". The main heading is "L2TP\_Over\_IPSec\_Pool" in orange. Below it, a note says "Use an IP4 Address item to define a name for a specific IP4 host, network or range." There are two tabs: "General" (selected) and "User Authentication". Under the "General" tab, the "Name" field contains "L2TP\_Over\_IPSec\_Pool" and the "Address" field contains "192.168.10.150-192.168.10.160". There is an empty "Comments" text area. An "OK" button is at the bottom right.

**Step 4.** Add a new object into the Address Book: “L2TP\_Over\_IPSec\_Server”. This address should be unique and from the IP subnet used on your LAN.

The screenshot shows the configuration page for the object "L2TP\_Over\_IPSec\_Server". The breadcrumb trail is "Objects » General » Address Book » InterfaceAddresses » L2TP\_Over\_IPSec\_Server". The main heading is "L2TP\_Over\_IPSec\_Server" in orange. Below it, a note says "Use an IP4 Address item to define a name for a specific IP4 host, network or range." There are two tabs: "General" (selected) and "User Authentication". Under the "General" tab, the "Name" field contains "L2TP\_Over\_IPSec\_Server" and the "Address" field contains "192.168.10.200". There is an empty "Comments" text area. An "OK" button is at the bottom right.

**Step 5.** Go to Object->Key Ring.

Add a Pre-Shared Key.

Enter a name e.g. "L2TP\_PSK".

Shared Secret Type – set as Passphrase then enter the shared secret.

**D-Link**

Status System **Objects** Network Policies

General  
Address Book  
Services  
ALG  
**Key Ring**

Address Pool  
IP Pools  
NAT Pools

VPN Objects  
LDAP  
IKE Config Mode Pool  
IKE ID Lists  
IKE Algorithms  
IPsec Algorithms  
CRL Distribution Point Lists

### Pre-Shared Key

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name:

Shared Secret

Type:

Shared Secret:

Confirm Secret:

! A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while this OS uses UTF-8.  
! Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments:

OK Cancel

**D-Link**

Status System **Objects** Network Policies

General  
Address Book  
Services  
ALG  
**Key Ring**

Address Pool  
IP Pools  
NAT Pools

VPN Objects  
LDAP  
IKE Config Mode Pool  
IKE ID Lists  
IKE Algorithms  
IPsec Algorithms  
CRL Distribution Point Lists

Objects » General » Key Ring

### Key Ring

+ Add

#	Name	Type	Type
1	auth_agent_psk	Pre-Shared Key	Hexadecimal key
2	HTTPSAdminCert	Certificate	Local
3	L2TP_PSK	Pre-Shared Key	Passphrase

**Step 6.** Go to Network->Interfaces and VPN->VPN and Tunnels->IPSec then add an IPSec Tunnel.

Name – Enter a name e.g. “L2TP\_IPSec\_Interface”.

IKE Version – set as IKEv1.

Encapsulation Mode – set as Transport.

The screenshot shows the configuration page for 'L2TP\_IPSec\_Interface' in the 'Network' section. The left sidebar lists various network services, with 'VPN and Tunnels' expanded to show 'IPsec'. The main content area has tabs for 'General', 'Authentication', 'IKE (Phase-1)', 'IPsec (Phase-2)', 'Virtual Routing', and 'Advanced'. The 'General' tab is active, showing the following fields:

- Name: L2TP\_IPSec\_Interface
- IKE Version: IKEv1
- Encapsulation Mode: Transport
- IKE Peer section with Remote Endpoint: (None)
- Comments: (empty text box)
- OK and Cancel buttons at the bottom right.

**Step 6.1.** Under Authentication Tab, select Pre-Shared Key in the Authentication Method and L2TP\_PSK that you add in **Step 5**.

The screenshot shows the configuration page for 'L2TP\_IPSec\_Interface' in the 'Network' section, with the 'Authentication' tab selected. The left sidebar is the same as in the previous screenshot. The main content area shows the following configuration for the Authentication tab:

- Authentication Method: Pre-shared Key
- Pre-Shared Key section with Pre-shared key: L2TP\_PSK
- Authenticated Identities section with Local ID: (empty text box), Remote ID: (None), and Enforce local ID: (unchecked checkbox)

## Step 6.2. Under IKE (Phase-1) and IPsec (Phase-2) tabs, select Deprecated Medium as Algorithm.

- ▼ Link Layer
  - Ethernet
  - Link Aggregation
  - VLAN
  - PPPoE
  - ARP/Neighbor Discovery
- ▼ VPN and Tunnels
  - IPsec**
  - SSL
  - PPTP/L2TP Servers
  - L2TPv3 Servers
  - PPTP/L2TP Clients
  - L2TPv3 Clients
  - GRE
  - 6in4
- ▼ Miscellaneous
  - Loopback
  - Switch Management
  - Interface Groups

Copyright © D-Link

Network » Interfaces and VPN » VPN and Tunnels » IPsec » L2TP\_IPSec\_Interface

### L2TP\_IPSec\_Interface

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General
Authentication
IKE (Phase-1)
IPsec (Phase-2)
Virtual Routing
Advanced

Proposal

Diffie-Hellman group:

Available	Selected
01 (768-bit) 05 (1536-bit) 14 (2048-bit) 15 (3072-bit) 16 (4096-bit) 17 (6144-bit) 18 (8192-bit)	02 (1024-bit)

Algorithms: Deprecated-Med

Lifetime:  seconds

Mode: Main mode

#### IKE Peers Settings

Outgoing Routing Table: main

Local Endpoint: (None)

Incoming Interface Filter: any

- ▼ Link Layer
  - Ethernet
  - Link Aggregation
  - VLAN
  - PPPoE
  - ARP/Neighbor Discovery
- ▼ VPN and Tunnels
  - IPsec**
  - SSL
  - PPTP/L2TP Servers
  - L2TPv3 Servers
  - PPTP/L2TP Clients
  - L2TPv3 Clients
  - GRE
  - 6in4
- ▼ Miscellaneous
  - Loopback
  - Switch Management
  - Interface Groups

