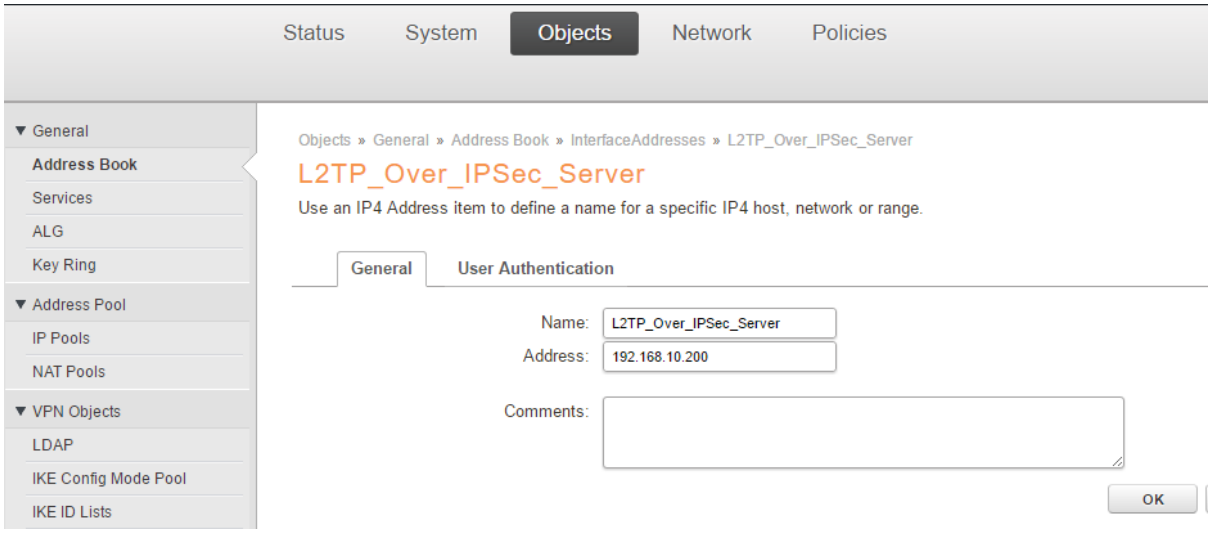
Setting up L2TP Over IPSec Server for remote access to LAN

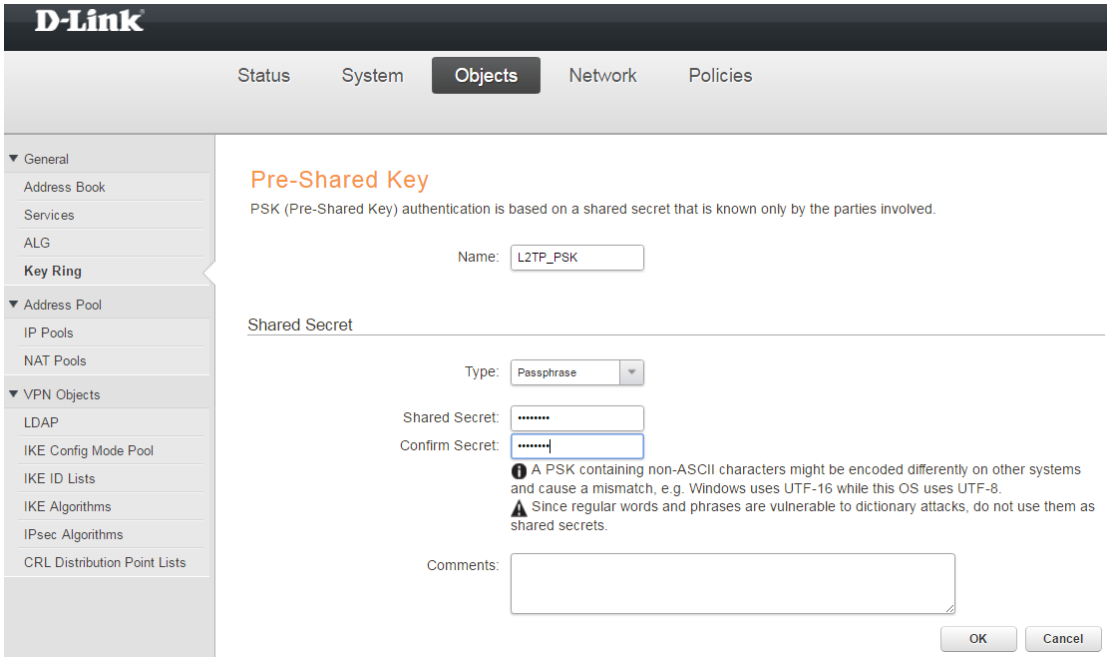
Remote clients: Android 5.0, iOS v10.3, Mac OS v10.12.2 and Windows 7.

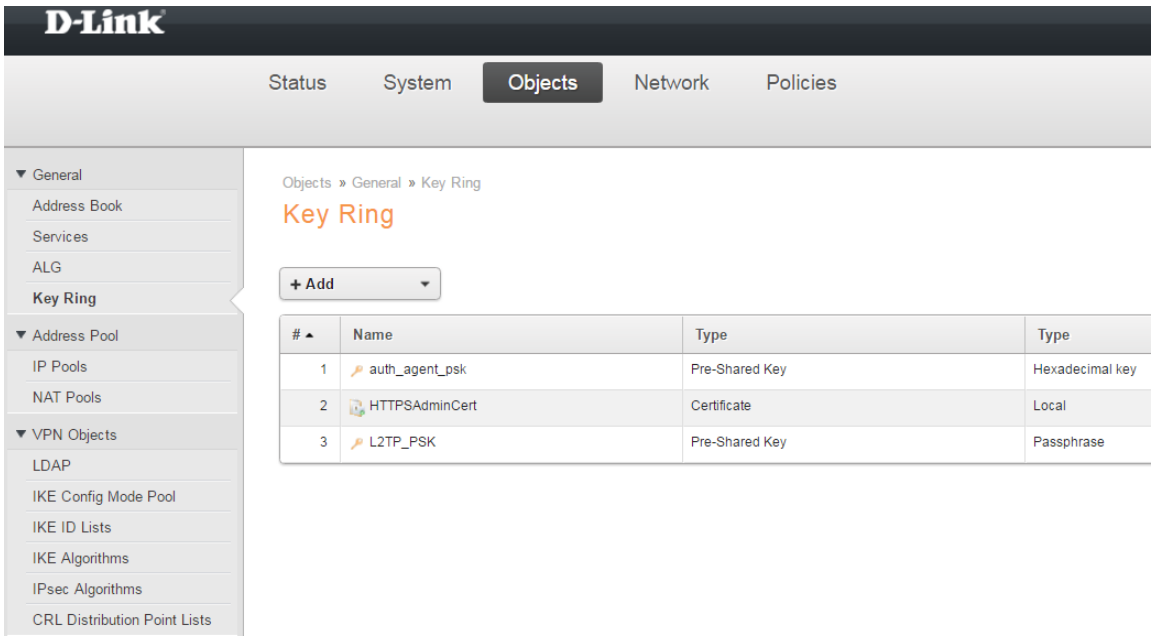
Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is “admin” and password is “admin”.
Step 2. Set your firewall’s WAN settings as per Internet provider requirements.
In our example WAN is set to PPPoE.
Step 3. Add a new object into the Address Book: “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.

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.



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.



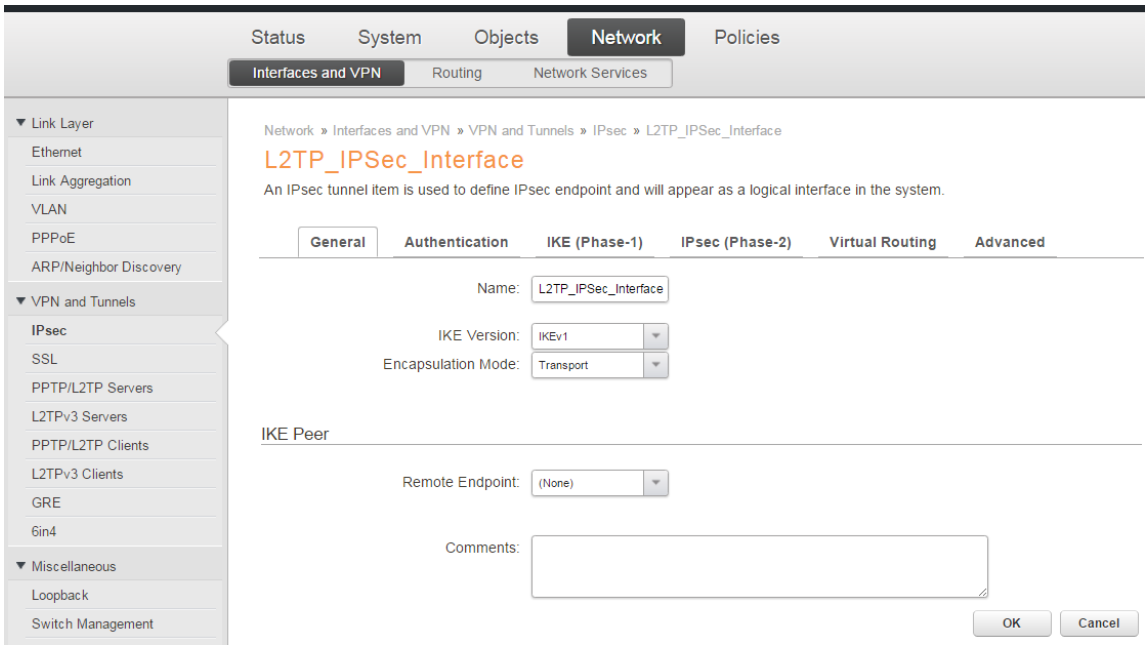


Step 6. Go to Network->Interfaces and VPN->VPN and Tunnels->IPSec then add an IPSec Tunnel.

