D-Link® CORPORATION

D-Link VPN Application
Quick Installation Guide

Contents

D-Link corporation

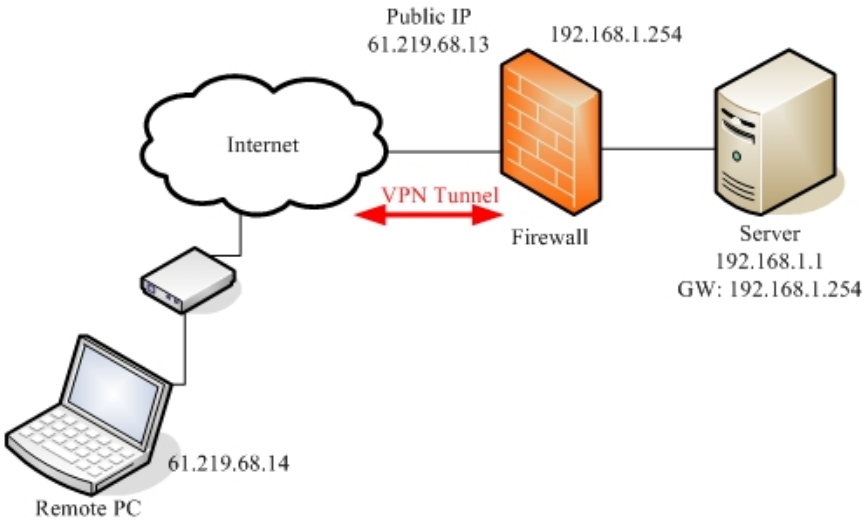
1. Remote Access

1-1 Objective:

Someone is out off office and need to connect back to company by using VPN function (PPTP/L2TP/IPSec).

1-2 Environment:

Configure a Remote Access (PPTP/L2TP/IPSec) VPN Dial-in Connection



1-3 Setup

1-3-1 PPTP Server

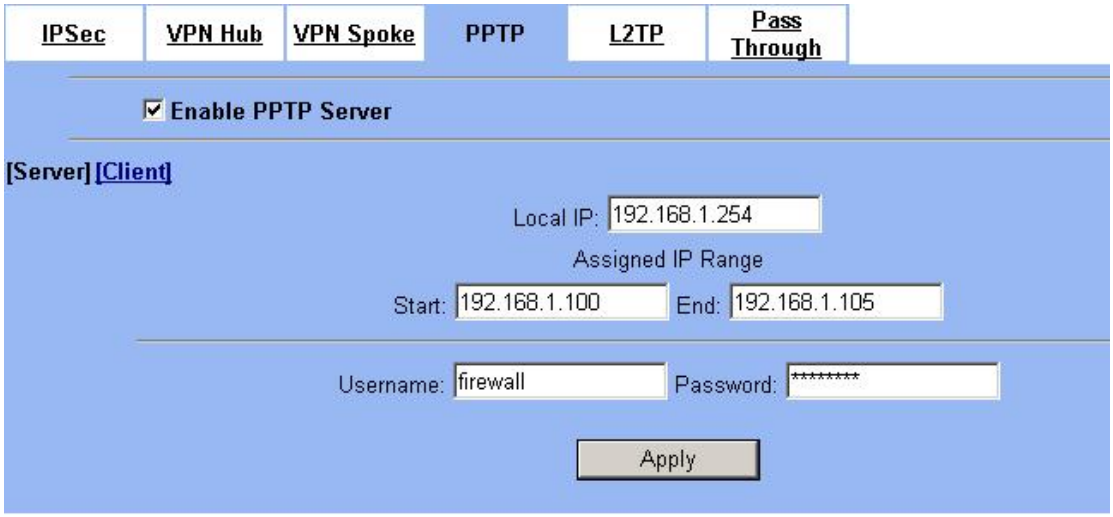
Remote PC settings	Firewall settings
01-Remote IP address: 61.219.68.13 02-VPN type: PPTP 03-Username: firewall 04-Password: firewall	01-Enable PPTP Server 02-Local IP address: 192.168.1.254 03-IP pool: 192.168.1.100~105 04-Username: firewall 05-Password: firewall

D-Link corporation

Device setting page

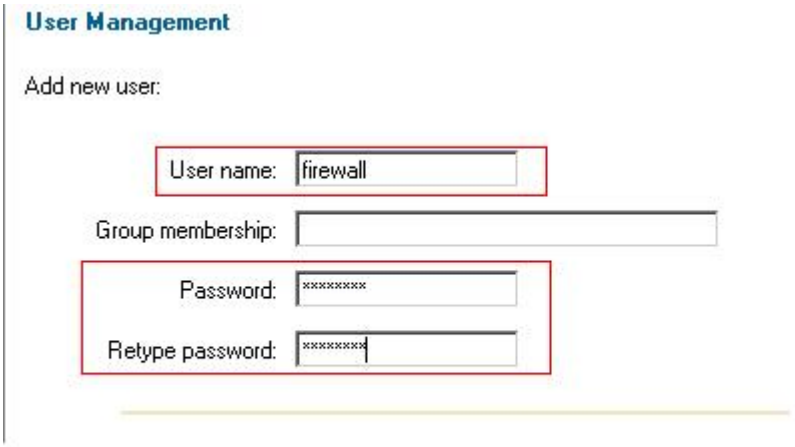
DFL-1500

01- Enable PPTP Server **(Advanced settings -> VPN settings -> PPTP)**



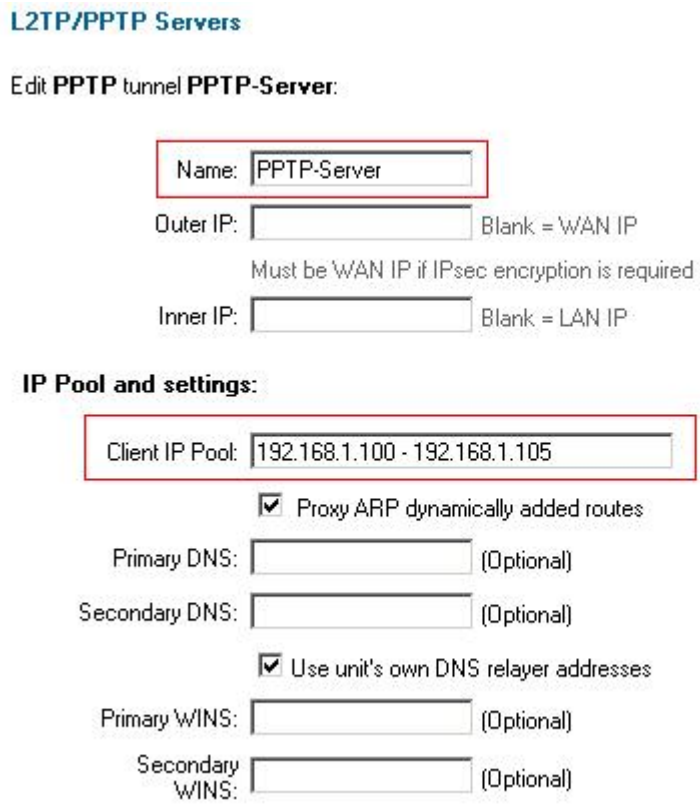
DFL-1100/700/200

01- Add User (**Firewall -> Users**)