Network » Interfaces and VPN » VPN and Tunnels » IPsec » L2TP\_IPSec\_Interface

### L2TP\_IPSec\_Interface

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General
Authentication
IKE (Phase-1)
IPsec (Phase-2)
Virtual Routing
Advanced

Proposal

Perfect Forward Security:

Available	Selected
14 (2048-bit) 15 (3072-bit) 16 (4096-bit) 17 (6144-bit) 18 (8192-bit)	None (No PFS) 01 (768-bit) 02 (1024-bit) 05 (1536-bit)

Algorithms: Deprecated-Med

Lifetime:  seconds

Lifetime:  kilobytes

#### Protected Networks Settings

Setup SA per: Network

Config Mode Pool: (None)

**Step 6.3.** Under Advanced tab, tick Add route dynamically. Then Press the OK button.

Network » Interfaces and VPN » VPN and Tunnels » IPsec » L2TP\_IPSec\_Interface

### L2TP\_IPSec\_Interface

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication IKE (Phase-1) IPsec (Phase-2) Virtual Routing **Advanced**

---

**Routing**

Add route dynamically:

Add route statically:

Plaintext MTU:

**Tunnel Monitor**

Tunnel Monitoring:

**IP Addresses**

Automatically pick the address of a local interface that corresponds to the local net.  
 Specify address manually:

OK Cancel

Status System Objects **Network** Policies

Interfaces and VPN Routing Network Services

Network » Interfaces and VPN » VPN and Tunnels » IPsec

### IPsec

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

+ Add Advanced Settings Fill

# ▲	Name	Local Net	Remote Net	Remote Endpoint	Local Endpoint	Auth
1	L2TP_IPSec_Interface					Pre-shared Key

**i**

**Step 7.** Go to Network->Interfaces and VPN->VPN and Tunnels->PPTP/L2TP Servers.

Add a new PPTP/L2TP Server.

Inner IP Address – set as “L2TP\_Over\_IPSec\_Server” you added in **Step 4**.

Tunnel Protocol – L2TP.

Outer Interface Filter – set as “L2TP\_IPSec\_Interface” you added in **Step 6**.

Server IP – set as inet\_ip (the PPPoE interface ip in this example).

The screenshot shows the Mikrotik WinBox configuration window for an L2TP Interface. The breadcrumb path is: Network » Interfaces and VPN » VPN and Tunnels » PPTP/L2TP Servers » L2TP\_Interface. The title is "L2TP\_Interface" and the description is "A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks." The "General" tab is selected, showing the following configuration fields:

- Name: L2TP\_Interface
- Inner IP Address: L2TP\_Over\_IPSec (dropdown menu)
- Tunnel Protocol: L2TP (dropdown menu)
- Outer Interface Filter: L2TP\_IPSec\_Inte (dropdown menu)
- Server IP: inet\_ip (dropdown menu)
- Comments: (empty text area)

At the bottom right, there are "OK" and "Cancel" buttons. The left sidebar shows the navigation tree with "PPTP/L2TP Servers" selected.

**Step 7.1.** Under PPP Parameters.

IP Pool – set as “L2TP\_Over\_IPSec\_Pool” you added in **Step 3** and set the Primary and Secondary DNS.

The screenshot shows the configuration page for 'L2TP\_Interface' under the 'Network' tab. The left sidebar contains a tree view with categories: Link Layer (Ethernet, Link Aggregation, VLAN, PPPoE, ARP/Neighbor Discovery), VPN and Tunnels (IPsec, SSL, PPTP/L2TP Servers, L2TPv3 Servers, PPTP/L2TP Clients, L2TPv3 Clients, GRE, 6in4), and Miscellaneous (Loopback, Switch Management, Interface Groups). The main content area is titled 'L2TP\_Interface' and includes a description: 'A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.' Below this are four tabs: 'General', 'PPP Parameters', 'Add Route', and 'Virtual Routing'. The 'PPP Parameters' tab is active. It contains a checkbox for 'Use User Authentication Rules' which is checked. A section for 'Microsoft Point-To-Point Encryption (MPPE)' has four checked options: 'None', 'RC4 40 bit', 'RC4 56 bit', and 'RC4 128 bit', and one unchecked option: 'Stateful MPPE (less secure, use only for compatibility)'. The 'IP Pool' section has a dropdown menu set to 'L2TP\_Over\_IPSec'. Below it are two columns for 'Primary' and 'Secondary' settings. The 'Primary' column has 'DNS' set to 'inet\_dns1' and 'NBNS/WINS' set to '(None)'. The 'Secondary' column has 'DNS' set to '8.8.8.8' and 'NBNS/WINS' set to '(None)'. At the bottom right are 'OK' and 'Cancel' buttons. A copyright notice 'Copyright © D-Link' is visible in the bottom left corner.

**Step 7.2.** Under Add Route tab.

Filter – set as “all-nets”

Proxy ARP – include “lan”

Then press OK button.

Network > Interfaces and VPN > VPN and Tunnels > PPTP/L2TP Servers > L2TP\_Interface

### L2TP\_Interface

A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.

**General** | **PPP Parameters** | **Add Route** | **Virtual Routing**

Filter

Allowed Networks:

Proxy ARP

Proxy ARP interfaces:

Available	Selected
dmz	lan
L2TP_IPSec_LAN_Group	
wan1	
wan2	

Network > Interfaces and VPN > VPN and Tunnels > PPTP/L2TP Servers

### PPTP/L2TP Servers

Add, remove and configure PPTP/L2TP (Point-to-Point Tunneling Protocol / Layer 2 Tunneling Protocol) servers used for terminating PPTP/L2TP-based VPN tunnels.