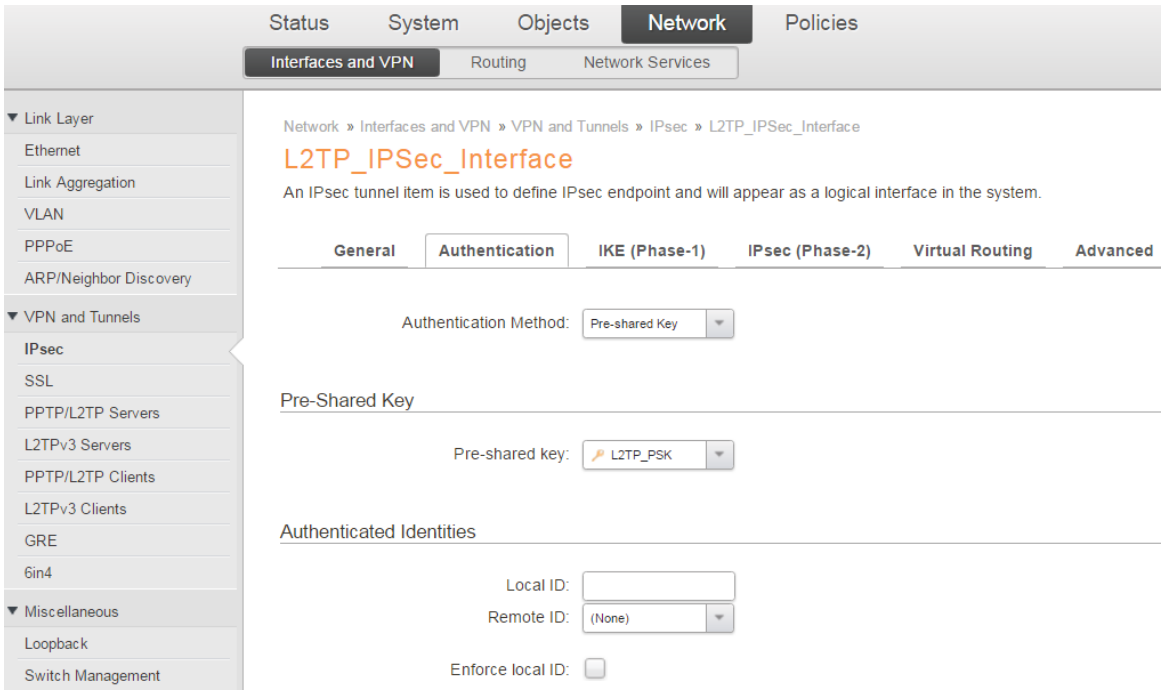
Name – Enter a name e.g. “L2TP_IPSec_Interface”.

IKE Version – set as IKEv1.

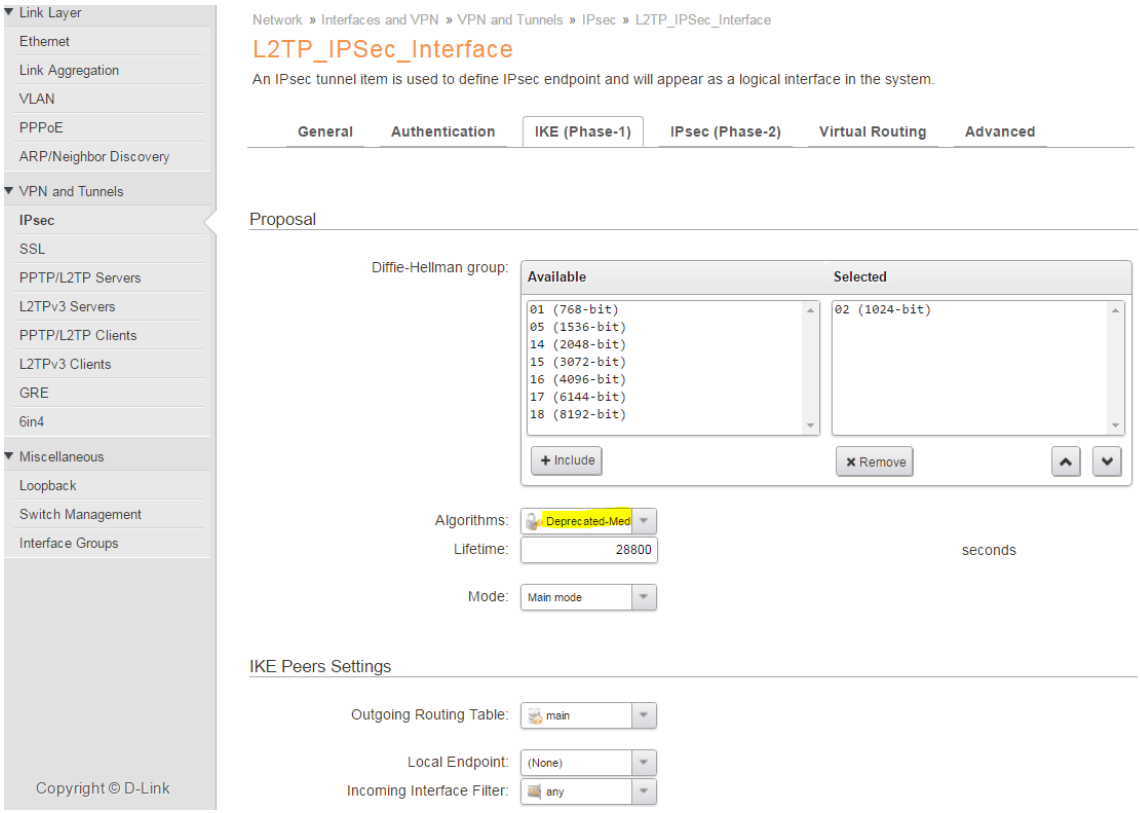
Encapsulation Mode – set as Transport.

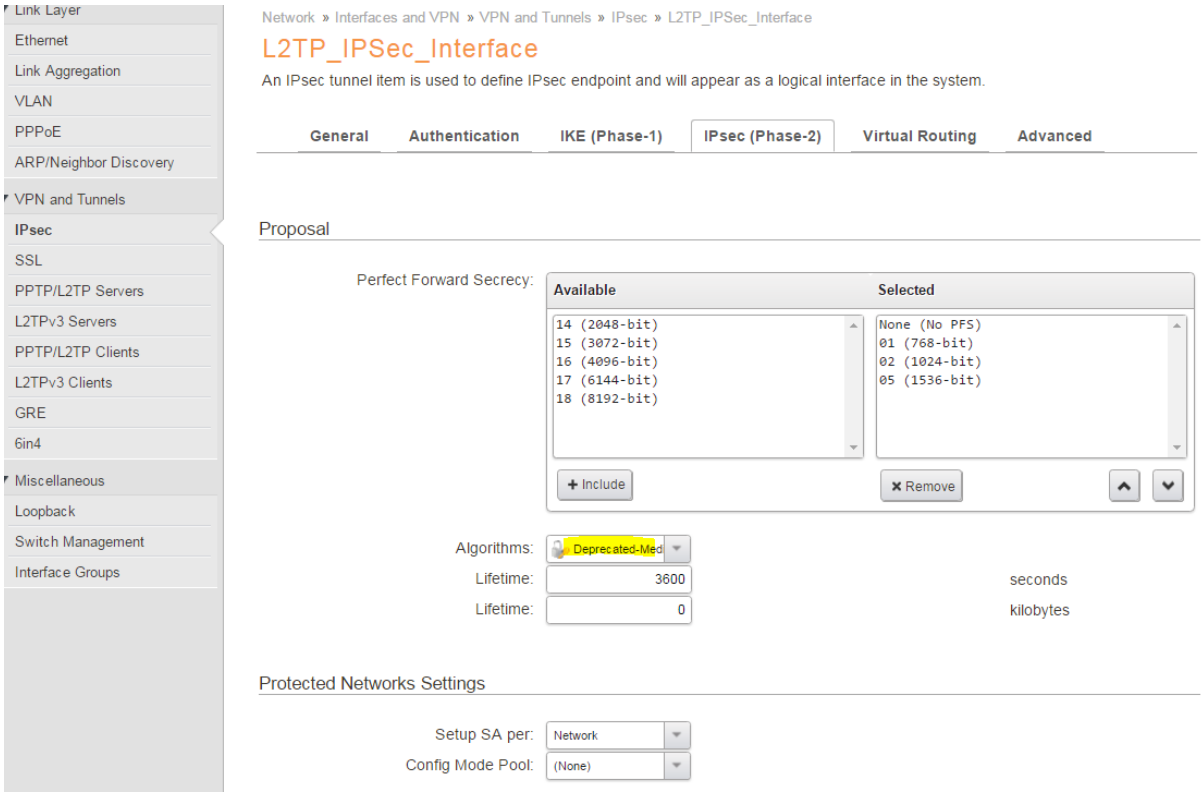


Step 6.1. Under Authentication Tab, select Pre-Shared Key in the Authentication Method and L2TP_PSK that you add in **Step 5.**

