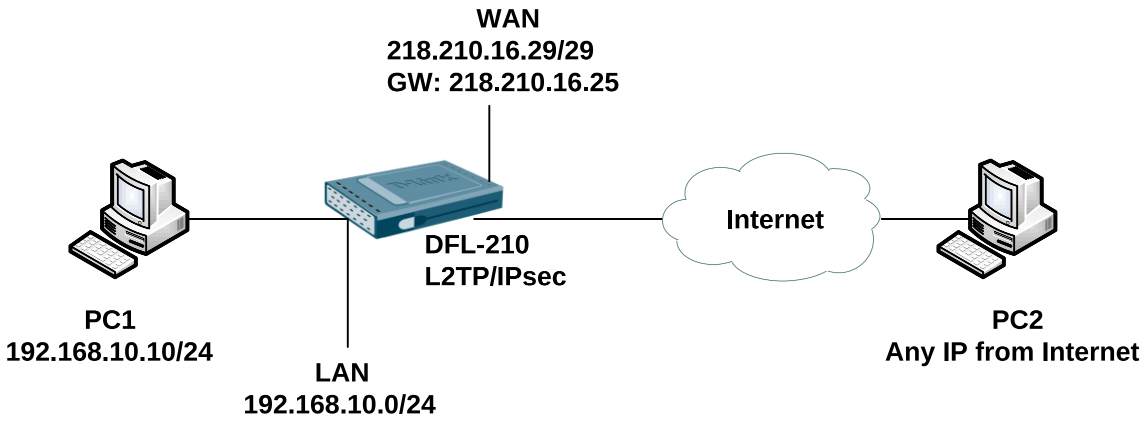
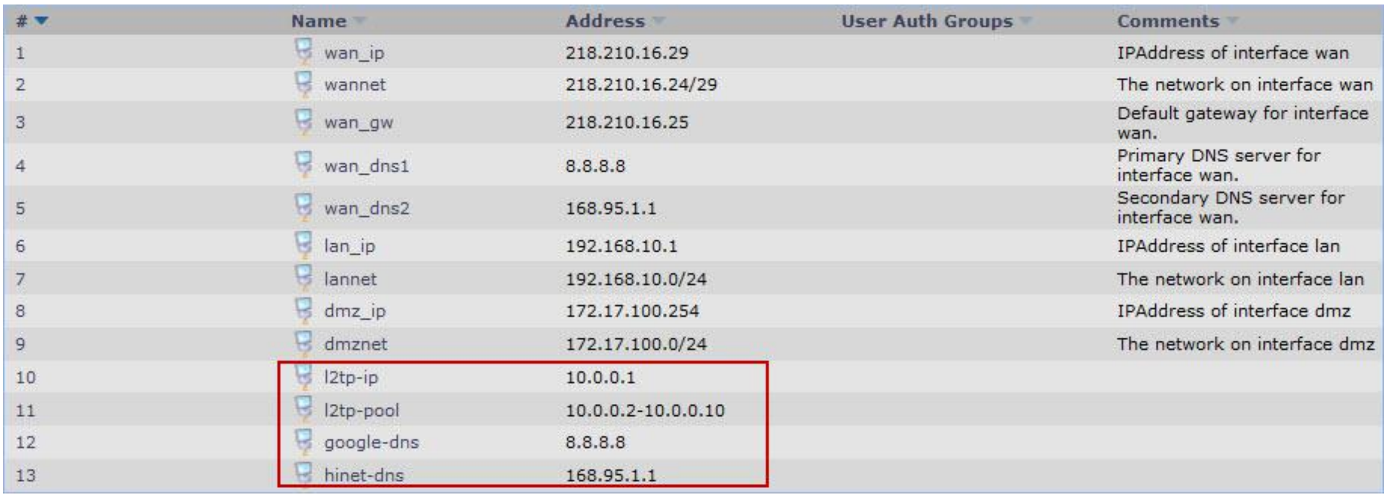
How to set up L2TP IPSec make remote user traffic to go through the internet



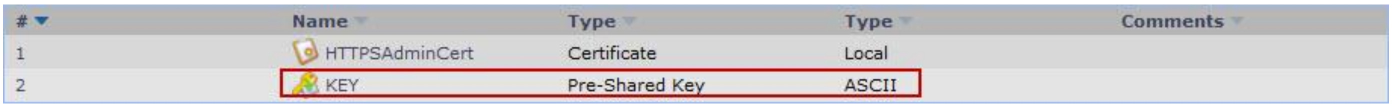
[DFL-210 Setup]