#	Name	Tunnel protocol	Inner IP address	Outer interface	IP pool	Outer server IP
1	pptp_server	PPTP	lan_ip	any	pptp_pool	liinet_ip
2	L2TP_Interface	L2TP	L2TP_Over_IPSec_Server	L2TP_IPSec_Interface	L2TP_Over_IPSec_Pool	liinet_ip

Right-click



**Step 8.** Go to Network->Interfaces and VPN->Miscellaneous->Interface Groups.  
 Add interface groups for “L2TP\_Interface” (added in **Step 7**) and “lan”

Status System Objects **Network** Policies

Interfaces and VPN Routing Network Services

▼ Link Layer  
 Ethernet  
 Link Aggregation  
 VLAN  
 PPPoE  
 ARP/Neighbor Discovery

▼ VPN and Tunnels  
 IPsec  
 SSL  
 PPTP/L2TP Servers  
 L2TPv3 Servers  
 PPTP/L2TP Clients  
 L2TPv3 Clients  
 GRE  
 6in4

▼ Miscellaneous  
 Loopback  
 Switch Management  
**Interface Groups**

### Interface Group

Use an interface group to combine several interfaces for a simplified security policy.

Name:   Security/Transport Equivalent

Interfaces

Available	Selected
core	L2TP_Interface
dmz	lan
iinet	
L2TP_IPSec_Interface	
pptp_server	
wan1	
wan2	

Comments:

Status System Objects **Network** Policies

Interfaces and VPN Routing Network Services

▼ Link Layer  
 Ethernet  
 Link Aggregation  
 VLAN  
 PPPoE  
 ARP/Neighbor Discovery

▼ VPN and Tunnels  
 IPsec  
 SSL  
 PPTP/L2TP Servers  
 L2TPv3 Servers  
 PPTP/L2TP Clients  
 L2TPv3 Clients  
 GRE  
 6in4

▼ Miscellaneous  
 Loopback  
 Switch Management  
**Interface Groups**

Network » Interfaces and VPN » Miscellaneous » Interface Groups

### Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

#	Name	Members
1	L2TP_IPSec_LAN_Group	L2TP_Interface, lan

**Step 9.** Go to Policies->Firewalling->Rules->Main IP Rules. Create a new IP Rule to allow L2TP Tunnel communication with LAN:

Set Action as "Allow".

Set Source Interface/Network as "L2TP\_IPSec\_LAN\_Group"/all-nets.

Set Destination Interface/Network as "L2TP\_IPSec\_LAN\_Group"/all-nets.

Service: all\_services.

Then press OK button.

The screenshot shows the Mikrotik WinBox interface with the 'Policies' tab selected. The breadcrumb trail is 'Policies » Firewalling » Rules » Main IP Rules » L2TP\_IPSec\_Allow'. The rule name is 'L2TP\_IPSec\_Allow' and the action is set to 'Allow'. Under the 'Address Filter' section, the source and destination are both set to 'L2TP\_IPSec\_LAN\_Group' for the interface and 'all-nets' for the network. The service is set to 'all\_services' and the schedule is '(None)'. The 'Application Control' section is currently turned 'OFF'.

The screenshot shows the 'Main IP Rules' configuration page in WinBox. It includes a '+ Add' button and a table listing existing rules. The table has columns for #, Name, Log, Src If, Src Net, Dest If, Dest Net, and Service.

#	Name	Log	Src If	Src Net	Dest If	Dest Net	Service
1	L2TP_IPSec_Allow	✓	L2TP_IPSec_LAN_Group	all-nets	L2TP_IPSec_LAN_Group	all-nets	all_tcpudpicmp
2	ping_fw		lan	lannet	core	lan_ip	ping-inbound
3	lan_to_wan1						



**Step 10.** Go to System->Device->Users->Local User Database.

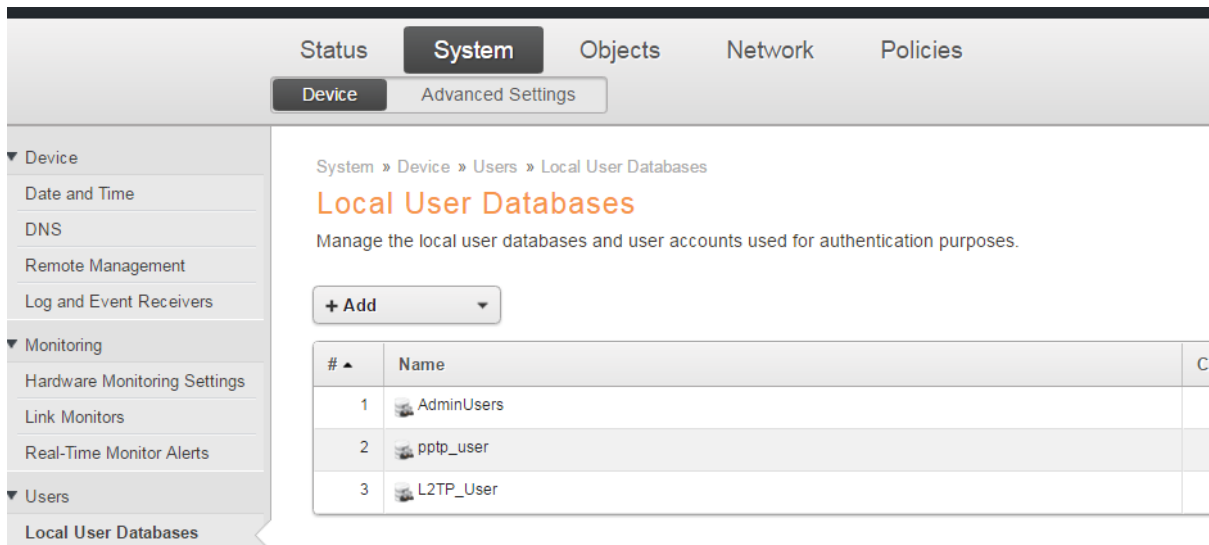
Add Local User Database.

Enter a name e.g. L2TP\_users.