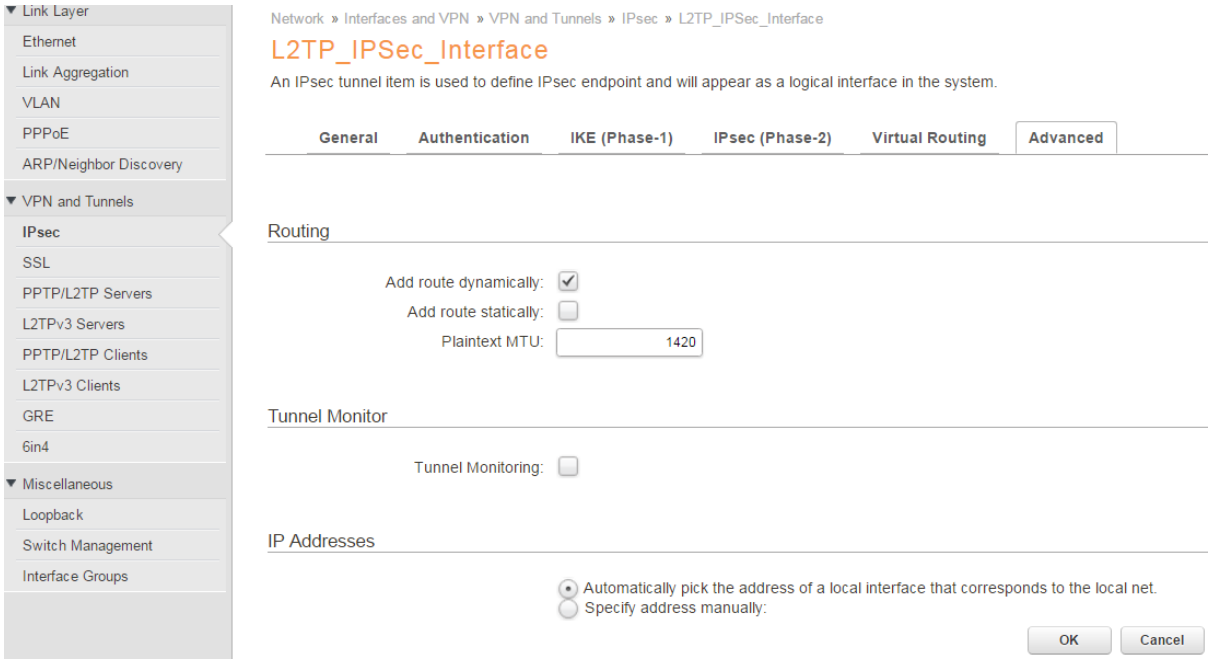


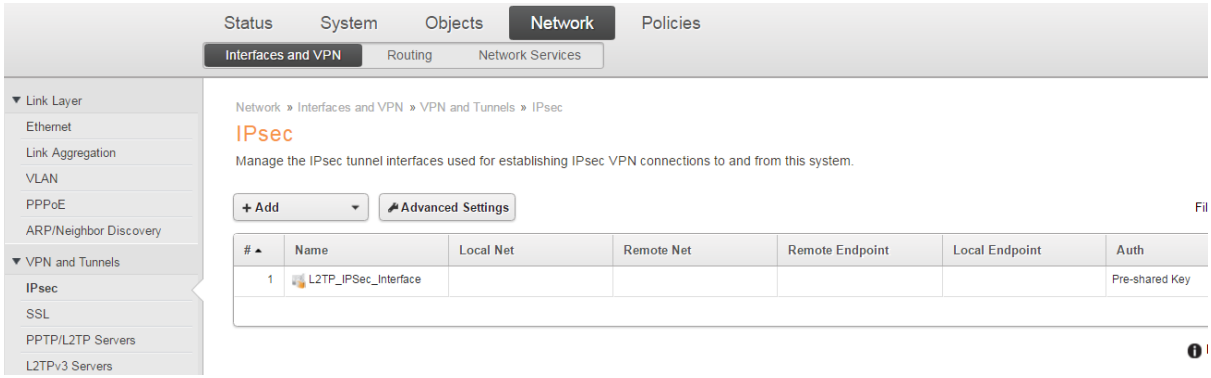
Step 6.2. Under IKE (Phase-1) and IPSec (Phase-2) tabs, select Deprecated Medium as Algorithm.



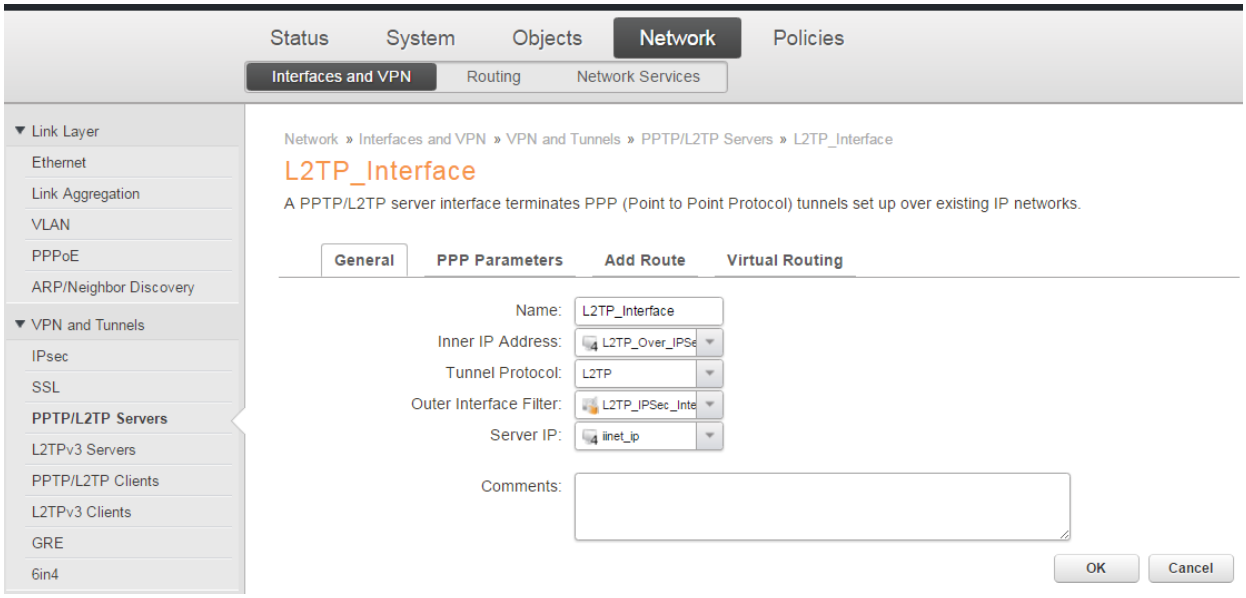


Step 6.3. Under Advanced tab, tick Add route dynamically. Then Press the OK button.



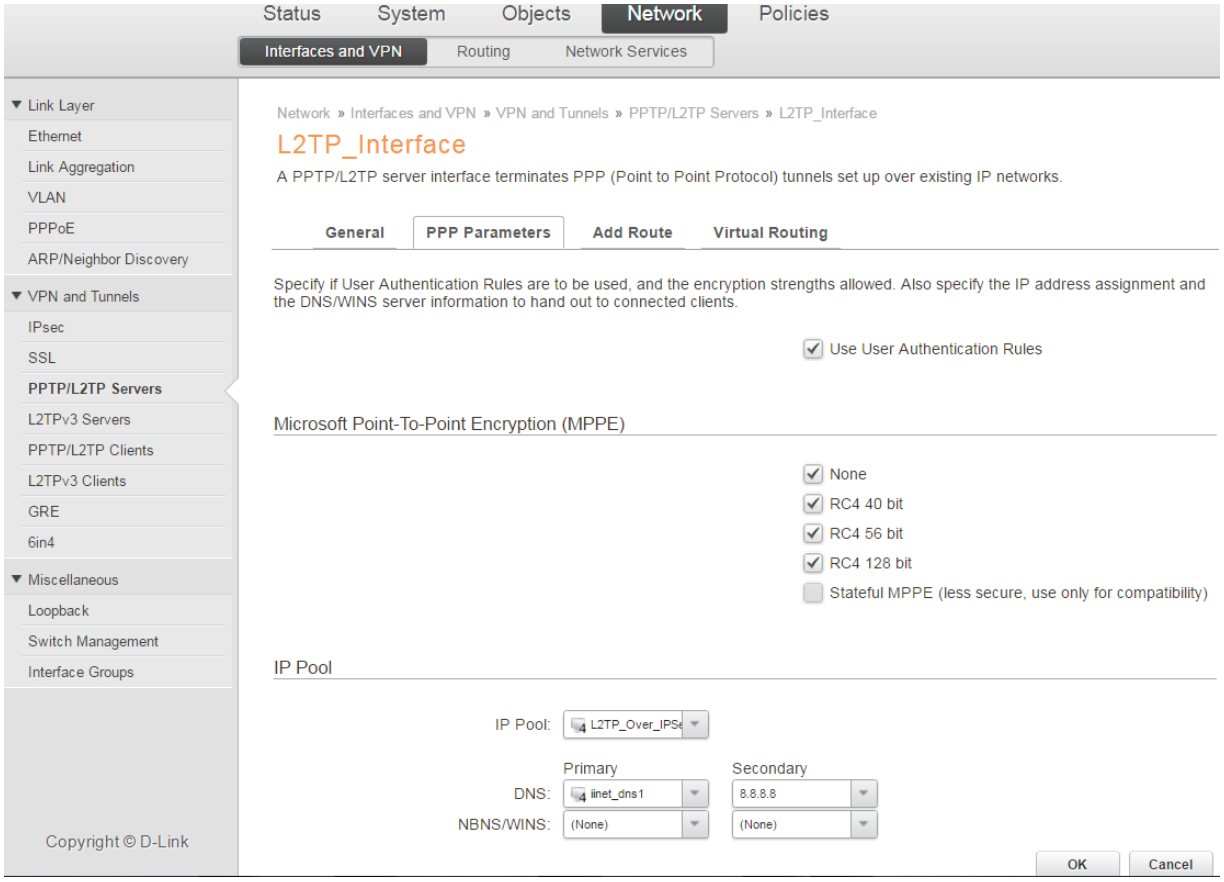


Step 7. Go to Network->Interfaces and VPN->VPN and Tunnels->PPTP/L2TP Servers.
Add a new PPTP/L2TP Server.
Inner IP Address – set as “L2TP_Over_IPSec_Server” you added in **Step 4**.
Tunnel Protocol – L2TP.
Outer Interface Filter – set as “L2TP_IPSec_Interface” you added in **Step 6**.
Server IP – set as iinet_ip (the PPPoE interface ip in this example).