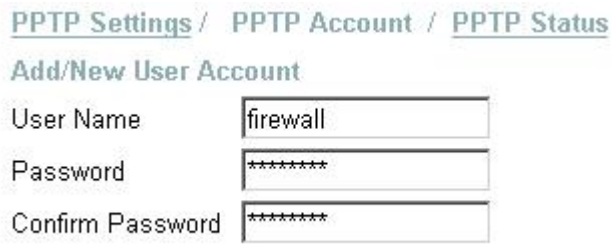
02- Enable PPTP Server (**Firewall -> VPN**)

D-Link corporation

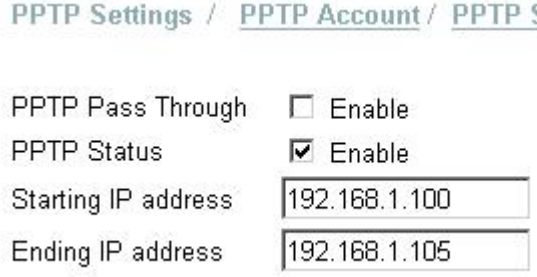


DFL-600

01- Add User (**Advanced -> VPN-PPTP -> PPTP Account**)



02- Enable PPTP Server (**Advanced -> VPN-PPTP -> PPTP settings**)



Configuring PPTP Client (Microsoft XP PRO's VPN adapter)

Setup1

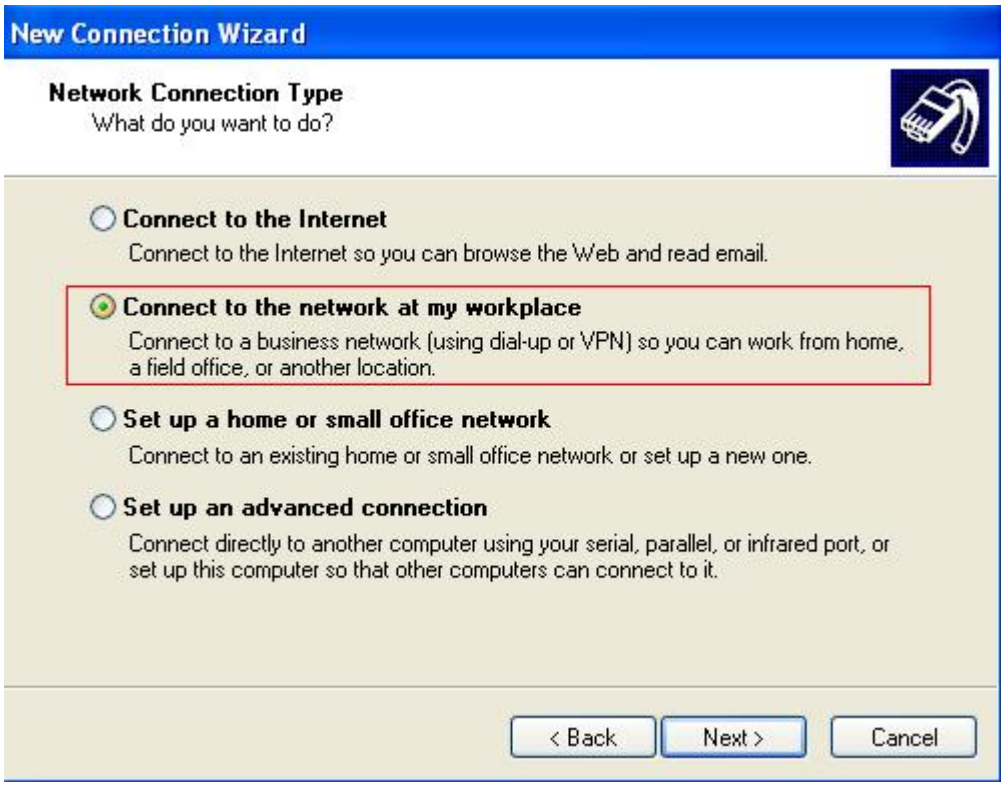
Select "Create a new connection" to create a VPN-PPTP dial out service.

Setup2

Click **Next** to the next step.

Setup3

Check **Connect to the network at my workplace** radio button. Click **Next** to the next step.



Steup4

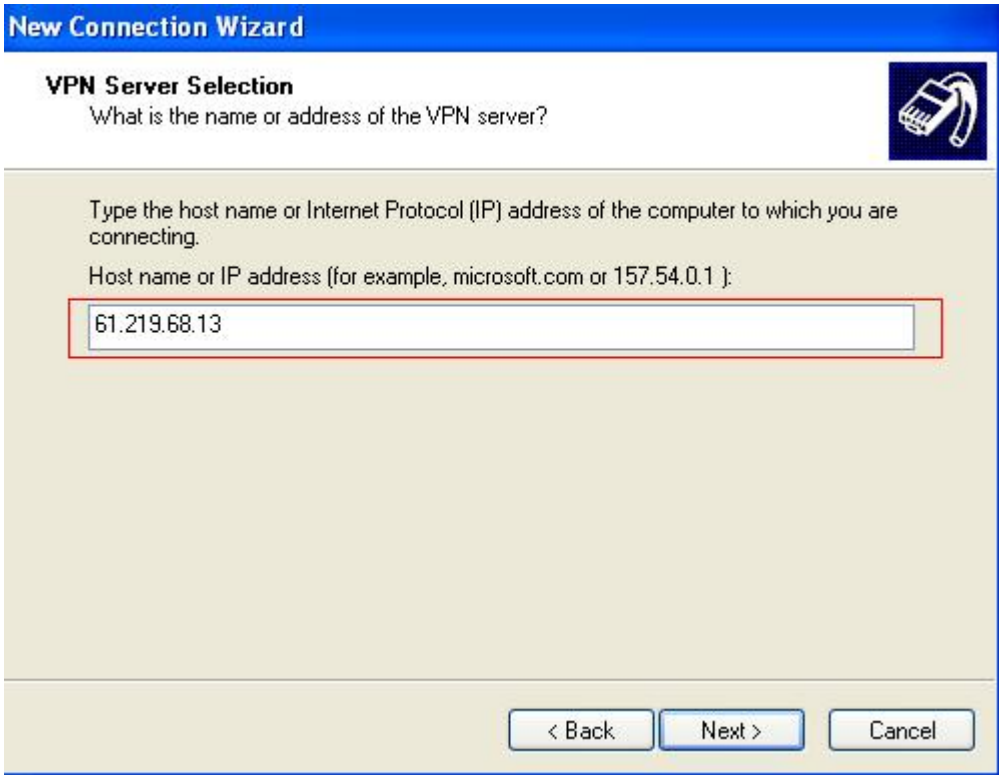
Check **Virtual Private Network connection** radio button. Click **Next** to the next step.

