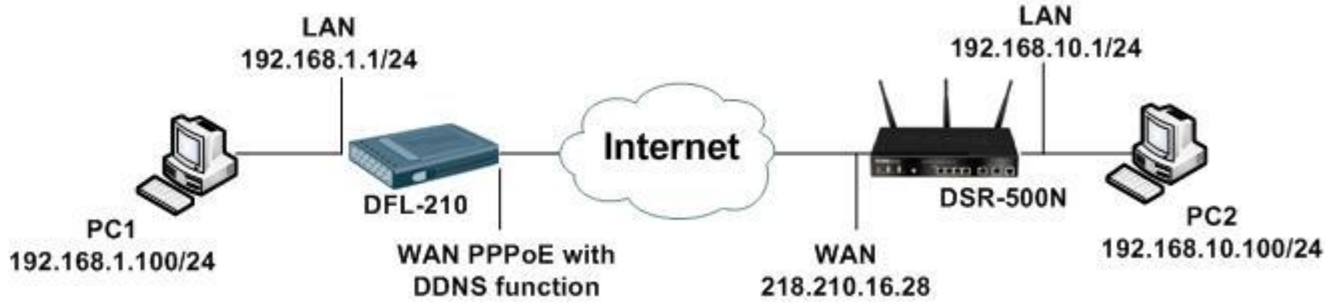
How to setup DDNS function on DFL model and create IPsec tunnel to DSR model

[Topology]



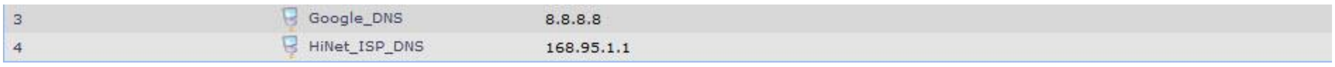
[DFL-210]

Firmware: 2.27.03.25-14787

DDNS Domain Name: chuckwang.dlinkddns.com

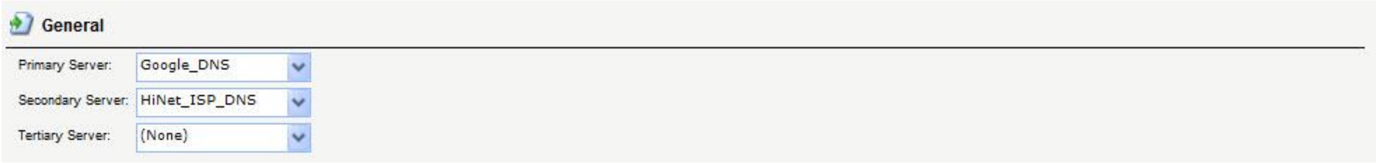
1. Objects > Address Book

   Add two of DNS server IP objects.



3	Google_DNS	8.8.8.8
4	HiNet_ISP_DNS	168.95.1.1

2. System > DNS



General

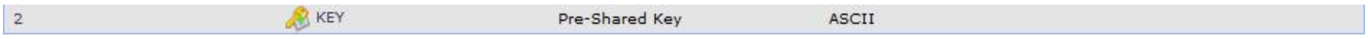
Primary Server: Google_DNS

Secondary Server: HiNet_ISP_DNS

Tertiary Server: (None)

3. Objects > Authentication Objects

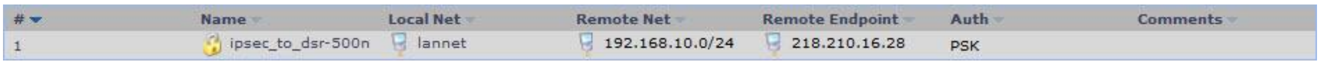
   Create Pre-Shared Key.