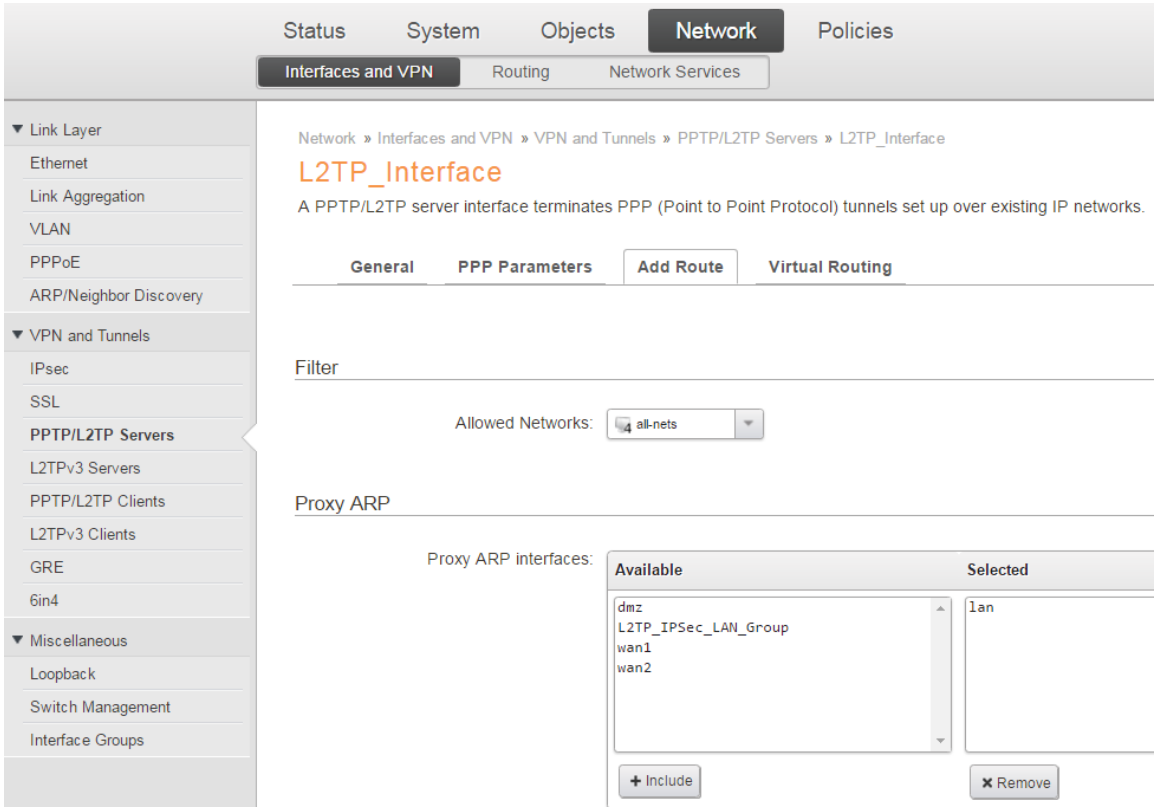


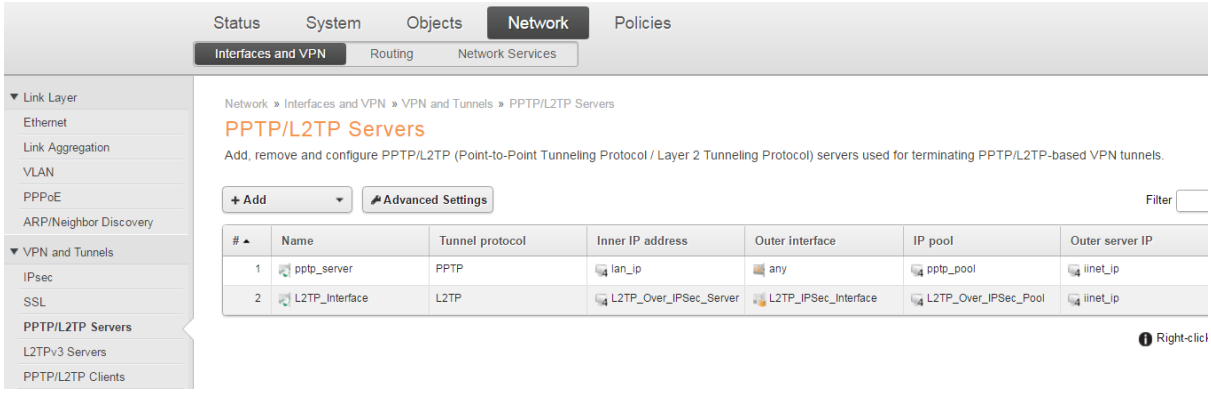
Step 7.1. Under PPP Parameters.

IP Pool – set as “L2TP_Over_IPSec_Pool” you added in **Step 3** and set the Primary and Secondary DNS.

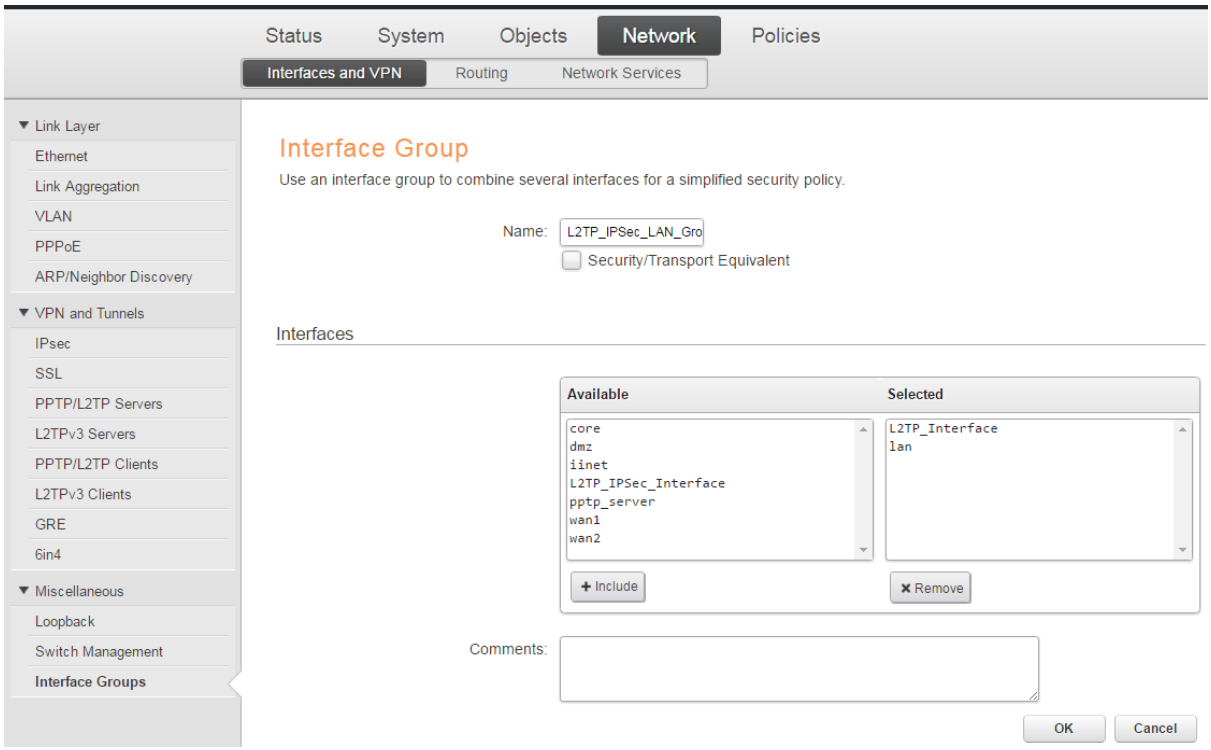


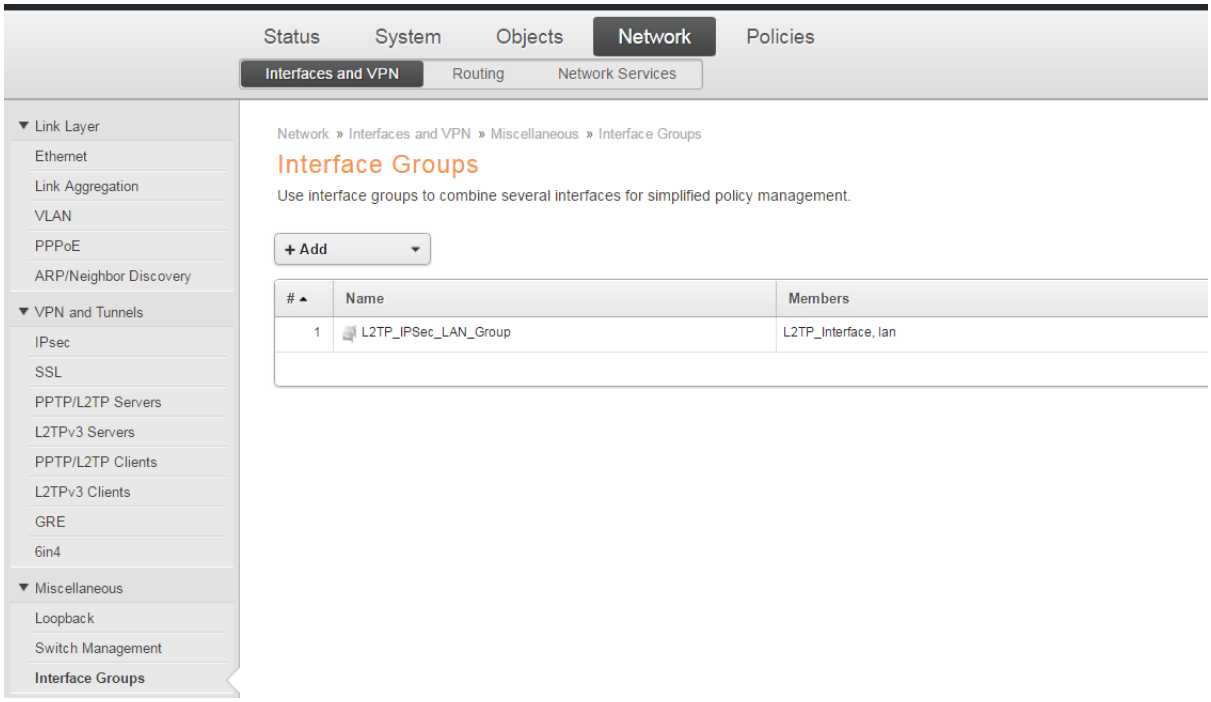
Step 7.2. Under Add Route tab.
Filter – set as “all-nets”
Proxy ARP – include “lan”
Then press OK button.