Step5

Give a name to the PPTP connection. Click **Next** to the next step.

Step6

Input VPN-PPTP Server IP address: 61.219.68.13. Click **Next** to the next step.



Step7

Click **Finish** completing VPN-PPTP setting.

Step8

Input your user name and password. Click **Connect** to establish a connection.

1-3-2 L2TP without IPSec

Remote PC settings	Firewall settings

For example: DFL-1500 with Microsoft's VPN adapter (Windows 2K)

1-3-3 IPSec

Remote PC settings	Firewall settings
01- Profile name: test	01- Rule Name: IPSec
02- Communication media: LAN over IP	02- Local IP address: 192.168.1.0/24
03- Gateway: 61.219.68.13	03- Remote IP address: 61.219.68.14
04- IKE policy: DES+MD5	04- Negotiation mode: Main
05- IKE key group: DH2	05- Encapsulation mode: Tunnel
06- IPSec policy: DES+MD5 (ESP)	06- Peers's IP address: 61.219.68.14
07- IPSec key group: DH1	07- PSK: 1234567890
08- Exch_mode: Main	08- IKE policy: DES+MD5
09- Local identity: IP address	09- IKE key group: DH2
10- ID: 61.219.68.14	10- IPSec policy: DES+MD5 (ESP)
11- PSK: 1234567890	11- IPSec key group: DH1
12- Remote Networks: 192.168.1.0/24	
13- Disable firewall settings	

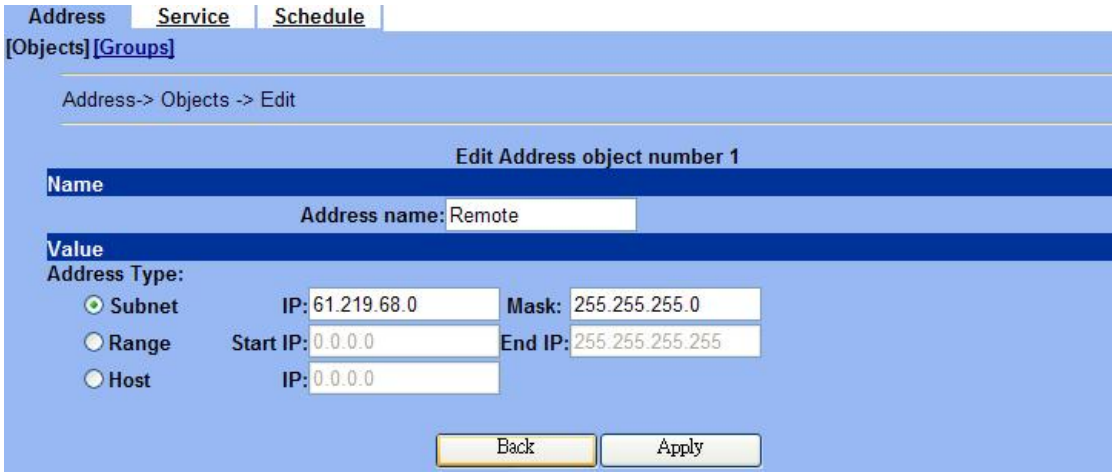
D-Link corporation

Device settings

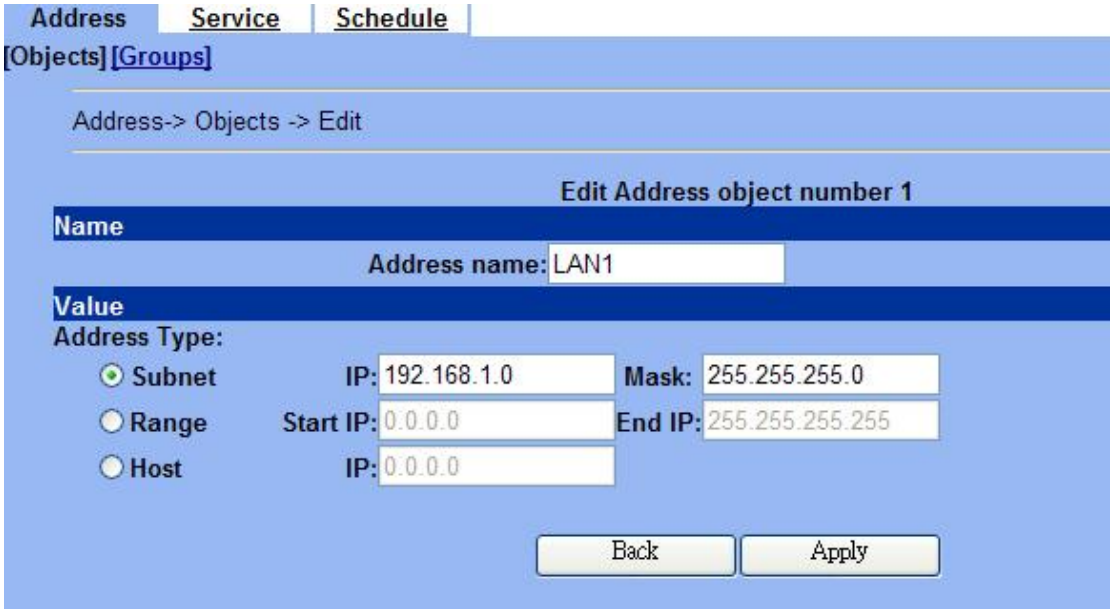
DFL-1500/900

01- Add books (**Basic -> Books**)