2	KEY	Pre-Shared Key	ASCII

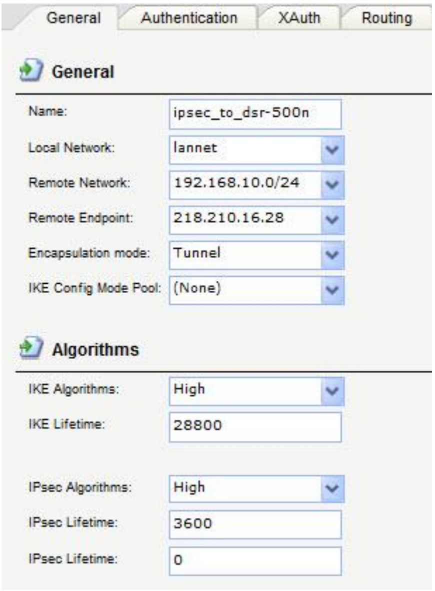
4. Interfaces > IPsec

   Create IPsec policy.



#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
1	ipsec_to_dsr-500n	lannet	192.168.10.0/24	218.210.16.28	PSK	

<General> < Authentication> <Routing>



General

Name: ipsec_to_dsr-500n

Local Network: lannet

Remote Network: 192.168.10.0/24

Remote Endpoint: 218.210.16.28

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

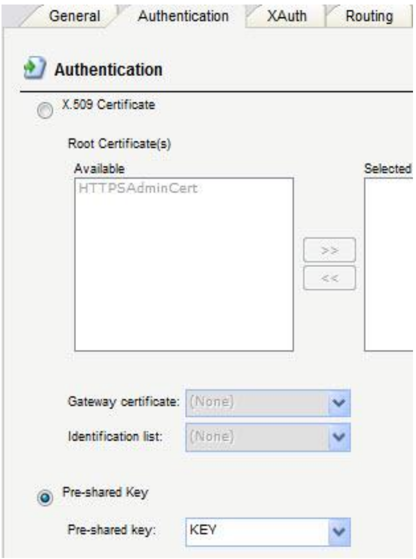
IKE Algorithms: High

IKE Lifetime: 28800

IPsec Algorithms: High

IPsec Lifetime: 3600

IPsec Lifetime: 0



Authentication

○ X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert

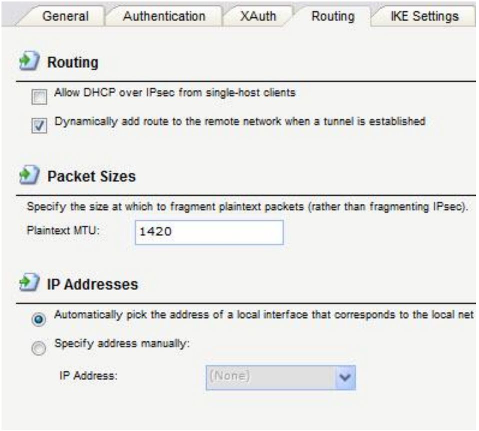
Selected

Gateway certificate: (None)

Identification list: (None)

● Pre-shared Key

Pre-shared key: KEY



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

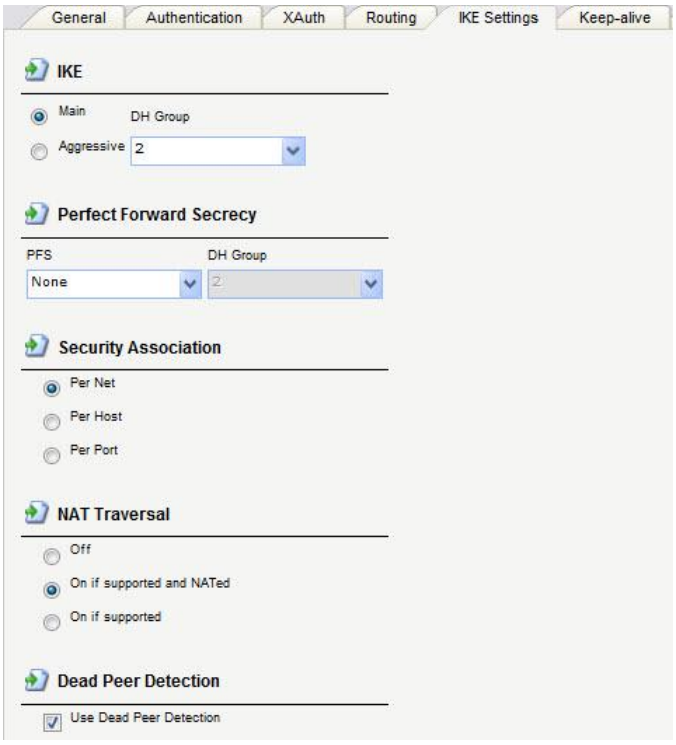
IP Addresses

● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)