The screenshot shows the 'System' tab in the configuration interface. The breadcrumb trail is 'System » Device » Users » Local User Databases » L2TP\_Users'. The page title is 'L2TP\_Users' and it includes a description: 'A local user database contains user accounts used for authentication purposes.' There are two tabs: 'General' and 'Users'. The 'General' tab is active, showing a 'Name' field with 'L2TP\_Users' and a 'Comments' text area. An 'OK' button is located at the bottom right.

**Step 10.1.** Go to Users tab then enter l2tp username and password. Then press OK button.

The screenshot shows the 'System' tab in the configuration interface. The breadcrumb trail is 'System » Device » Users » Local User Databases ». The page title is 'User' and it includes a description: 'User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, etc'. There are two tabs: 'General' and 'SSH Public Key'. The 'General' tab is active, showing a 'Name' field with 'l2tpuser', a 'Password' field with a strength indicator 'Very Weak', a 'Confirm Password' field, and a 'Groups' text area. Below the 'Groups' field, there is an information icon and text: 'Comma separated list of groups. Users that are members of the 'administrators' group are allowed to change the firewall configurator. Users that are members of the 'auditors' group are only allowed to view the firewall configurator'. There are two buttons: 'Add administrators' and 'Add auditors'. Below this, there is a section for 'Per-User IP Configuration (For PPTP, L2TP And SSL VPN)' with fields for 'Static Client IP Address', 'Networks behind user', and 'Metric for networks'. A 'Comments' field is at the bottom. The copyright notice 'Copyright © D-Link' is at the bottom left.



**Step 11.** Go to Policies->User Authentication->Rules->Authentication Rules.

Add User Authentication Rule.

Name: L2TP\_Auth.

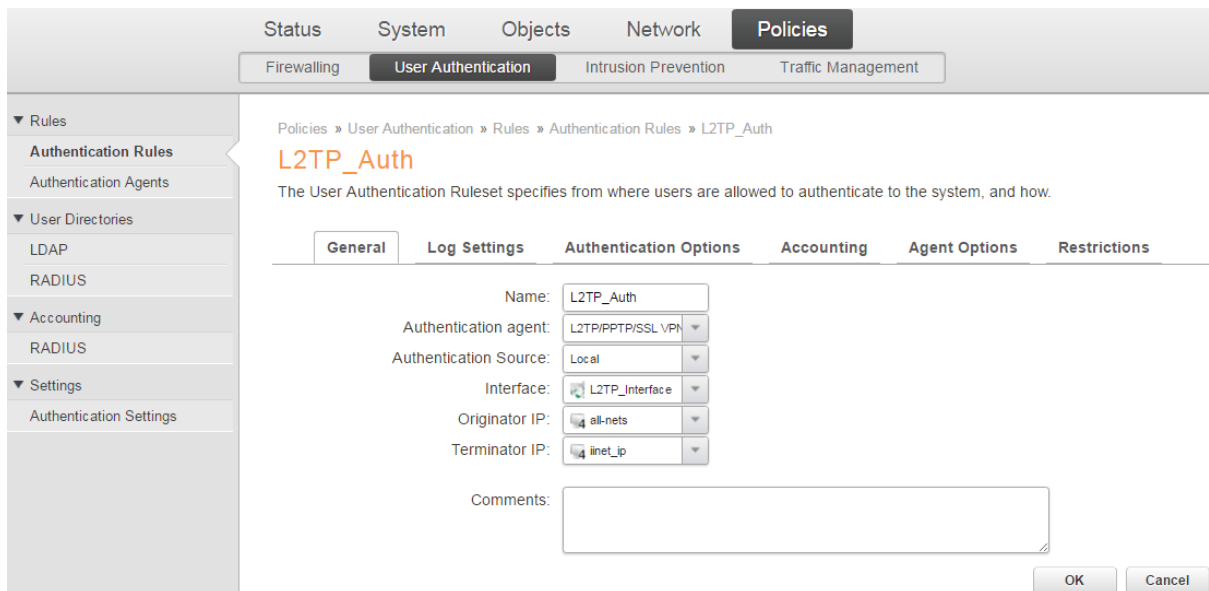
Authentication agent – set as L2TP/PPTP/SSL VPN.

Authentication Source – set as Local.

Interface – set as “L2TP\_Interface” added in **Step 7**.

Originator IP – set as “all-nets”.

Terminator IP – set as “inet\_ip” (PPPoE interface ip in this example).



**Step 11.1.** Go to Authentication Options tab, select L2TP\_user as Local User DB then press OK button.

- Rules
  - Authentication Rules**
  - Authentication Agents
- User Directories
  - LDAP
  - RADIUS
- Accounting
  - RADIUS
- Settings
  - Authentication Settings

Copyright © D-Link

Policies » User Authentication » Rules » Authentication Rules » L2TP\_Auth

## L2TP\_Auth

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

**General**   **Log Settings**   **Authentication Options**   **Accounting**   **Agent Options**   **Restrictions**

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

RADIUS servers:

Available	Selected
<div style="border: 1px solid gray; height: 50px;"></div>	<div style="border: 1px solid gray; height: 50px;"></div>
+ Include	x Remove
	⬆ ⬇

Primary Retry Interval:

LDAP servers:

Available	Selected
<div style="border: 1px solid gray; height: 50px;"></div>	<div style="border: 1px solid gray; height: 50px;"></div>
+ Include	x Remove
	⬆ ⬇