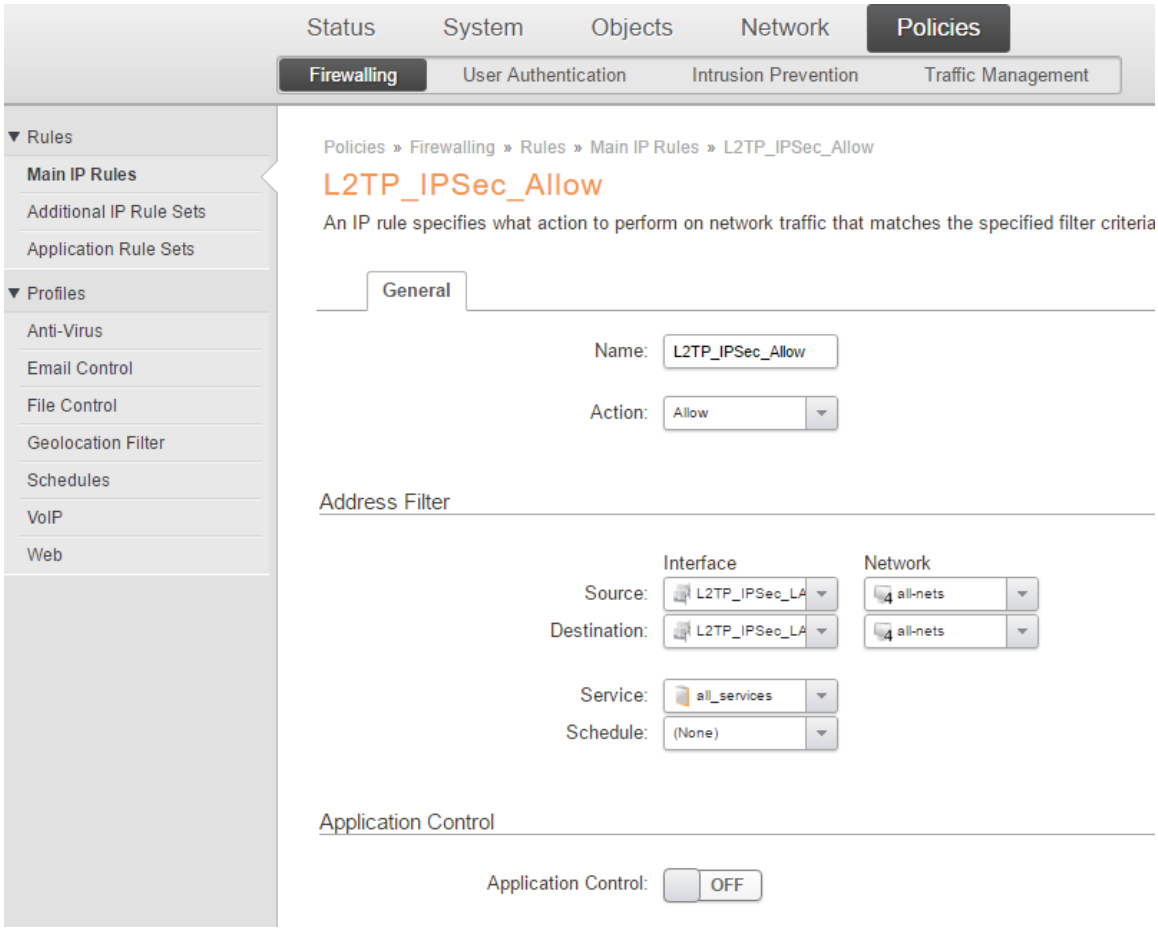


Step 8. Go to Network->Interfaces and VPN->Miscellaneous->Interface Groups.
Add interface groups for “L2TP_Interface” (added in **Step 7**) and “lan”

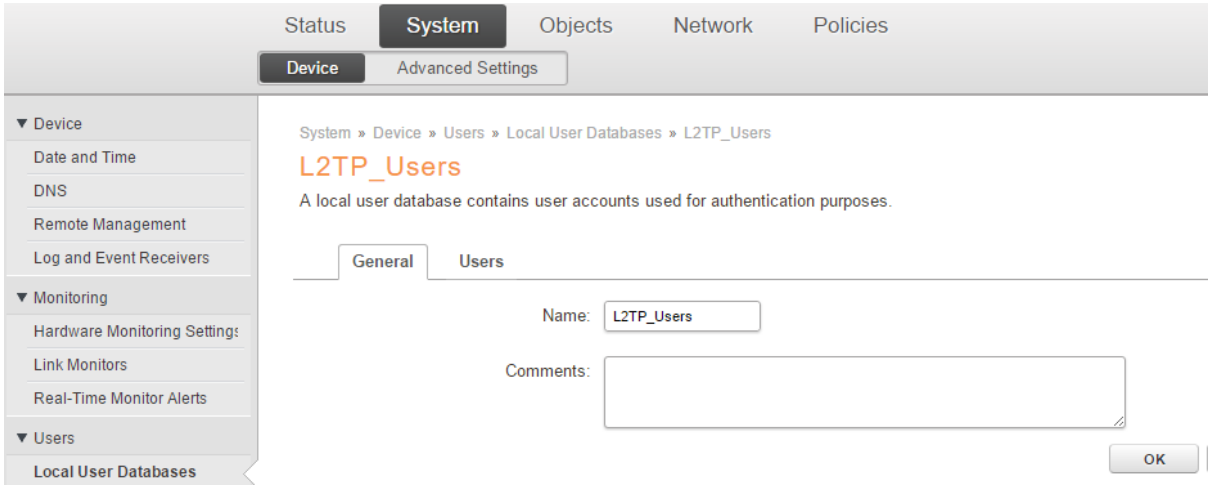




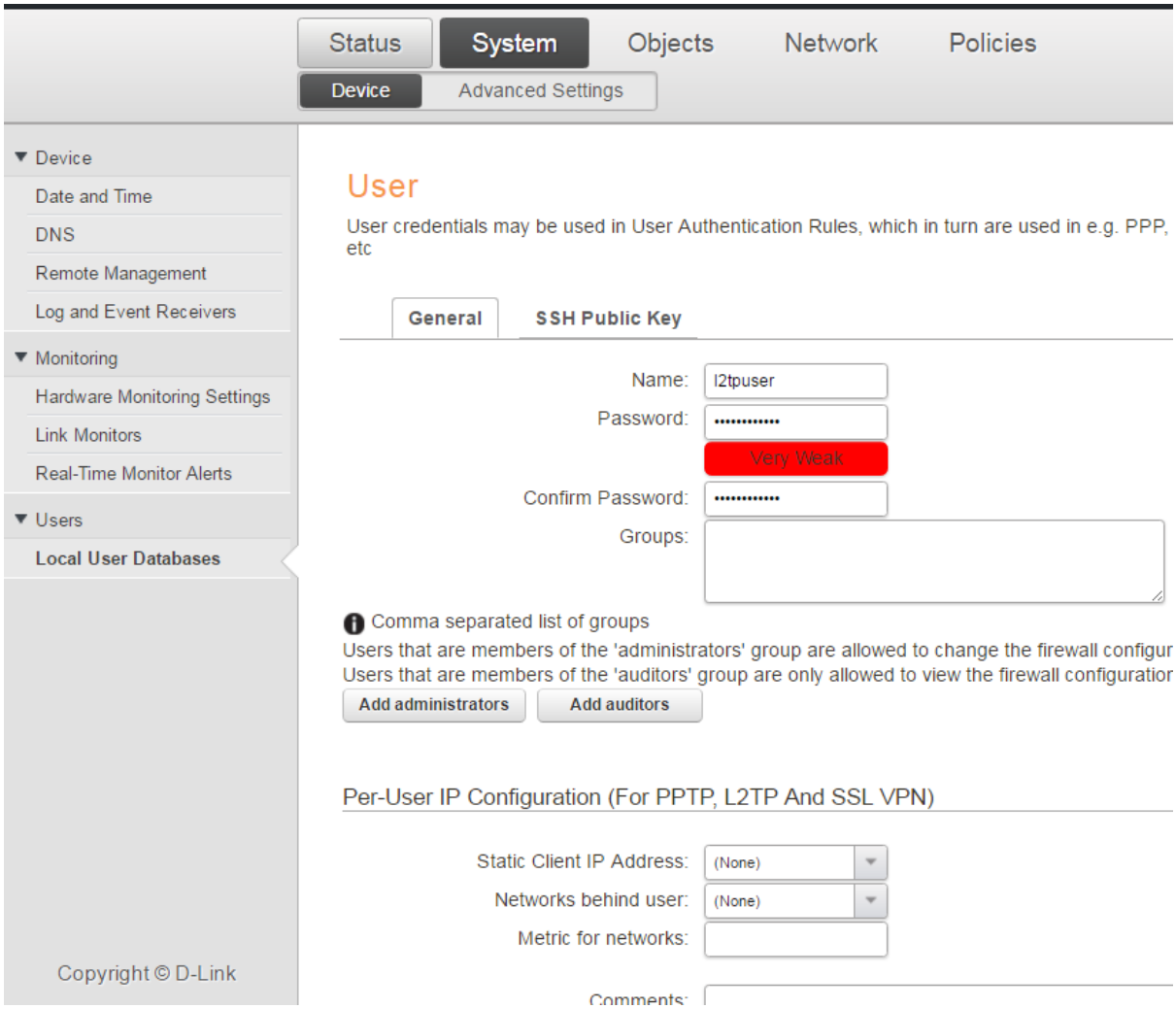
Step 9. Go to Policies->Firewalling->Rules->Main IP Rules. Create a new IP Rule to allow L2TP Tunnel communication with LAN:
Set Action as “Allow”.
Set Source Interface/Network as “L2TP_IPSec_LAN_Group”/all-nets.
Set Destination Interface/Network as “L2TP_IPSec_LAN_Group”/all-nets.
Service: all_services.
Then press OK button.