1. Address Book > InterfaceAddresses



#	Name	Address	User Auth Groups	Comments
1	wan_ip	218.210.16.29		IPAddress of interface wan
2	wannet	218.210.16.24/29		The network on interface wan
3	wan_gw	218.210.16.25		Default gateway for interface wan.
4	wan_dns1	8.8.8.8		Primary DNS server for interface wan.
5	wan_dns2	168.95.1.1		Secondary DNS server for interface wan.
6	lan_ip	192.168.10.1		IPAddress of interface lan
7	lannet	192.168.10.0/24		The network on interface lan
8	dmz_ip	172.17.100.254		IPAddress of interface dmz
9	dmznet	172.17.100.0/24		The network on interface dmz
10	l2tp-ip	10.0.0.1		
11	l2tp-pool	10.0.0.2-10.0.0.10		
12	google-dns	8.8.8.8		
13	hinet-dns	168.95.1.1		

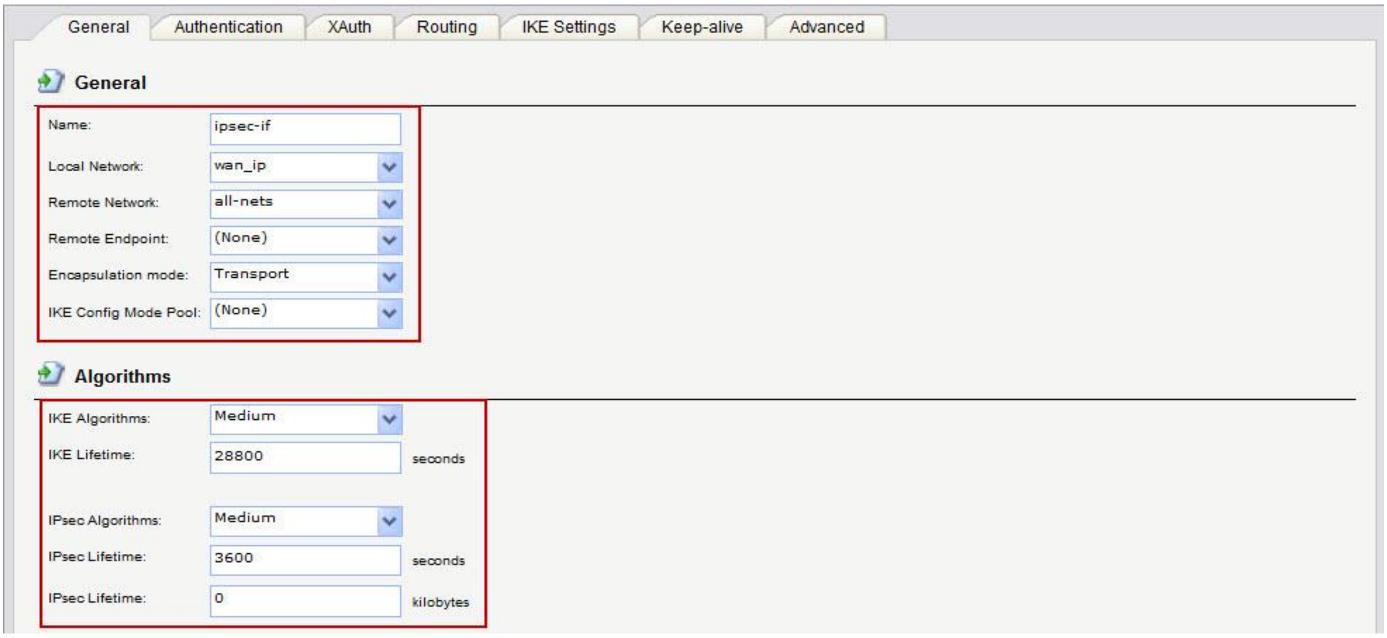
2. Objects > Authentication Objects > Add > Pre-Shared Key