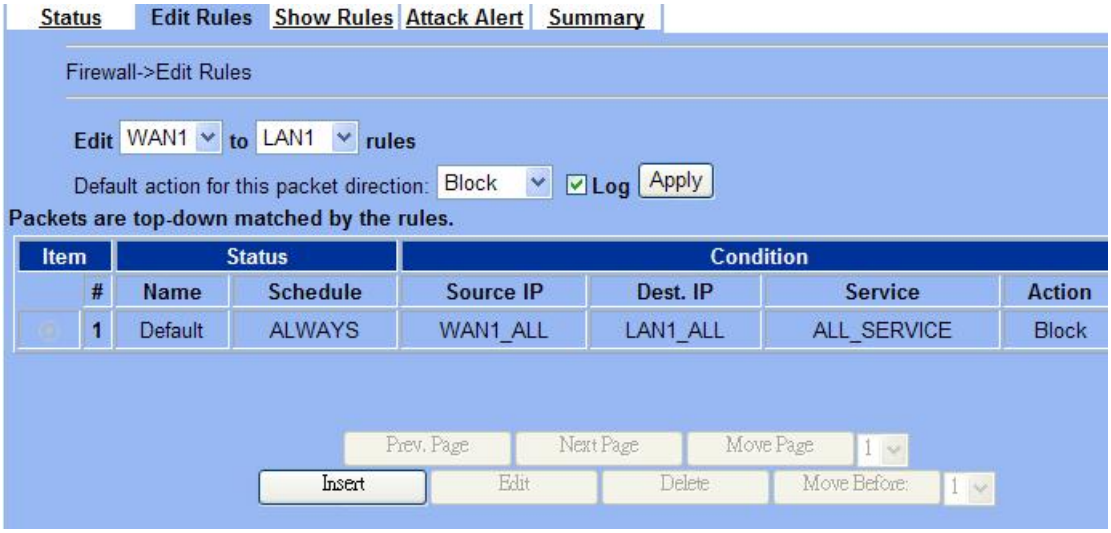
WAN1:

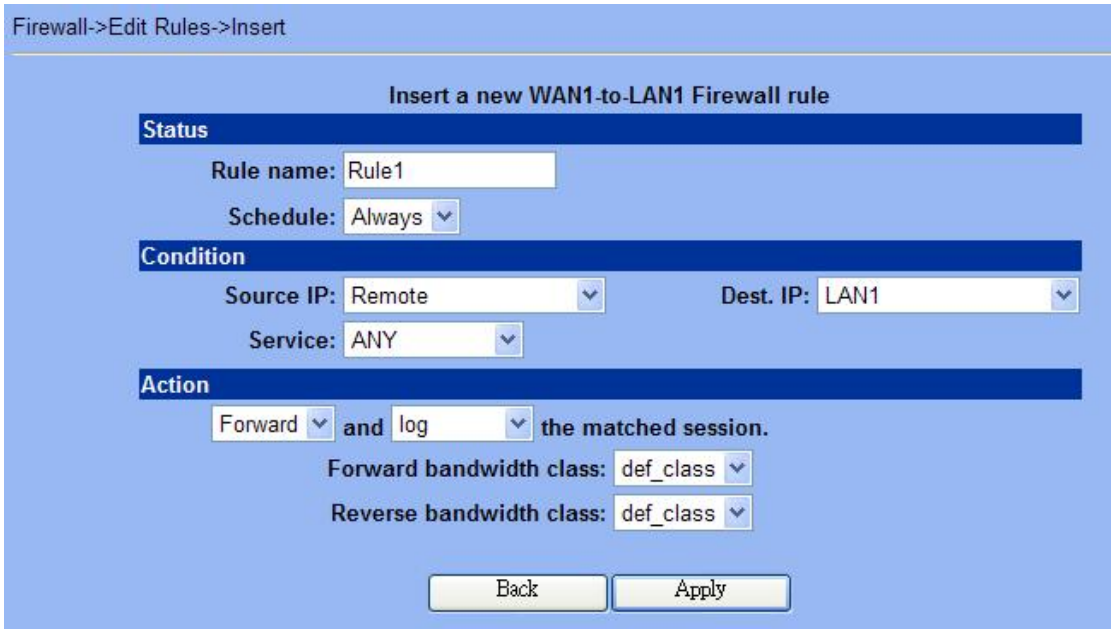


LAN1:

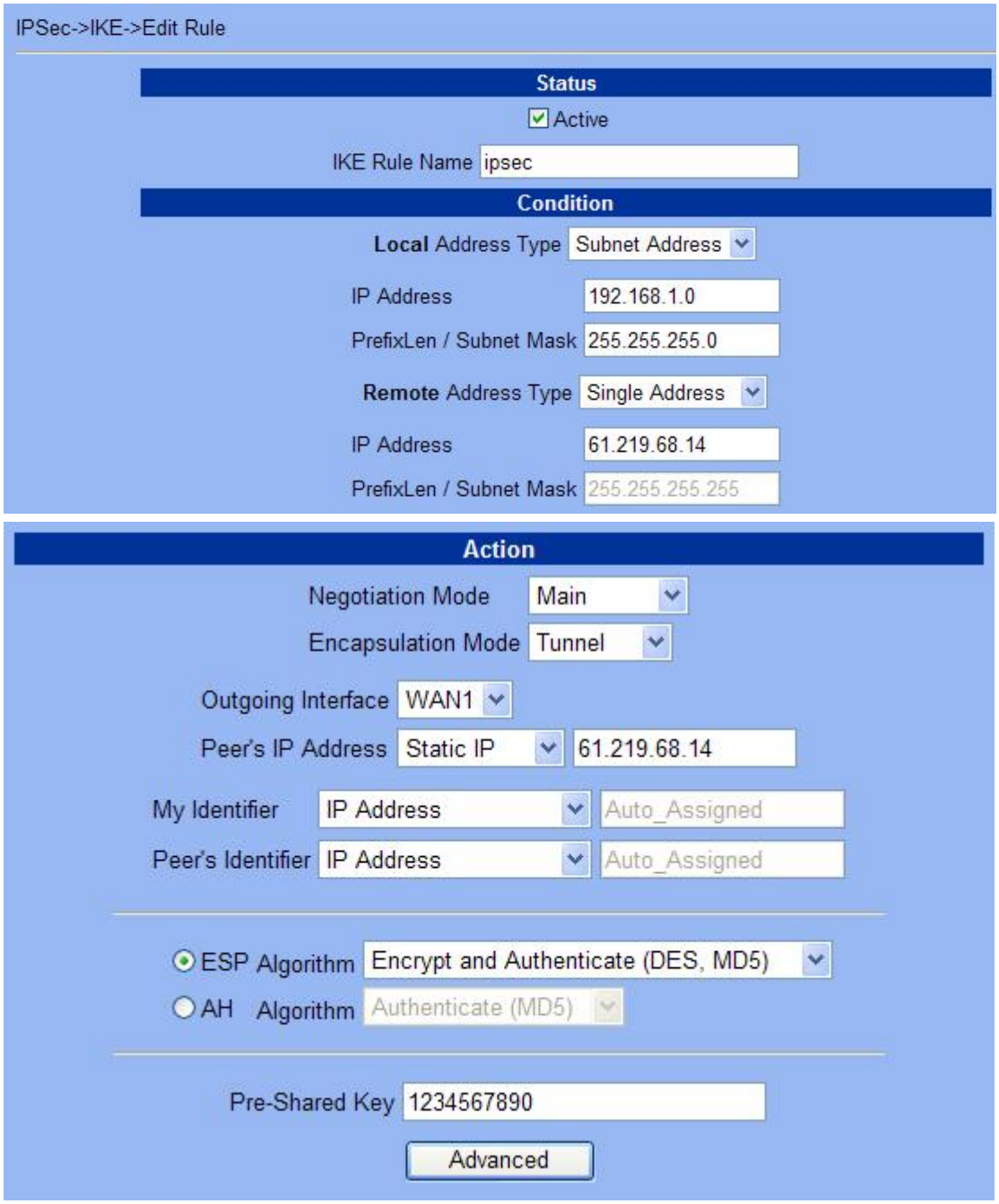


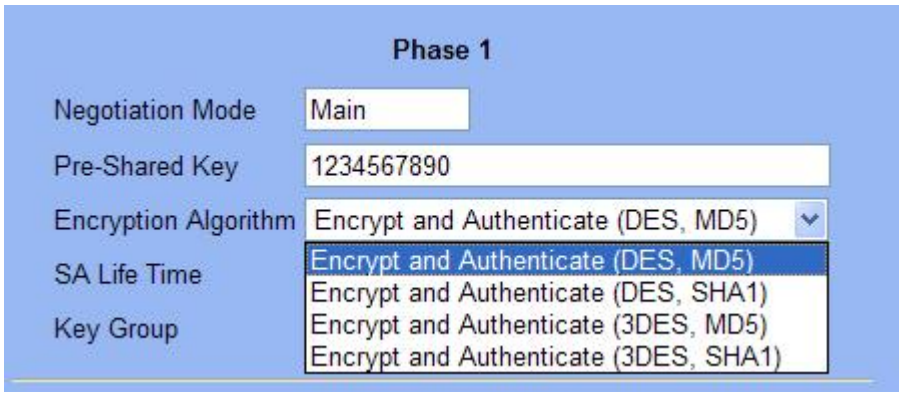
02- Edit Firewall rules (**Advanced Settings -> Firewall -> Edit Rules**)

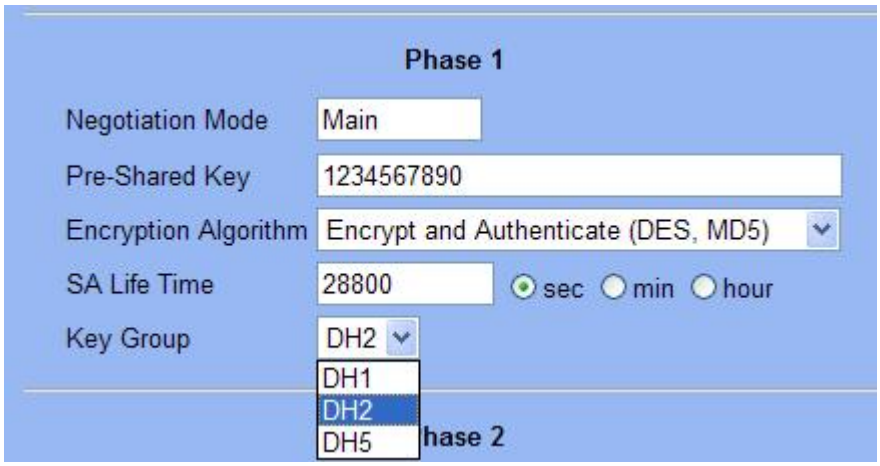


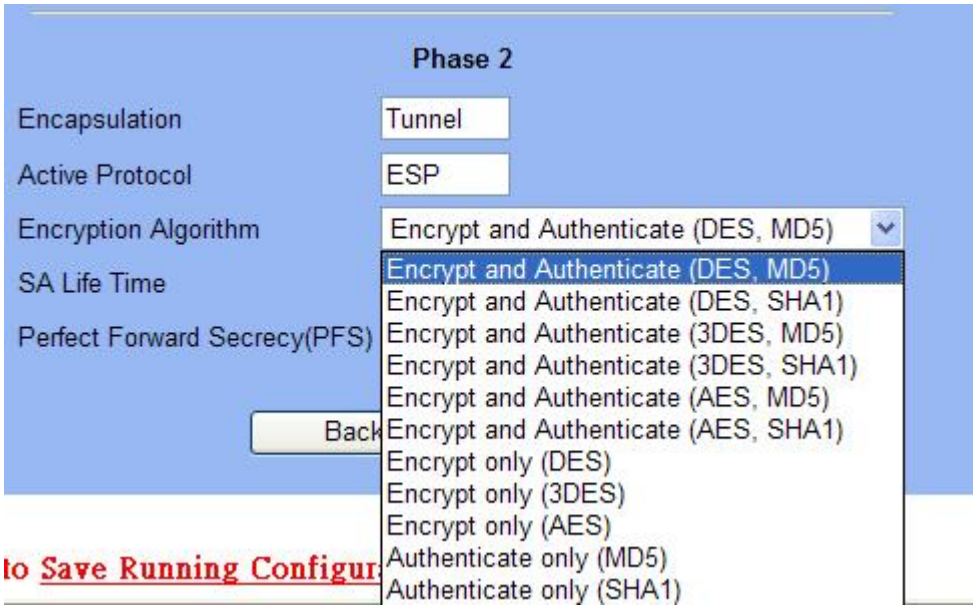


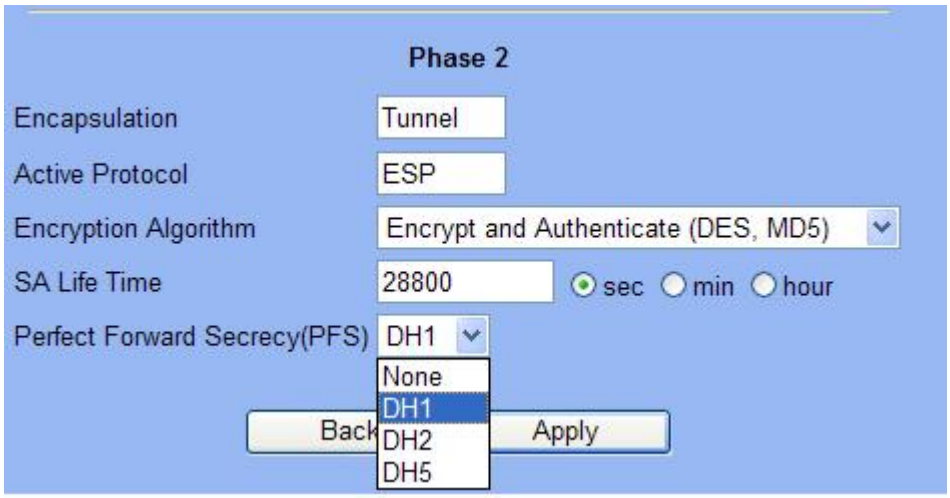
03- Enable IPSec and edit IPSec rule (**Advanced Settings -> VPN Settings**)