<IKE Settings>



IKE

● Main
○ Aggressive

DH Group: 2

Perfect Forward Secrecy

PFS: None
DH Group: 2

Security Association

● Per Net
○ Per Host
○ Per Port

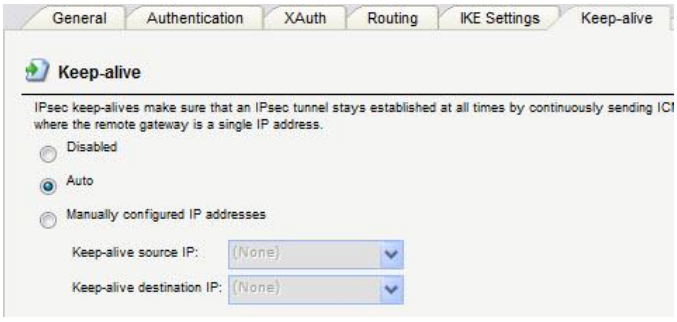
NAT Traversal

○ Off
● On if supported and NATed
○ On if supported

Dead Peer Detection

☑ Use Dead Peer Detection

<Keep-alive>



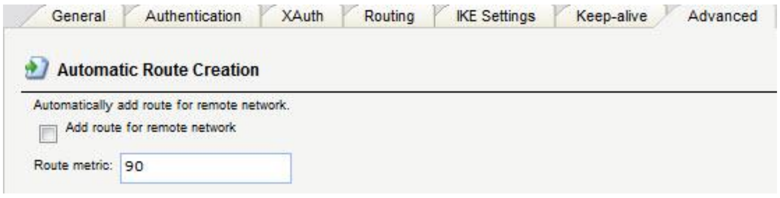
Keep-alive

IPsec keep-alives make sure that an IPsec tunnel stays established at all times by continuously sending ICI
where the remote gateway is a single IP address.

○ Disabled
● Auto
○ Manually configured IP addresses

Keep-alive source IP: (None)
Keep-alive destination IP: (None)

<Advanced>



Automatic Route Creation

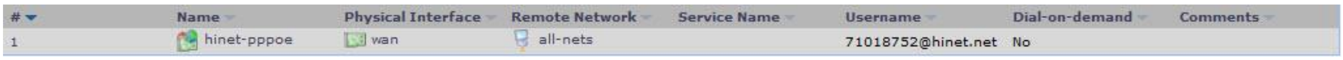
Automatically add route for remote network.

□ Add route for remote network

Route metric: 90

5. Interfaces > PPPoE

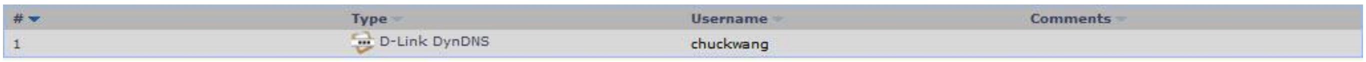
   Create PPPoE interface.



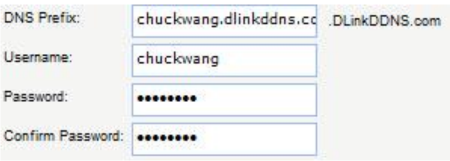
#	Name	Physical Interface	Remote Network	Service Name	Username	Dial-on-demand	Comments
1	hinet-pppoe	wan	all-nets		71018752@hinet.net	No	

6. System > Misc. Clients

   Setup DDNS



#	Type	Username	Comments
1	D-Link DynDNS	chuckwang	



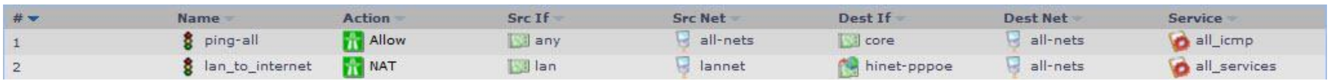
DNS Prefix: chuckwang.dlinkddns.cc .DLinkDDNS.com