#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	KEY	Pre-Shared Key	ASCII	

3. Interfaces > IPsec

General



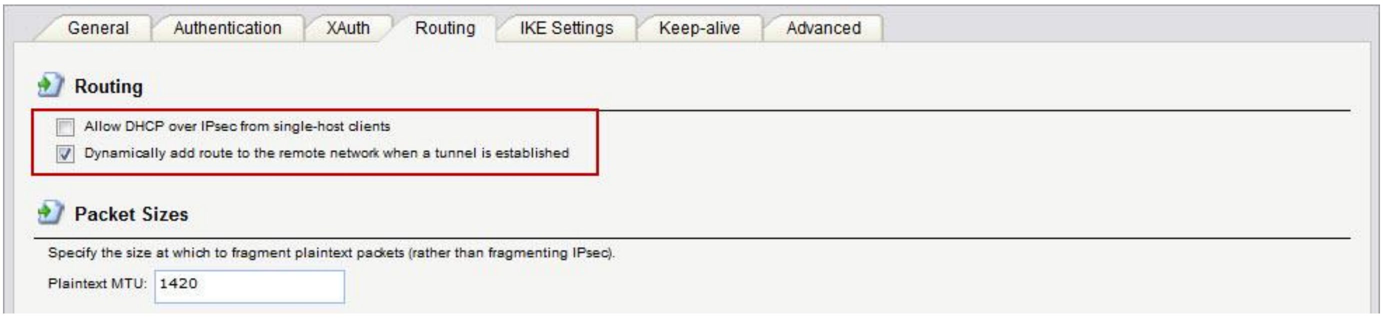
General

Name:	ipsec-if
Local Network:	wan_ip
Remote Network:	all-nets
Remote Endpoint:	(None)
Encapsulation mode:	Transport
IKE Config Mode Pool:	(None)

Algorithms

IKE Algorithms:	Medium	
IKE Lifetime:	28800	seconds
IPsec Algorithms:	Medium	
IPsec Lifetime:	3600	seconds
IPsec Lifetime:	0	kilobytes

Routing



Routing

□ Allow DHCP over IPsec from single-host clients

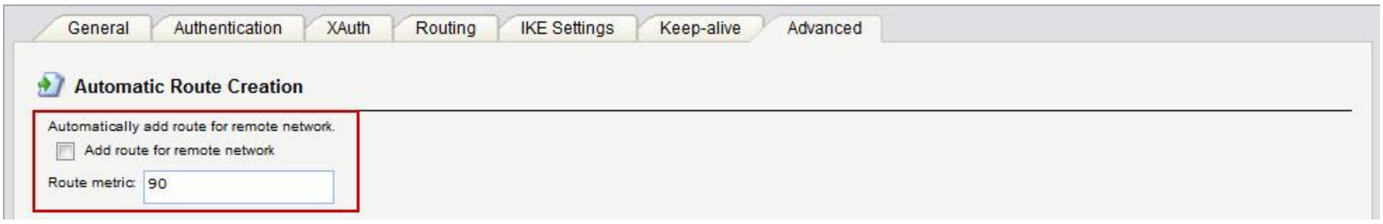
☑ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1420

Advanced



Automatic Route Creation

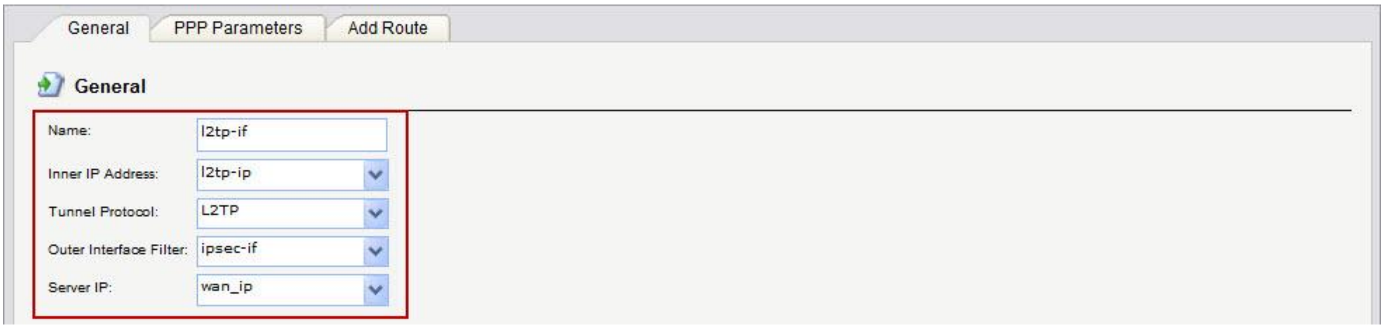
Automatically add route for remote network.