IPSec->IKE->Edit Rule
Status
Active
IKE Rule Name ipsec
Condition
Local Address Type Subnet Address
IP Address 192.168.1.0
PrefixLen / Subnet Mask 255.255.255.0
Remote Address Type Single Address
IP Address 61.219.68.14
PrefixLen / Subnet Mask 255.255.255.255
Action
Negotiation Mode Main
Encapsulation Mode Tunnel
Outgoing Interface WAN1
Peer's IP Address Static IP 61.219.68.14
My Identifier IP Address Auto_Assigned
Peer's Identifier IP Address Auto_Assigned
ESP Algorithm Encrypt and Authenticate (DES, MD5)
AH Algorithm Authenticate (MD5)
Pre-Shared Key 1234567890
Advanced


Phase 1
Negotiation Mode Main
Pre-Shared Key 1234567890
Encryption Algorithm Encrypt and Authenticate (DES, MD5)
SA Life Time
Key Group
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)


Phase 1
Negotiation Mode
Main
Pre-Shared Key
1234567890
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Key Group
DH2
DH1
DH2
DH5
hase 2

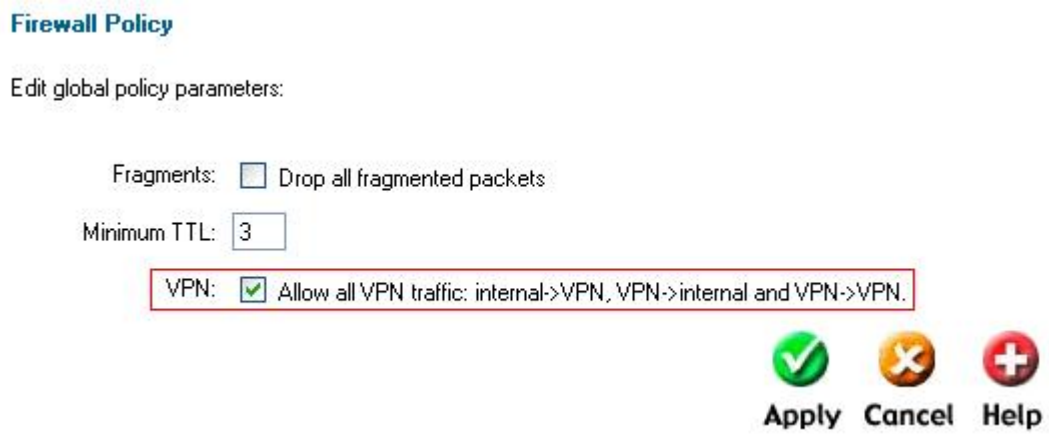

Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
Perfect Forward Secrecy(PFS)
Back
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)
Encrypt and Authenticate (AES, MD5)
Encrypt and Authenticate (AES, SHA1)
Encrypt only (DES)
Encrypt only (3DES)
Encrypt only (AES)
Authenticate only (MD5)
Authenticate only (SHA1)
lo Save Running Configur


Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Perfect Forward Secrecy(PFS)
DH1
None
DH1
DH2
DH5
Back
Apply