Username: chuckwang

Password: ••••••••

Confirm Password: ••••••••

7. Rules > IP Rules



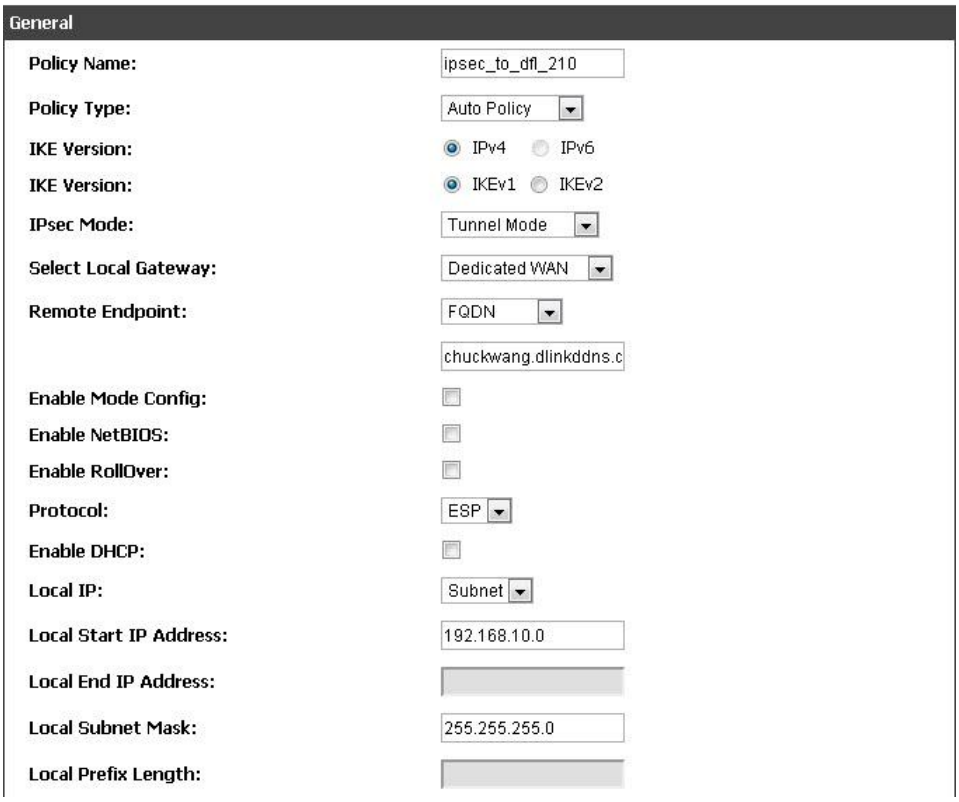
#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	ping-all	Allow	any	all-nets	core	all-nets	all_icmp
2	lan_to_internet	NAT	lan	lannet	hinet-pppoe	all-nets	all_services

[DSR-500N] Firmware: 1.06B55

1. Setup > Internet Settings > WAN1 Settings > WAN1 Status

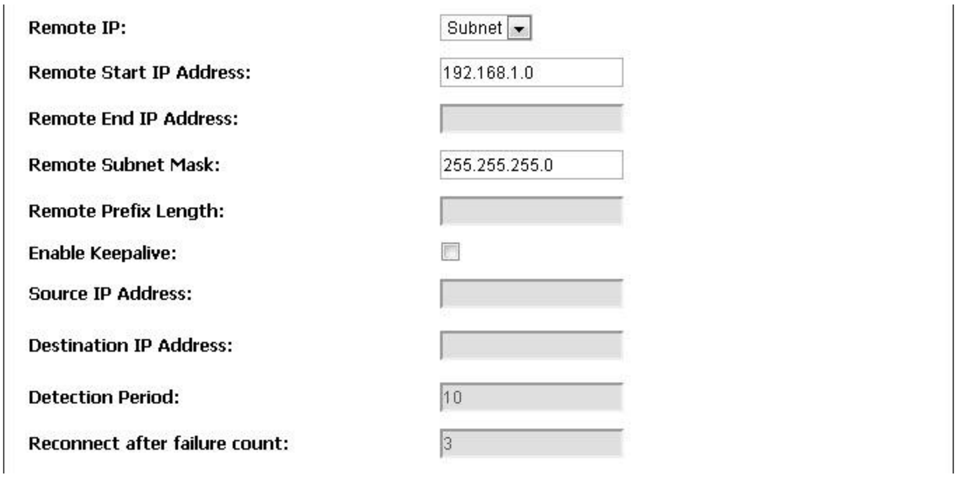
   Setup WAN interfaces IP.