□ Add route for remote network

Route metric: 90

4. Interfaces > PPTP/L2TP Servers

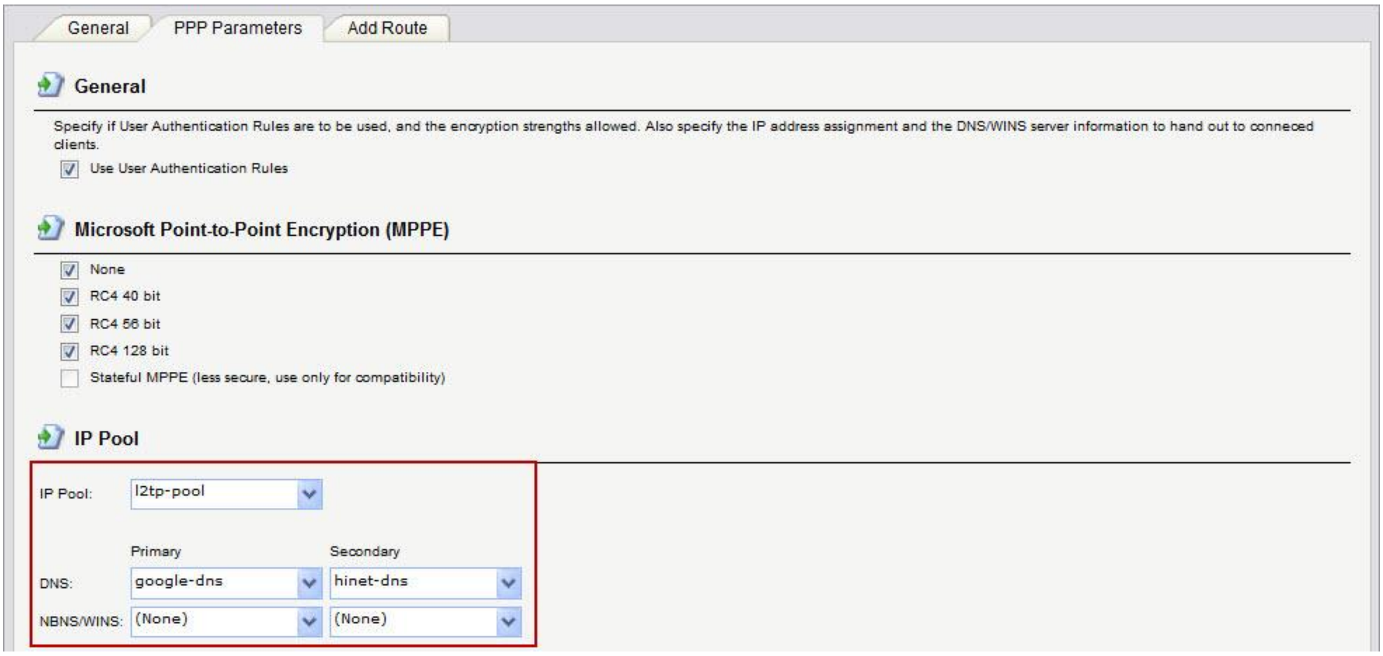
General



General

Name:	l2tp-if
Inner IP Address:	l2tp-ip
Tunnel Protocol:	L2TP
Outer Interface Filter:	ipsec-if
Server IP:	wan_ip

PPP Parameters



General

Specify if User Authentication Rules are to be used, and the encryption strengths allowed. Also specify the IP address assignment and the DNS/WINS server information to hand out to conneced clients.

☑ Use User Authentication Rules

Microsoft Point-to-Point Encryption (MPPE)

☑ None

☑ RC4 40 bit

☑ RC4 56 bit

☑ RC4 128 bit

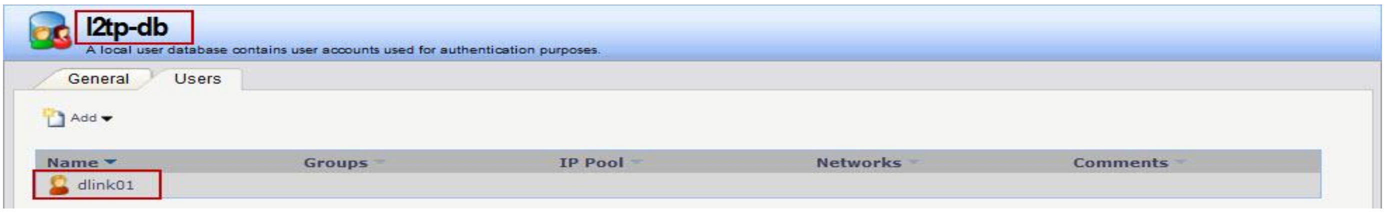
□ Stateful MPPE (less secure, use only for compatibility)

IP Pool

IP Pool: l2tp-pool

	Primary	Secondary
DNS:	google-dns	hinet-dns
NBNS/WINS:	(None)	(None)