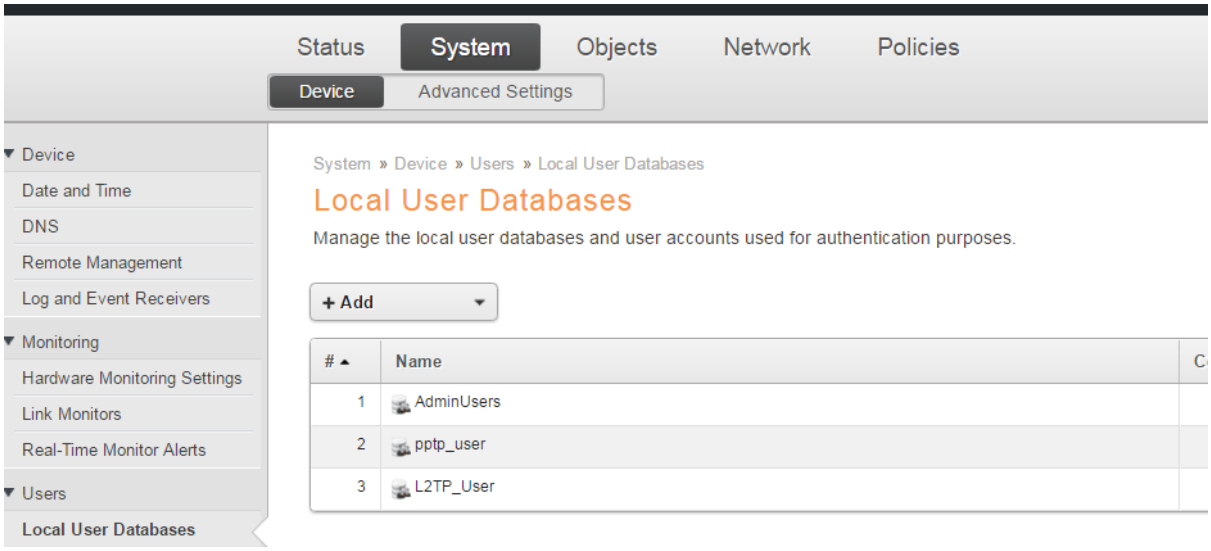


Step 10. Go to System->Device->Users->Local User Database.
Add Local User Database.
Enter a name e.g. L2TP_users.

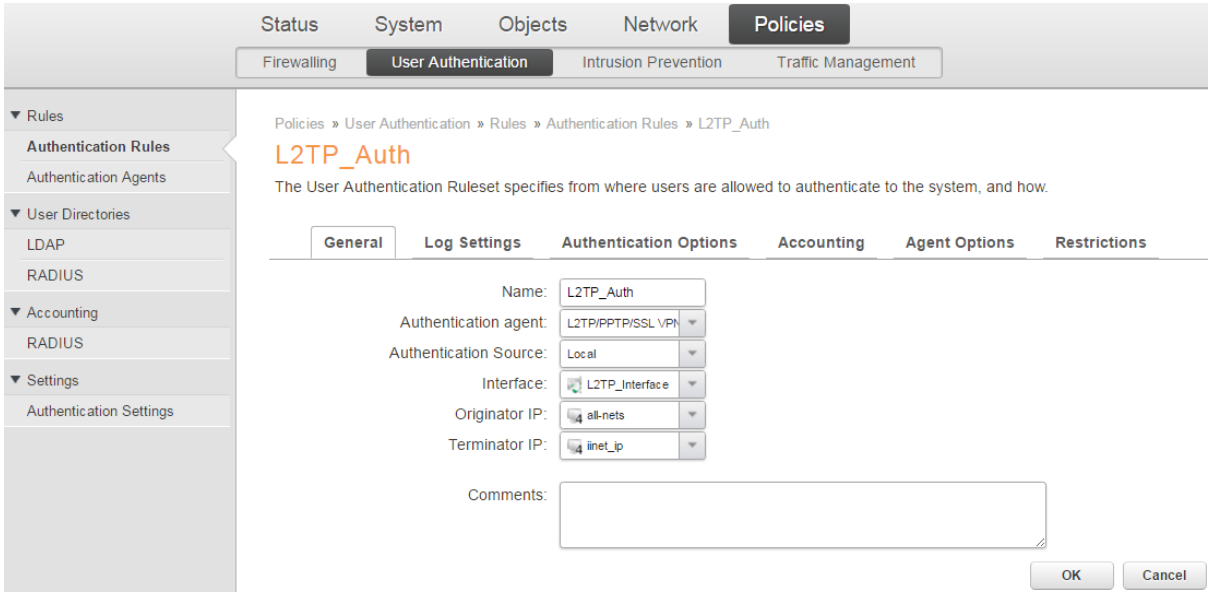


Step 10.1. Go to Users tab then enter l2tp username and password. Then press OK button.

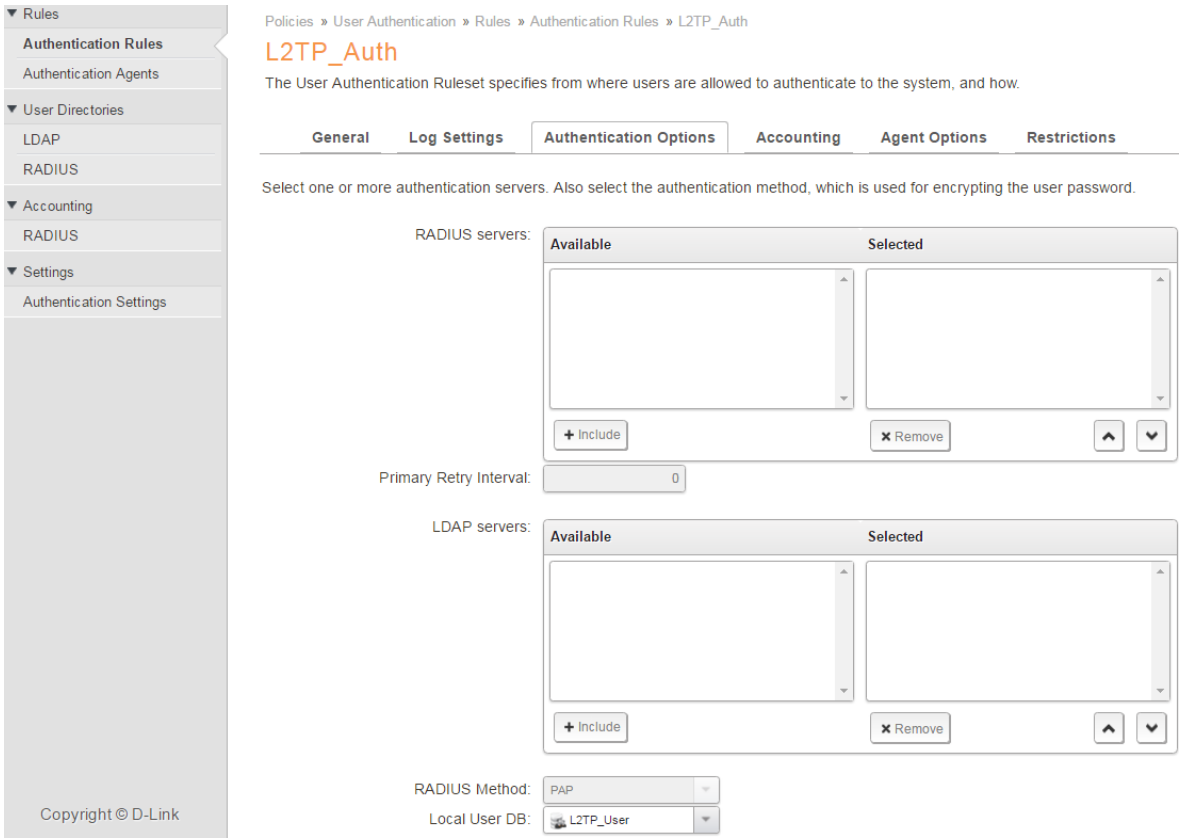




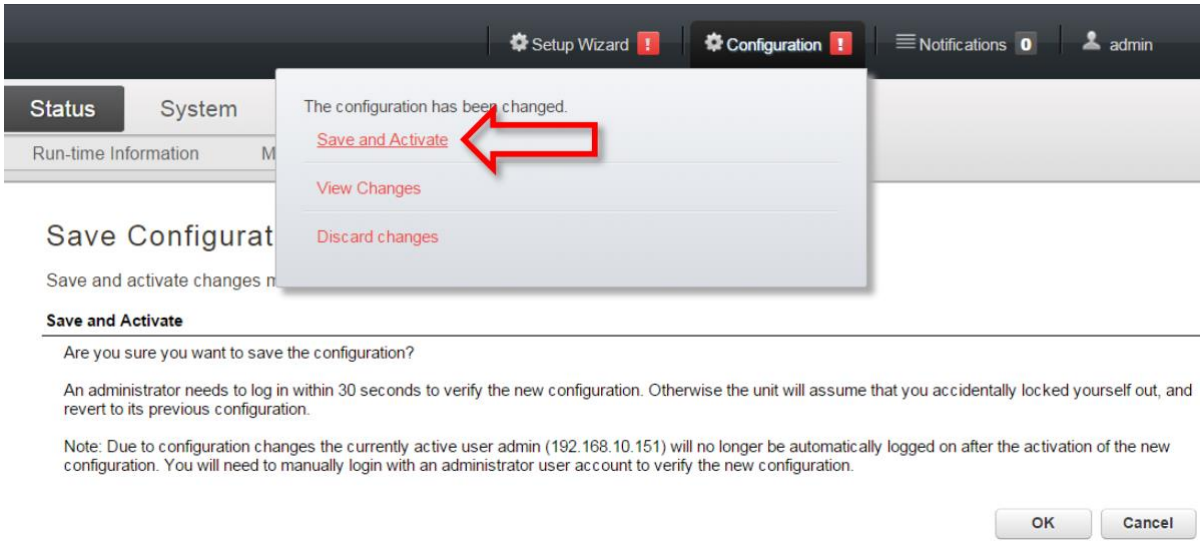
Step 11. Go to Policies->User Authentication->Rules->Authentication Rules.
Add User Authentication Rule.
Name: L2TP_Auth.
Authentication agent – set as L2TP/PPTP/SSL VPN.
Authentication Source – set as Local.
Interface – set as “L2TP_Interface” added in **Step 7**.
Originator IP – set as “all-nets”.
Terminator IP – set as “iinet_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.