2. Setup > VPN Settings > IPsec > IPsec Policies

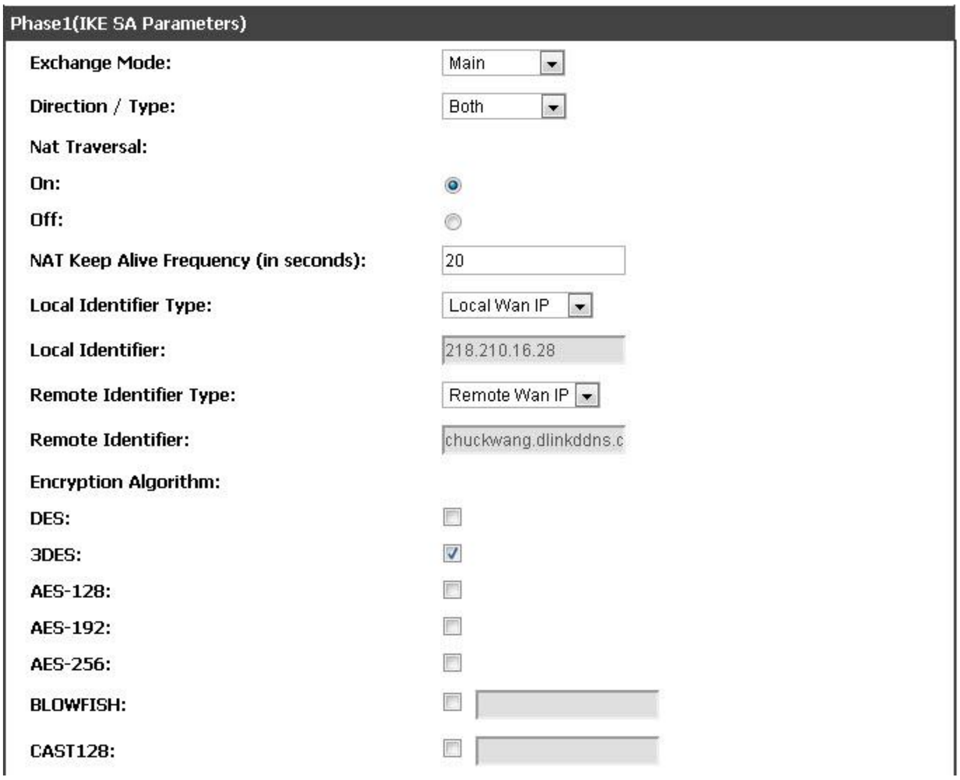


General

Policy Name:	ipsec_to_dfl_210
Policy Type:	Auto Policy
IKE Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	FQDN chuckwang.dlinkddns.c
Enable Mode Config:	□
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	