5. Create a new Authentication DB for L2TP and create a new dial-in user account.



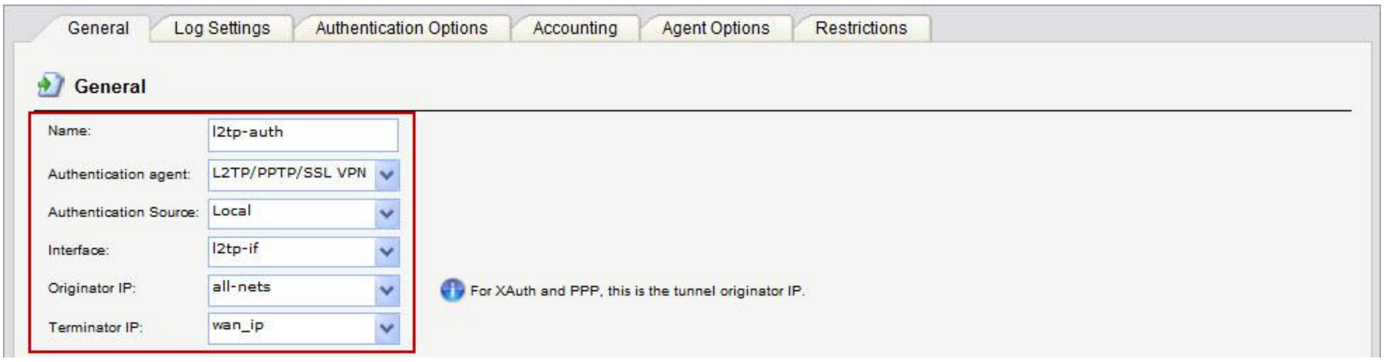
l2tp-db

A local user database contains user accounts used for authentication purposes.

Name	Groups	IP Pool	Networks	Comments
dlink01				

6. User Authentication > User Authentication Rule

General

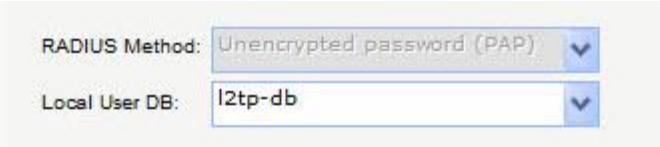


General

Name:	l2tp-auth
Authentication agent:	L2TP/PPTP/SSL VPN
Authentication Source:	Local
Interface:	l2tp-if
Originator IP:	all-nets
Terminator IP:	wan_ip

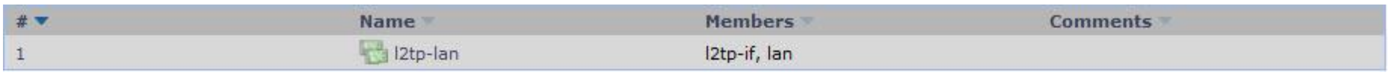
For XAuth and PPP, this is the tunnel originator IP.

Authentication Options



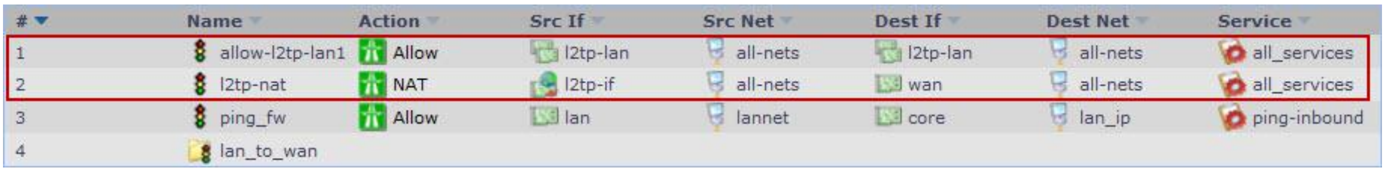
RADIUS Method:	Unencrypted password (PAP)
Local User DB:	l2tp-db

7. Create an interface groups for IP rules use.



#	Name	Members	Comments
1	l2tp-lan	l2tp-if, lan	

8. Rules > IP Rules



#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	allow-l2tp-lan1	Allow	l2tp-lan	all-nets	l2tp-lan	all-nets	all_services
2	l2tp-nat	NAT	l2tp-if	all-nets	wan	all-nets	all_services
3	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
4	lan_to_wan						

※ NAT rule must law than allow this rule.

[Test]

1. Before dial-in PC2 is use 111.250.24.114 this public IP.
2. When PC2 dial-in to DFL-210, PC2 will use DFL-210 WAN IP and pass through Internet.
3. PC2 can go through Internet and connect to PC1 at the same time

END