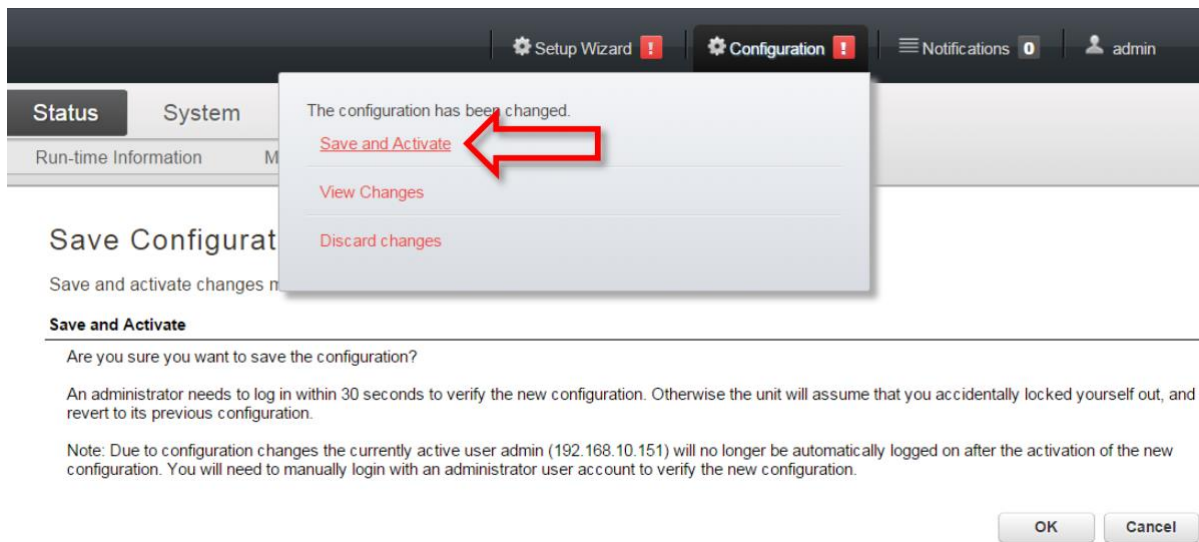
RADIUS Method:

Local User DB:

**Step 12.** After the configuration is done, click “Configuration” in main bar and select “Save and Activate”.

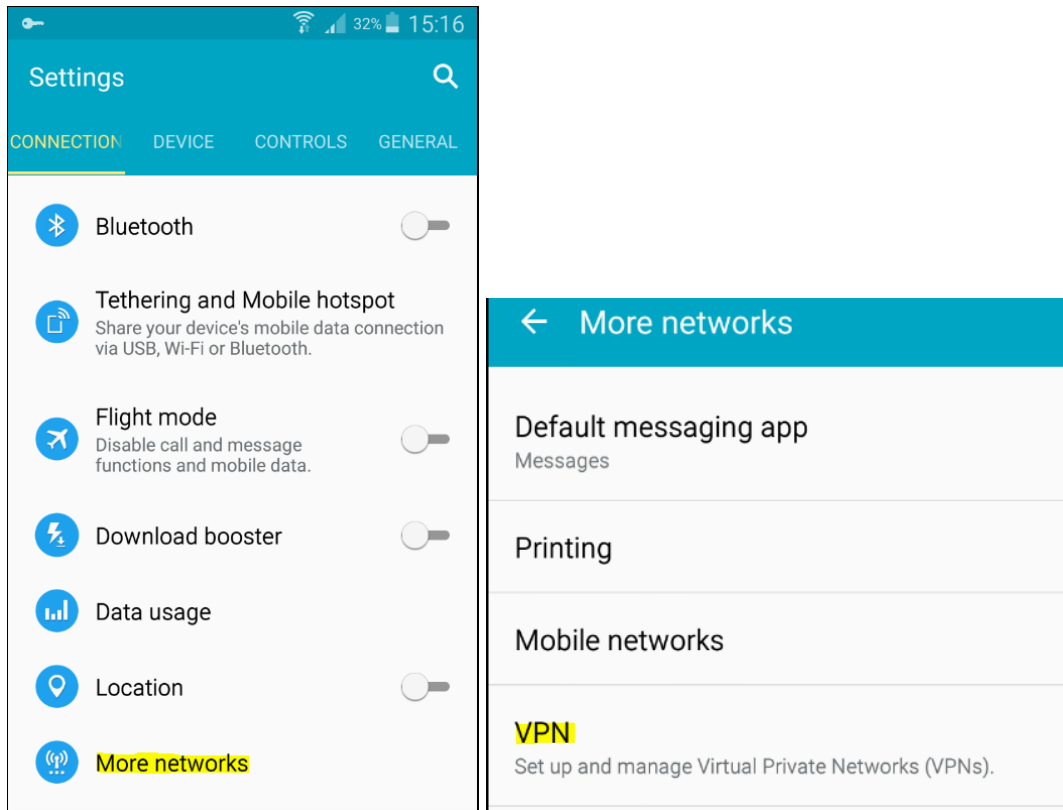
Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