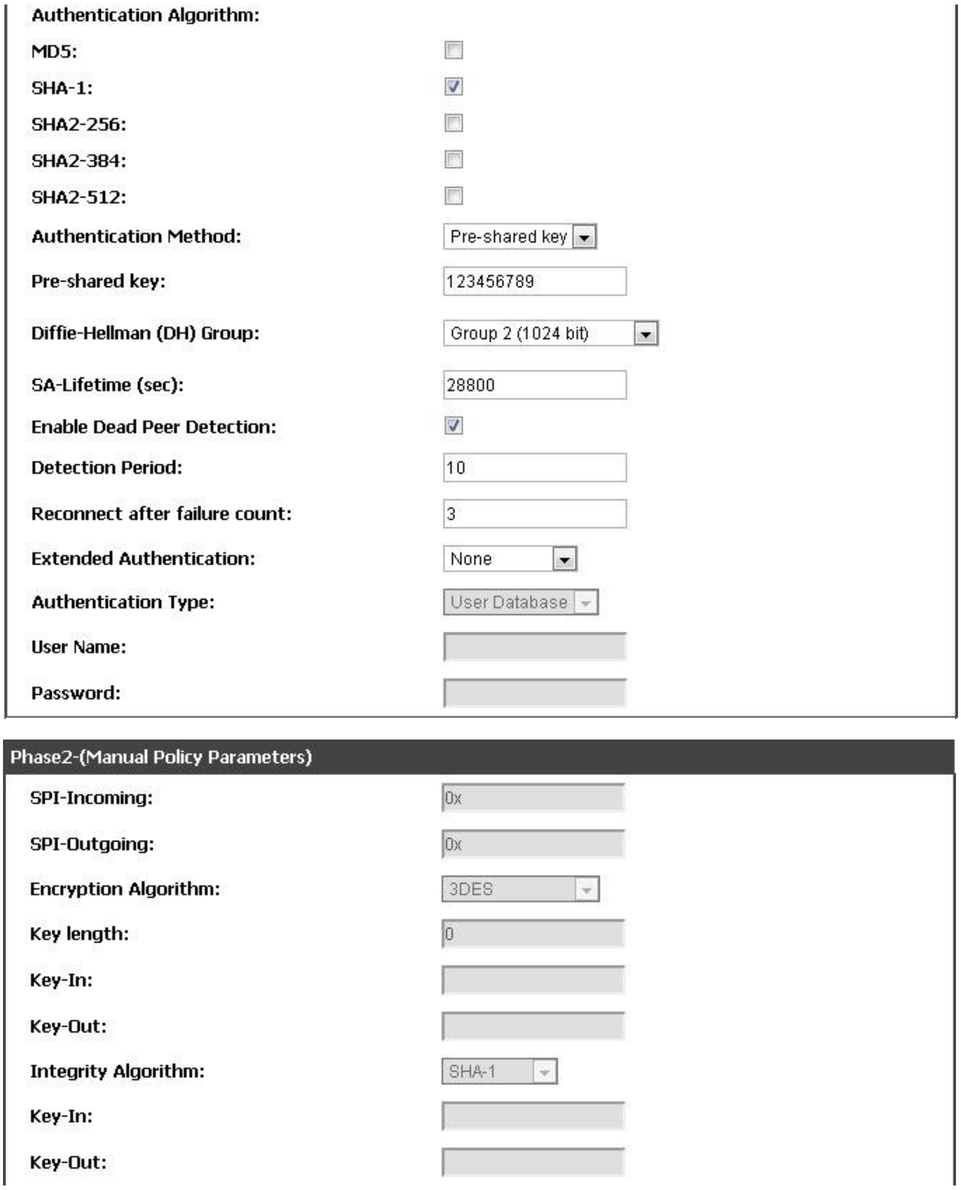


Remote IP:	Subnet
Remote Start IP Address:	192.168.1.0
Remote End IP Address:	
Remote Subnet Mask:	255.255.255.0
Remote Prefix Length:	
Enable Keepalive:	□
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect after failure count:	3



Phase1(IKE SA Parameters)