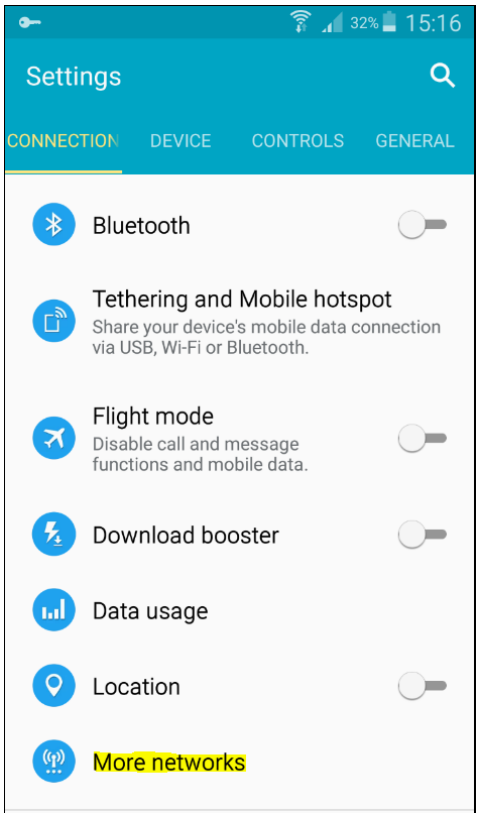


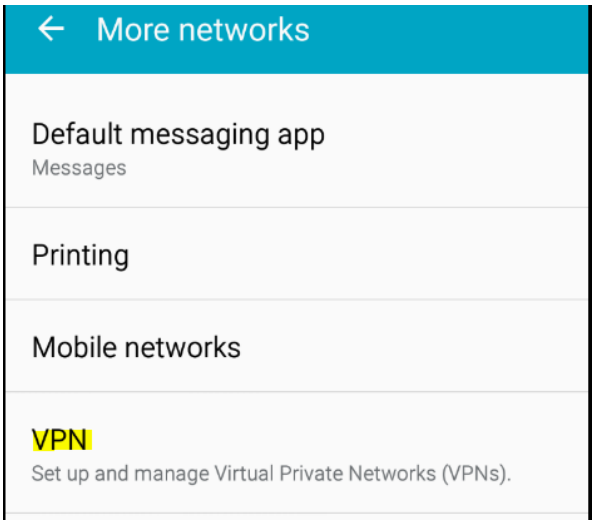
Step 12. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”.
Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.
NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.



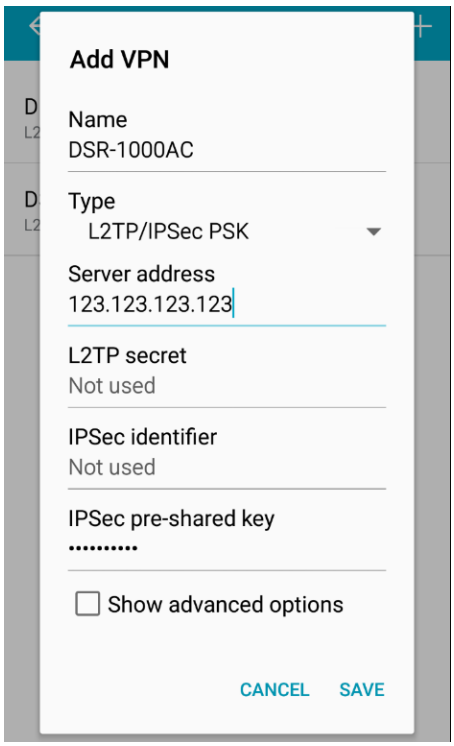
Android 5.0 Settings.

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

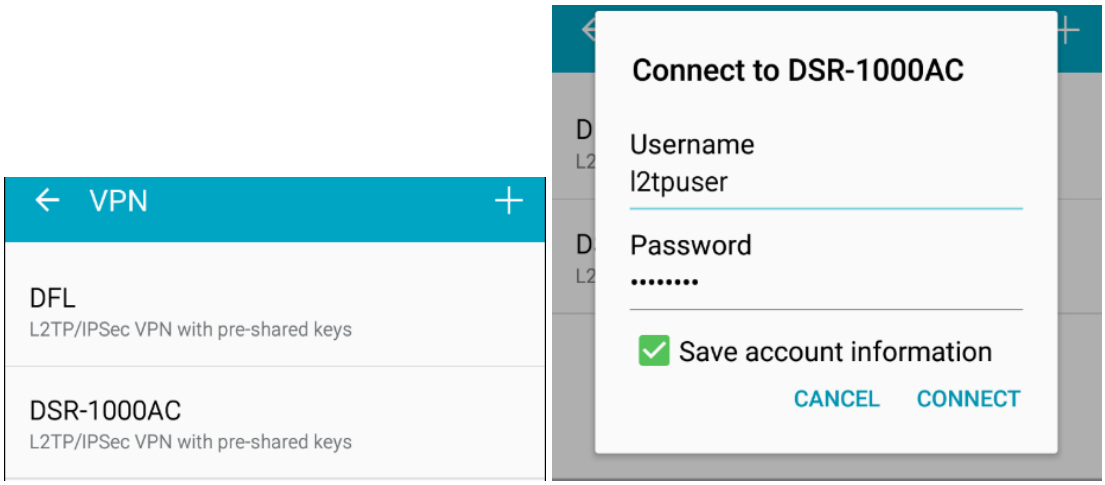




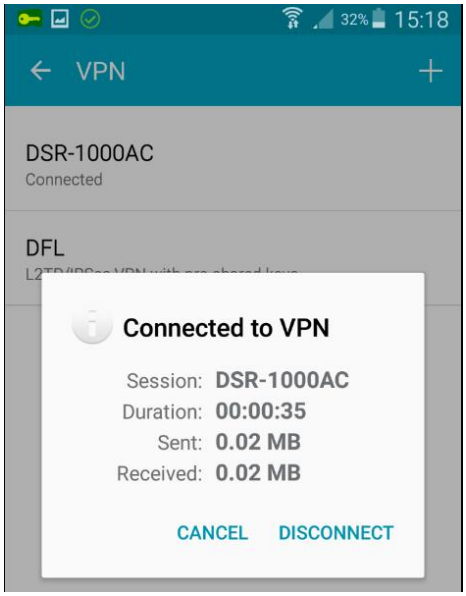
1.1 Add a new L2TP/IPSec PSK Profile and enter the L2TP server public IP address and Pre-Shared Key (entered in **Step 5**) then Save.



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



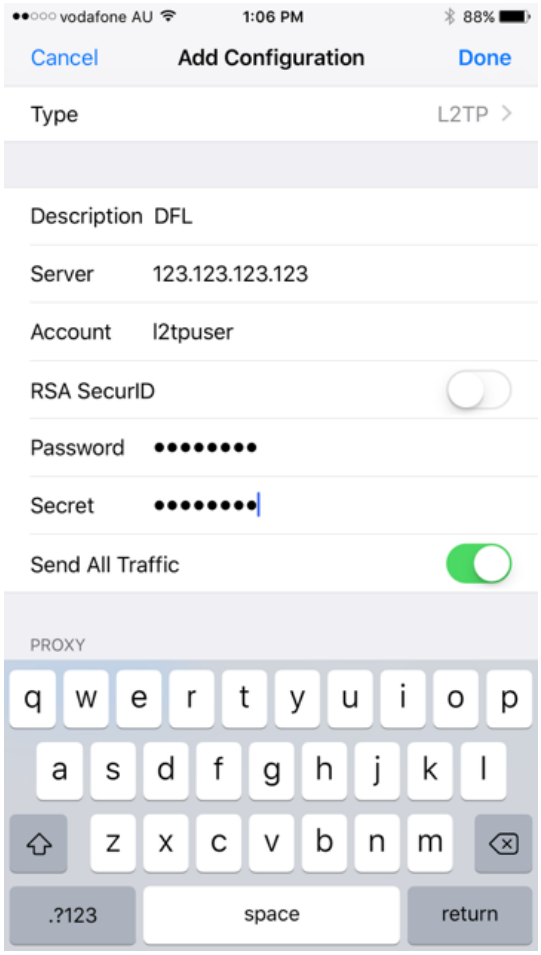
You should see a Key icon on the top-left hand corner that indicates it is connected.



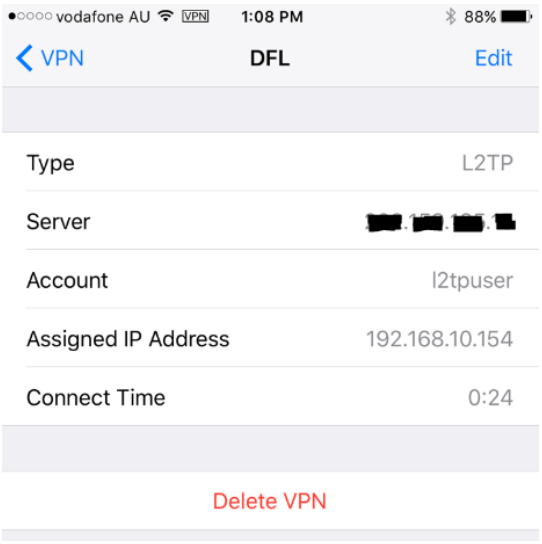
IOS v10.3 (iPhone 7 Plus running) Settings:

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**.



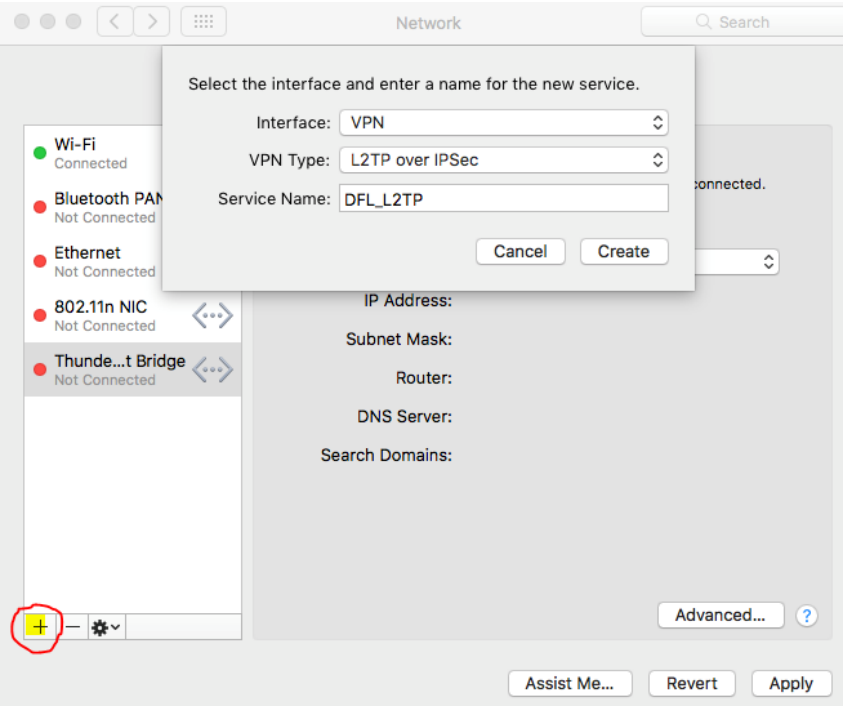
2.1 Select DFL and enable the **Status** to connect.