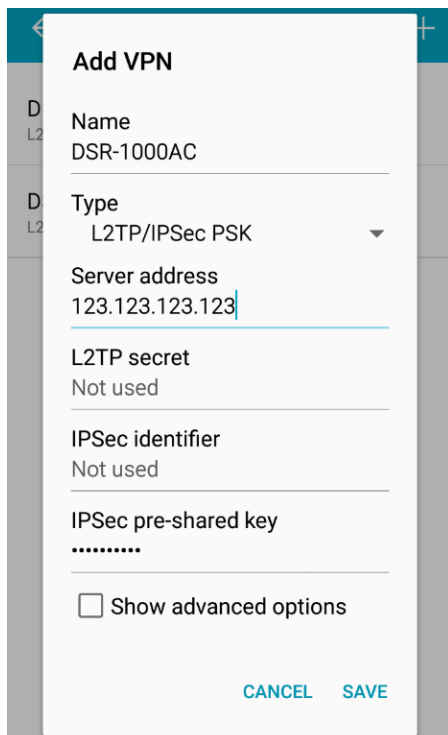


## Android 5.0 Settings.

1.0 Go to Settings->Connections->More Networks->VPN.

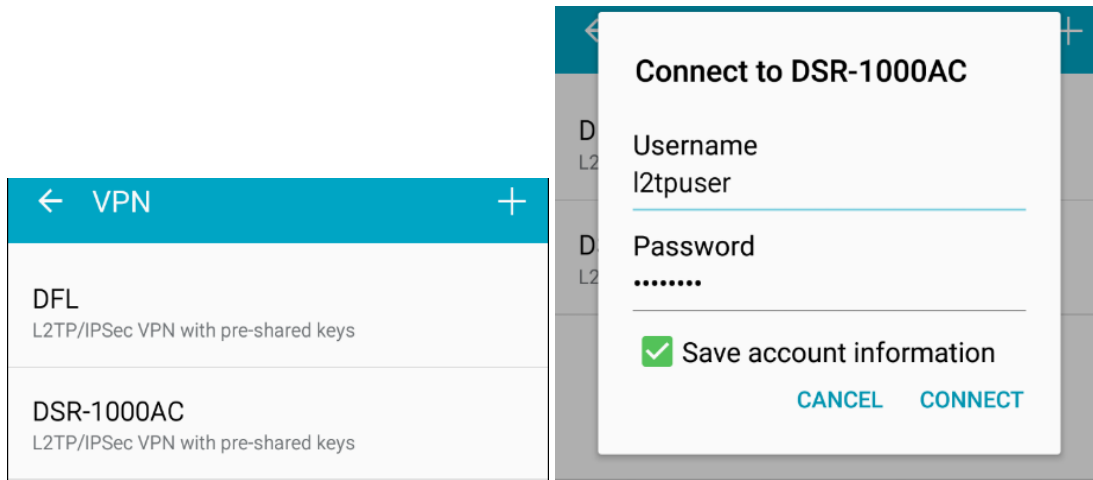


1.1 Add a new L2TP/IPSec PSK Profile and enter the L2TP server public IP address and Pre-Shared Key (entered in **Step 5**) then Save.

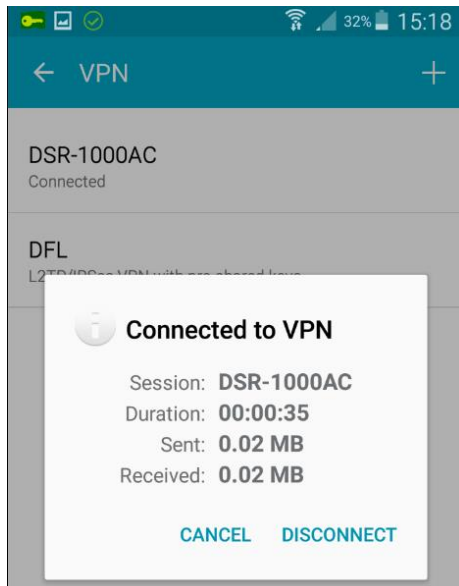




1.2 Press the L2TP/IPSec Profile you added to connect. Enter the L2TP username and password you added in **Step 10**.



You should see a Key icon on the top-left hand corner that indicates it is connected.



## IOS v10.3 (iPhone 7 Plus running ) Settings:

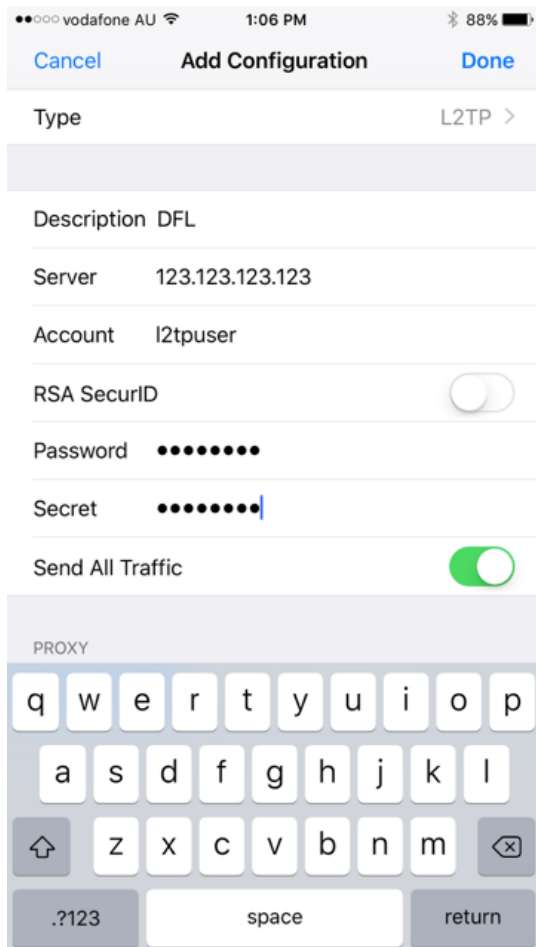
**2.0** Go to Settings->VPN->Add VPN Configuration:

Description – set as DFL.

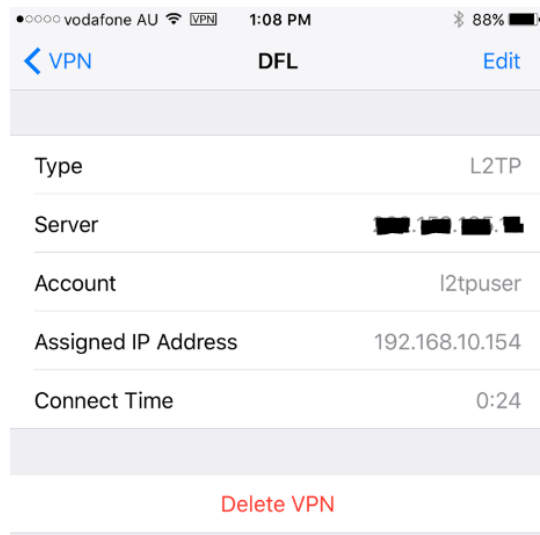
Account – enter the L2TP username added **Step 10**.

Password – enter the L2TP password added **Step 10**.

Secret – enter the shared secret in **Step 5** then click **Done**.