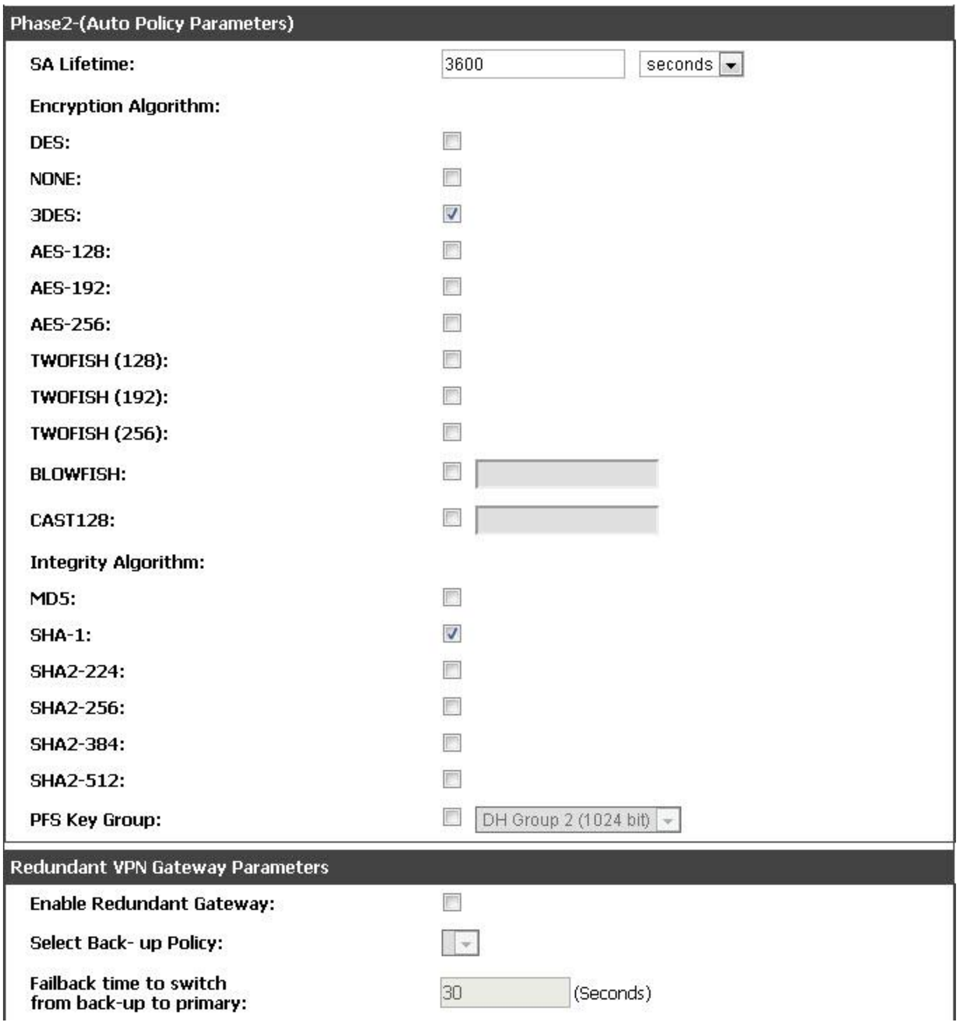
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	218.210.16.28
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	chuckwang.dlinkddns.c
Encryption Algorithm:	
DES:	□
3DES:	☑
AES-128:	□
AES-192:	□
AES-256:	□
BLOWFISH:	□
CAST128:	□



Authentication Algorithm:	
MD5:	☐
SHA-1:	☑
SHA2-256:	☐
SHA2-384:	☐
SHA2-512:	☐
Authentication Method:	Pre-shared key
Pre-shared key:	123456789
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	☑
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None
Authentication Type:	User Database
User Name:	
Password:	

Phase2-(Manual Policy Parameters)

SPI-Incoming:	0x
SPI-Outgoing:	0x
Encryption Algorithm:	3DES
Key length:	0
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1
Key-In:	
Key-Out:	



Phase2-(Auto Policy Parameters)

SA Lifetime:	3600 seconds
Encryption Algorithm:	
DES:	□
NONE:	□
3DES:	☑
AES-128:	□
AES-192:	□
AES-256:	□
TWOFISH (128):	□
TWOFISH (192):	□
TWOFISH (256):	□
BLOWFISH:	□
CAST128:	□
Integrity Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-224:	□
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
PFS Key Group:	□ DH Group 2 (1024 bit)