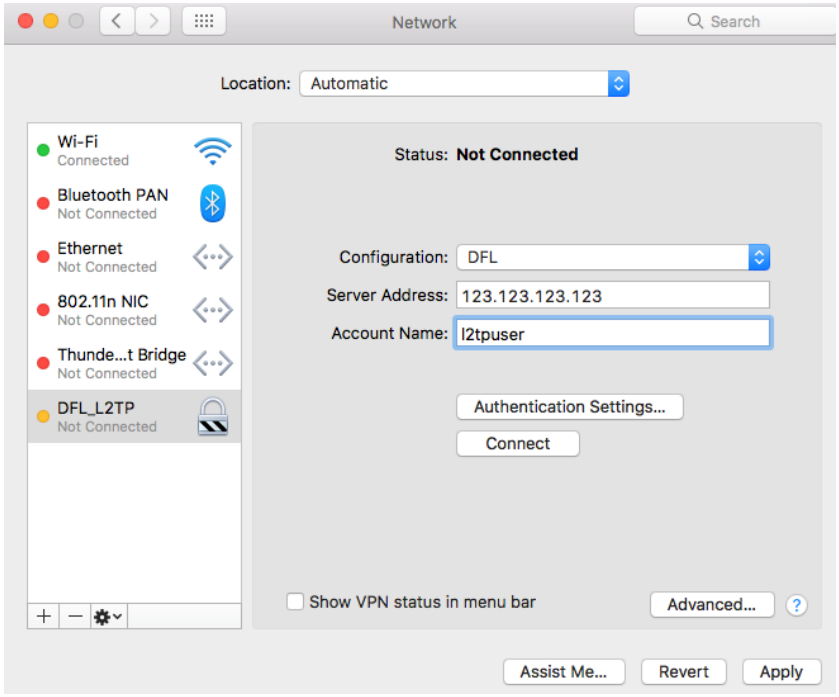
MAC OS Sierra v10.12.2 Settings.

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

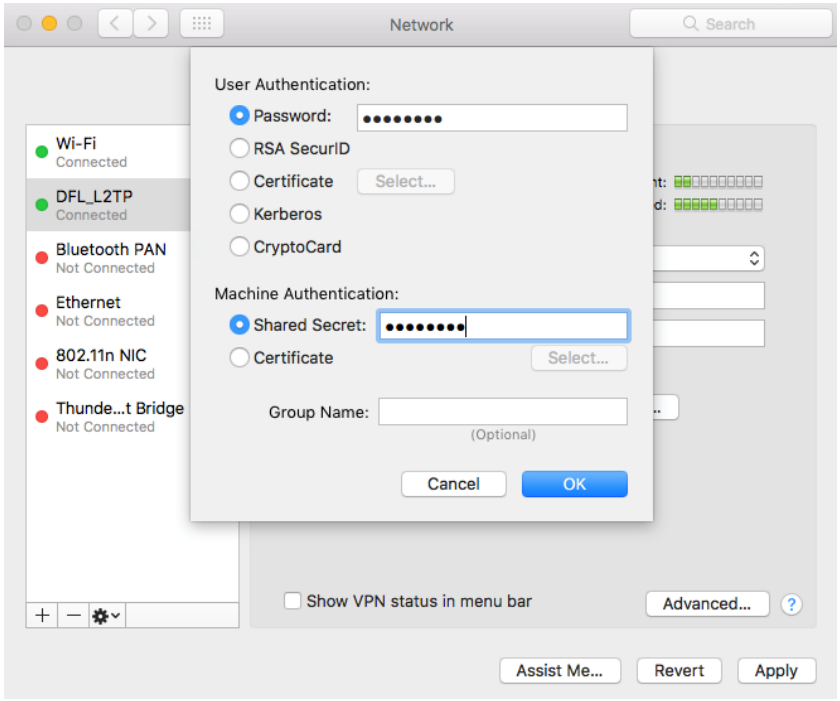
Interface – set as VPN.
VPN type – set as L2TP Over IPSec.
Service name – enter a name you prefer e.g. DFL_L2TP then click Create.



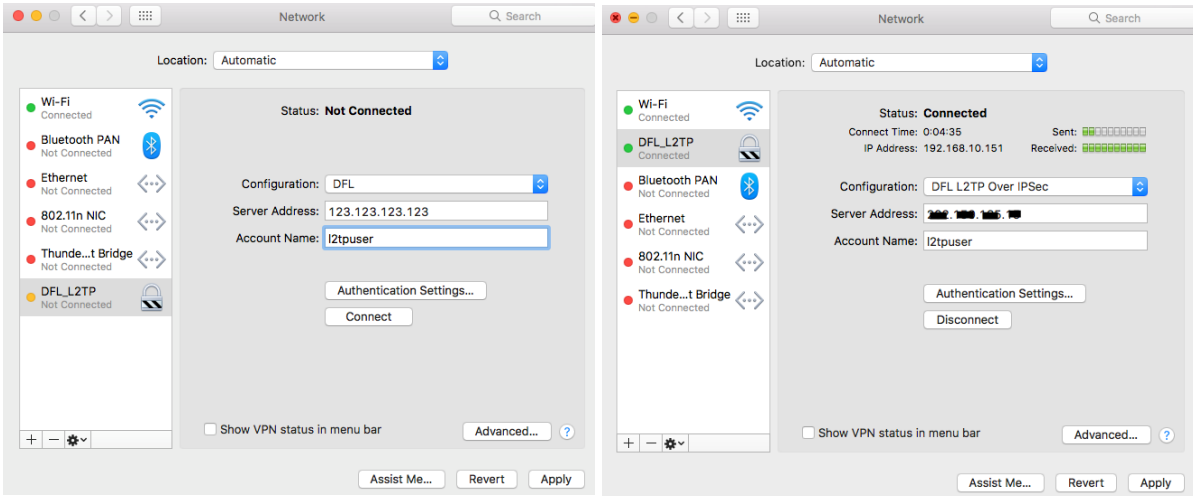
3.1 Enter a Configuration name, Server Address and the L2TP username added in **Step 10**.



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.

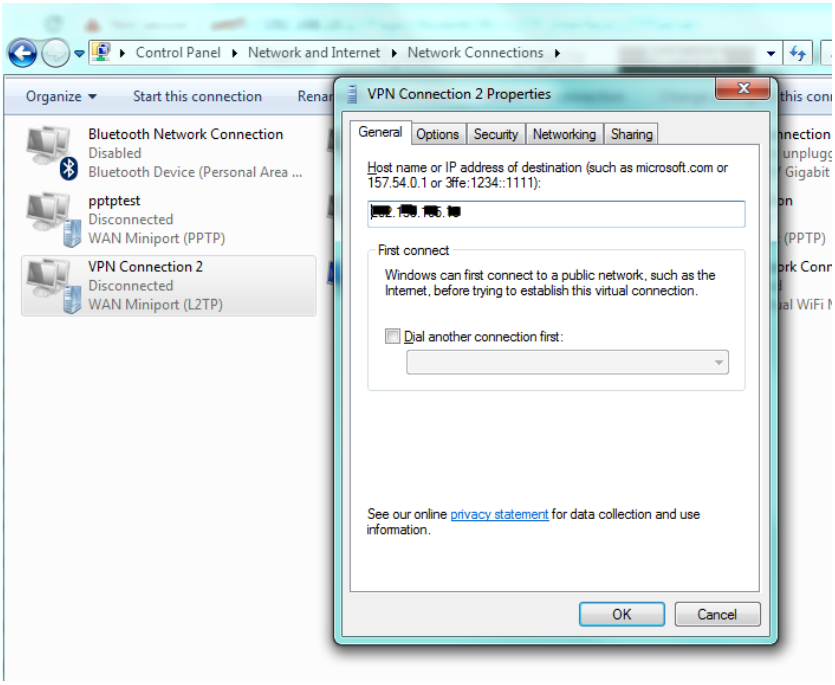


3.3 Click **Connect** button to established a connection.



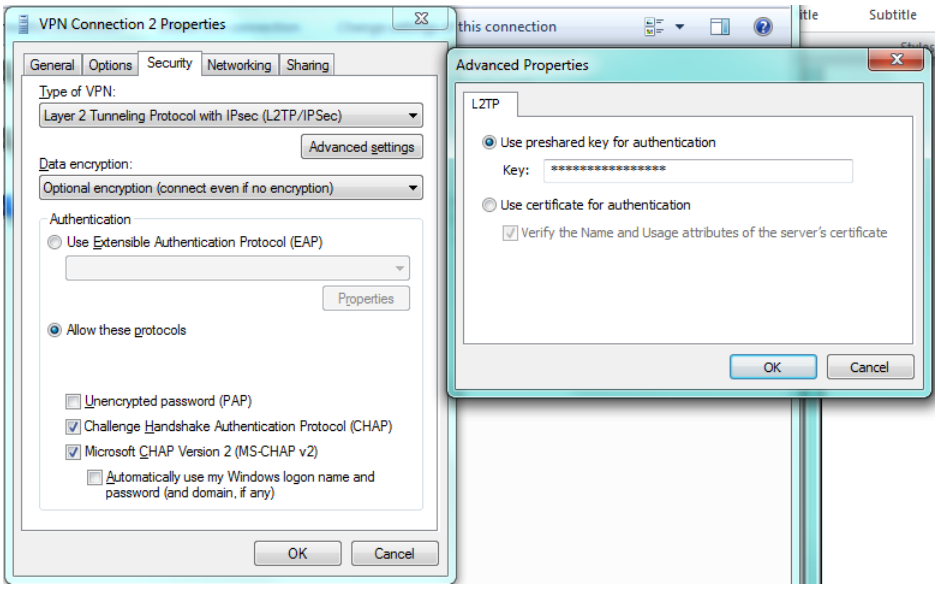
Windows L2TP Client Settings:

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**.