## 2.1 Select DFL and enable the **Status** to connect.



## MAC OS Sierra v10.12.2 Settings.

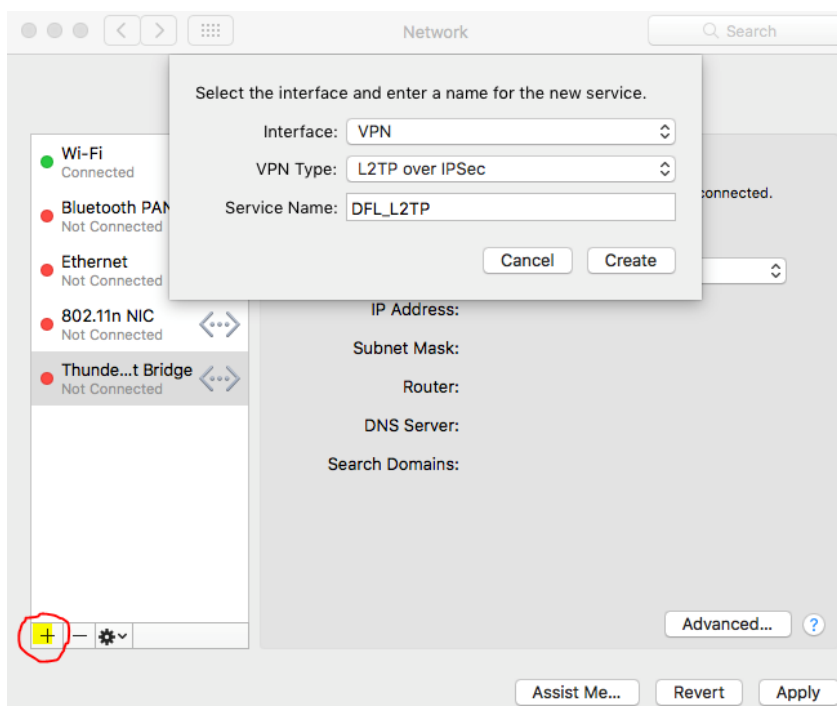


**3.0** Go to System Preferences->Network then click on the (+) sign to add a new connection.

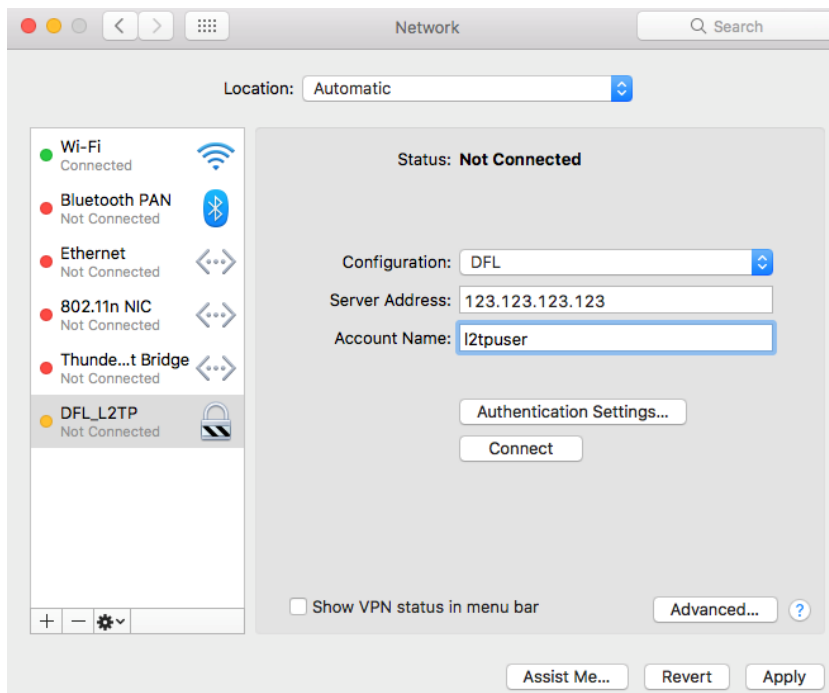
Interface – set as VPN.

VPN type – set as L2TP Over IPSec.

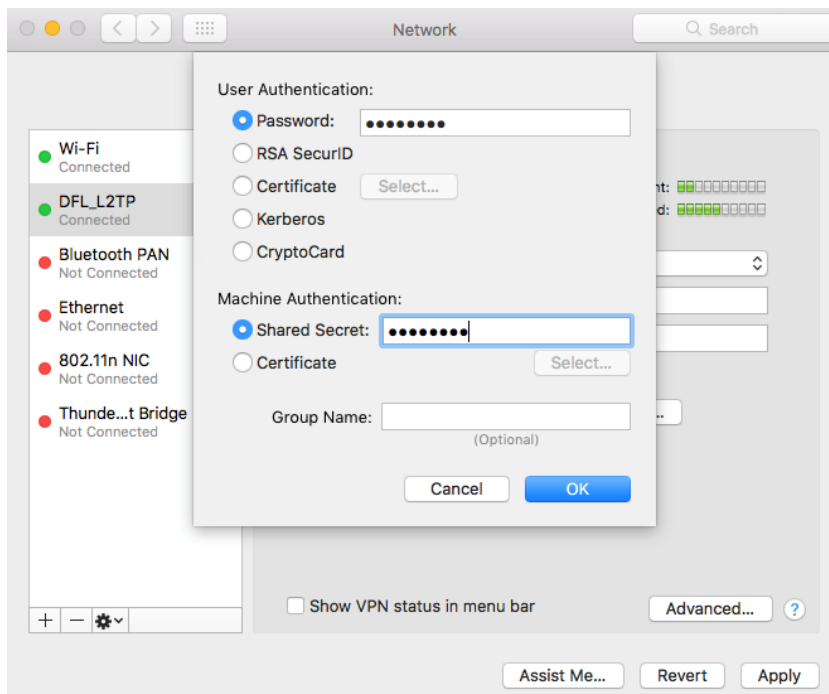
Service name – enter a name you prefer e.g. DFL\_L2TP then click Create.