Redundant VPN Gateway Parameters

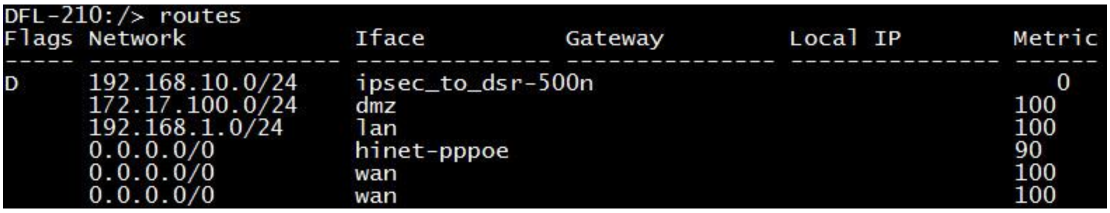
Enable Redundant Gateway:	□
Select Back- up Policy:	
Failback time to switch from back-up to primary:	30 (Seconds)

[Check]

DFL Console:

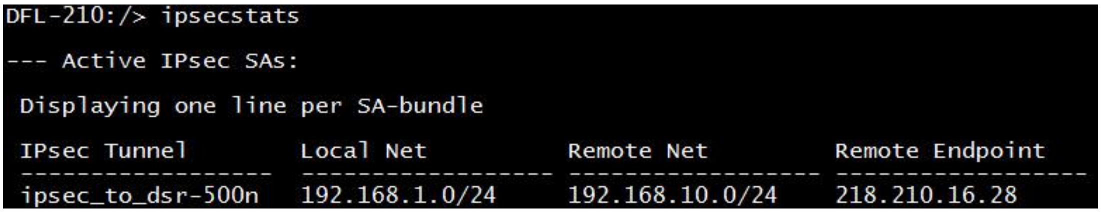
DFL-210:/> routes

You can see the IPsec Dynamic route.



```
DFL-210:/> routes
Flags Network            Iface          Gateway        Local IP       Metric
----- ------------------ -------------- -------------- -------------- ------
D     192.168.10.0/24    ipsec_to_dsr-500n                                 0
      172.17.100.0/24    dmz                                          100
      192.168.1.0/24     lan                                          100
      0.0.0.0/0          hinet-pppoe                                  90
      0.0.0.0/0          wan                                          100
      0.0.0.0/0          wan                                          100
```

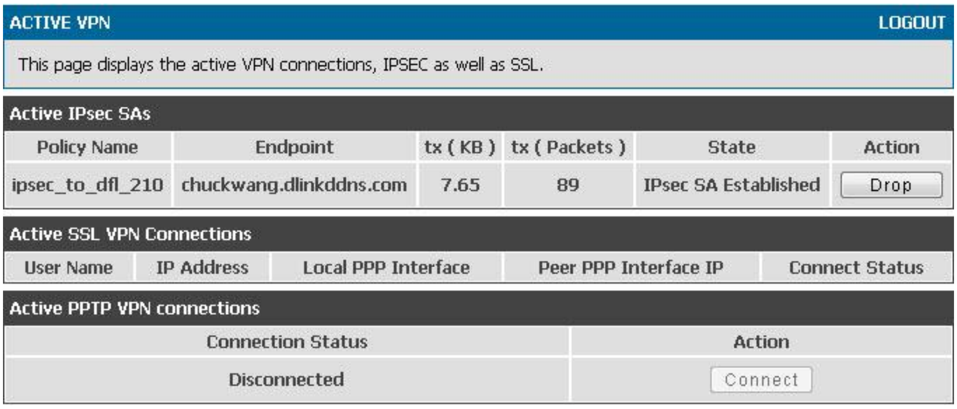
DFL-210:/> ipsecstats



```
DFL-210:/> ipsecstats

--- Active IPsec SAs:

 Displaying one line per SA-bundle

 IPsec Tunnel       Local Net          Remote Net         Remote Endpoint
 ------------------ ------------------ ------------------ ------------------
 ipsec_to_dsr-500n  192.168.1.0/24     192.168.10.0/24    218.210.16.28
```

DSR Web GUI:

Status > Active VPNs



This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action
ipsec_to_dfl_210	chuckwang.dlinkddns.com	7.65	89	IPsec SA Established	Drop

Active SSL VPN Connections

User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status

Active PPTP VPN connections

Connection Status	Action
Disconnected	Connect

[Result]

The tunnel will keep established and both of PC can ping each other.

END