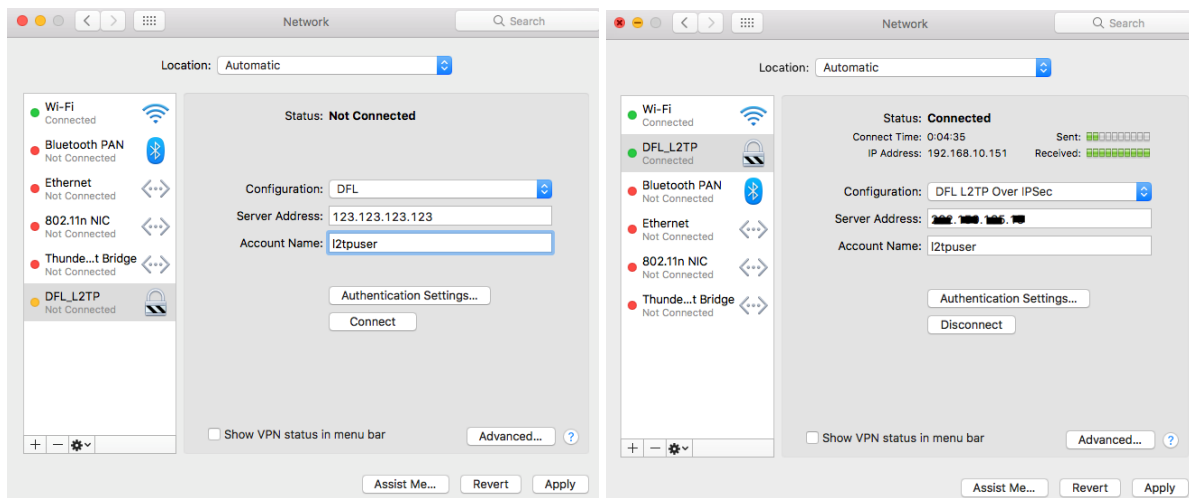
**3.1** Enter a Configuration name, Server Address and the L2TP username added in **Step 10**.



**3.2** Click on “Authentication Settings...” then enter the L2TP user password added in **Step 10** and “Shared Secret” added in **Step 5** then Press OK.

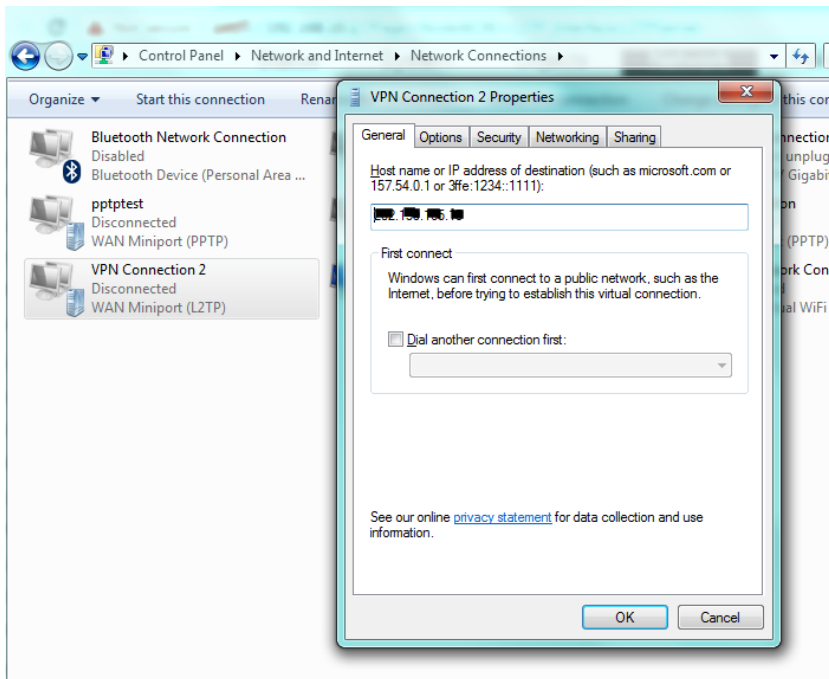


### 3.3 Click **Connect** button to established a connection.



## Windows L2TP Client Settings:

**4.0** Go to Properties of the VPN connection, enter the WAN ip address of the DFL.

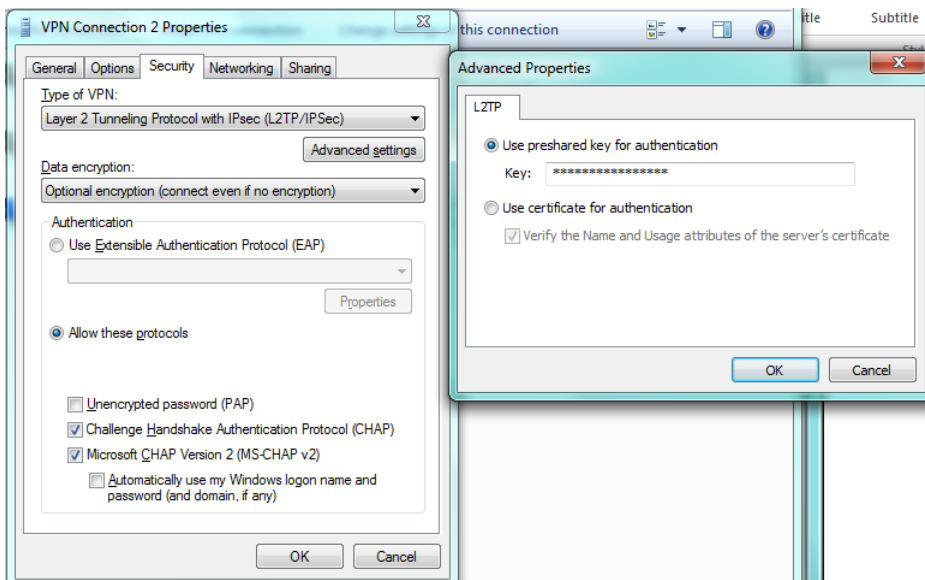


**4.1** Go to Security tab:

Type of VPN – set as L2TP/IPSec.

Data Encryption – set as Optional encryption

Click on Advanced Settings then enter the L2TP Shared key added in **Step 5**.



**4.2** Enter the L2TP username and password added in **Step 10** then click **Connect**.