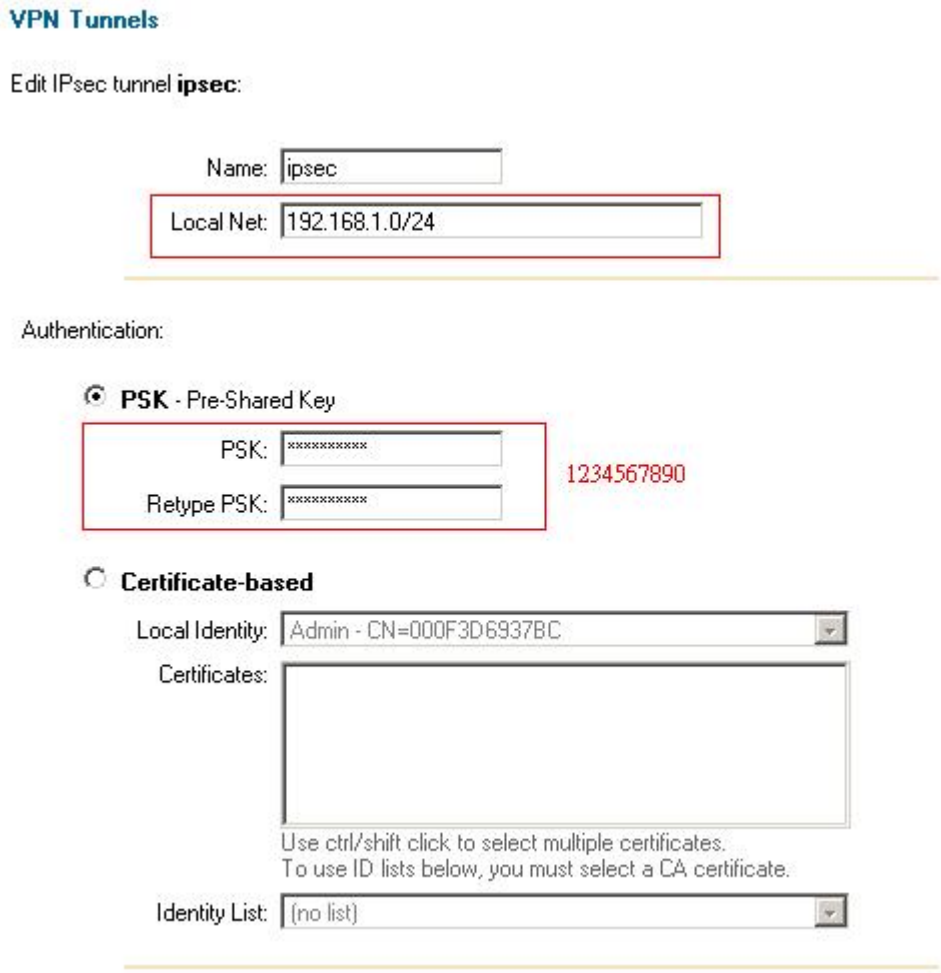
D-Link corporation

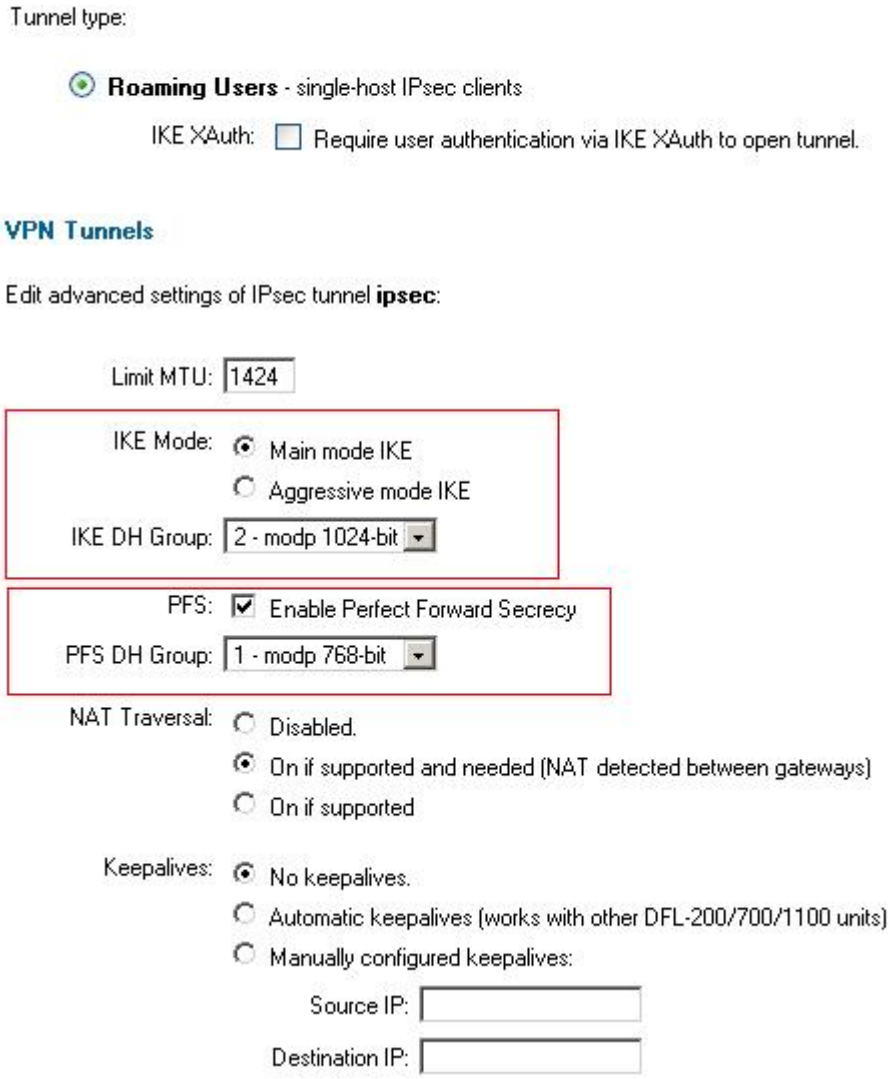
DFL-1100/700/200

01- Enable allow all VPN traffic (**Firewall -> Policy**)

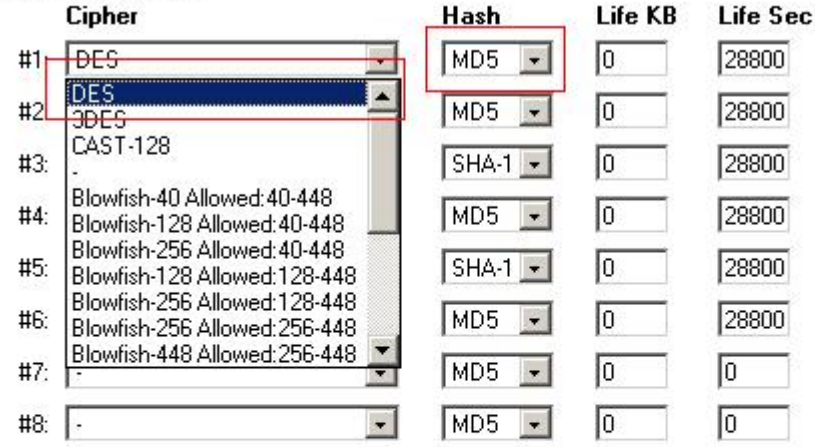


02- Enable IPSec and edit IPSec rule (**Firewall -> VPN -> IPSec Tunnels**)

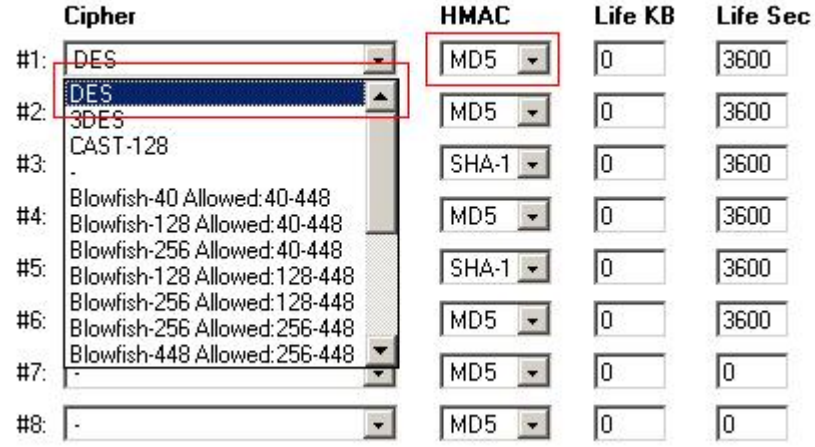



Tunnel type:
Roaming Users - single-host IPsec clients
IKE XAuth: Require user authentication via IKE XAuth to open tunnel.
VPN Tunnels
Edit advanced settings of IPsec tunnel ipsec:
Limit MTU: 1424
IKE Mode: Main mode IKE
Aggressive mode IKE
IKE DH Group: 2 - modp 1024-bit
PFS: Enable Perfect Forward Secrecy
PFS DH Group: 1 - modp 768-bit
NAT Traversal: Disabled.
On if supported and needed (NAT detected between gateways)
On if supported
Keepalives: No keepalives.
Automatic keepalives (works with other DFL-200/700/1100 units)
Manually configured keepalives:
Source IP:
Destination IP:

IKE Proposal List



IPsec Proposal List

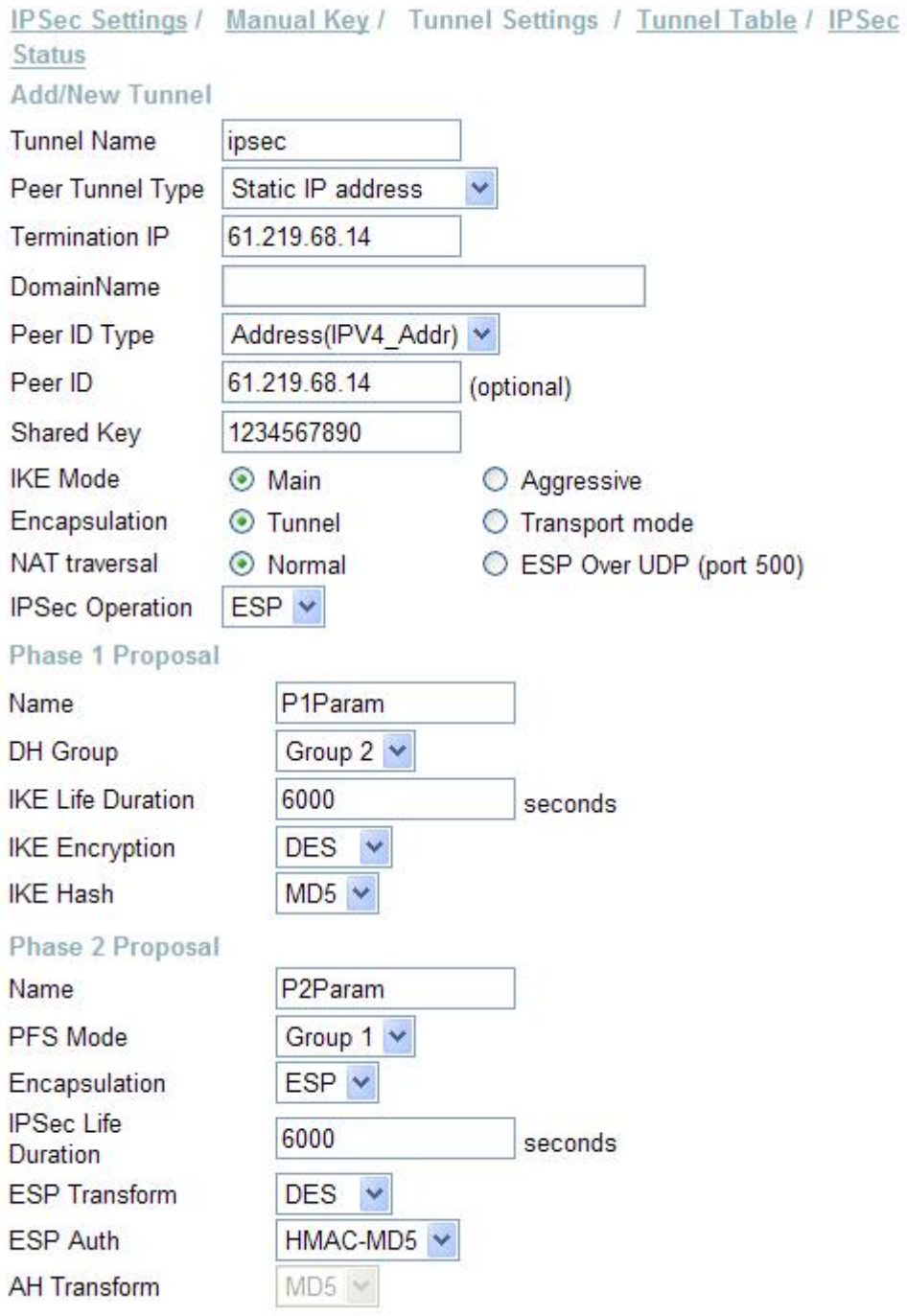


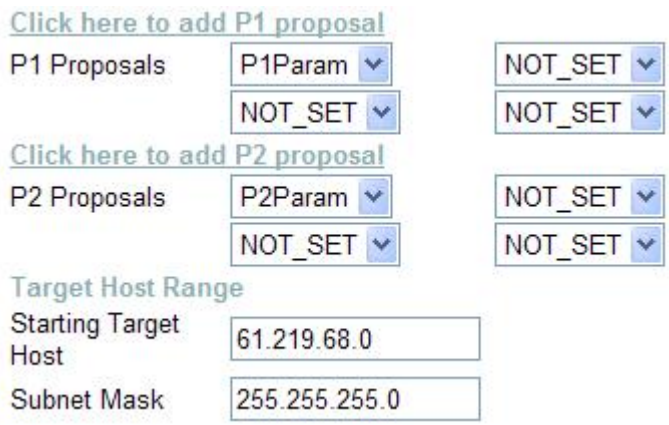
D-Link corporation

DFL-600

01- Enable allow all VPN traffic (**Advanced -> Policy -> Global Policy Status)**

02- Enable IPSec and edit IPSec rule (**Firewall -> VPN -> IPSec Tunnels**)




Click here to add P1 proposal
P1 Proposals
P1Param
NOT_SET
NOT_SET
NOT_SET
Click here to add P2 proposal
P2 Proposals
P2Param
NOT_SET
NOT_SET
NOT_SET
Target Host Range
Starting Target Host
61.219.68.0
Subnet Mask
255.255.255.0

Configuring IPSec connection (D-Link DS-601)

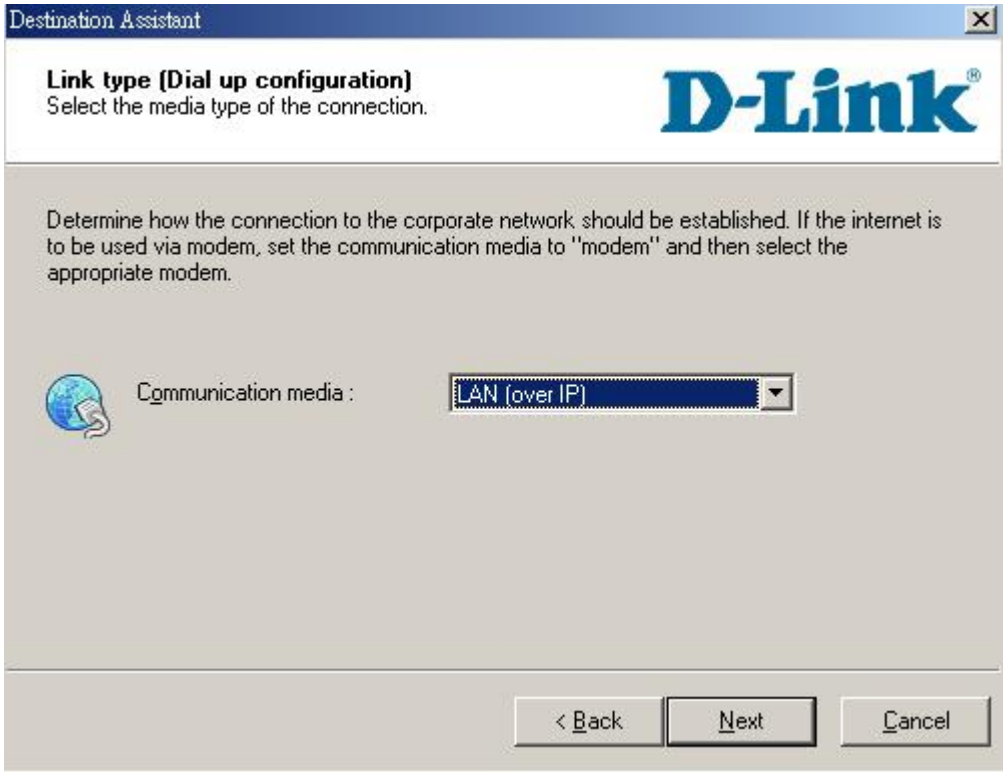
Setup1

Configuration->Profile settings->New Entry

Input your **profile name** and click **Next** button

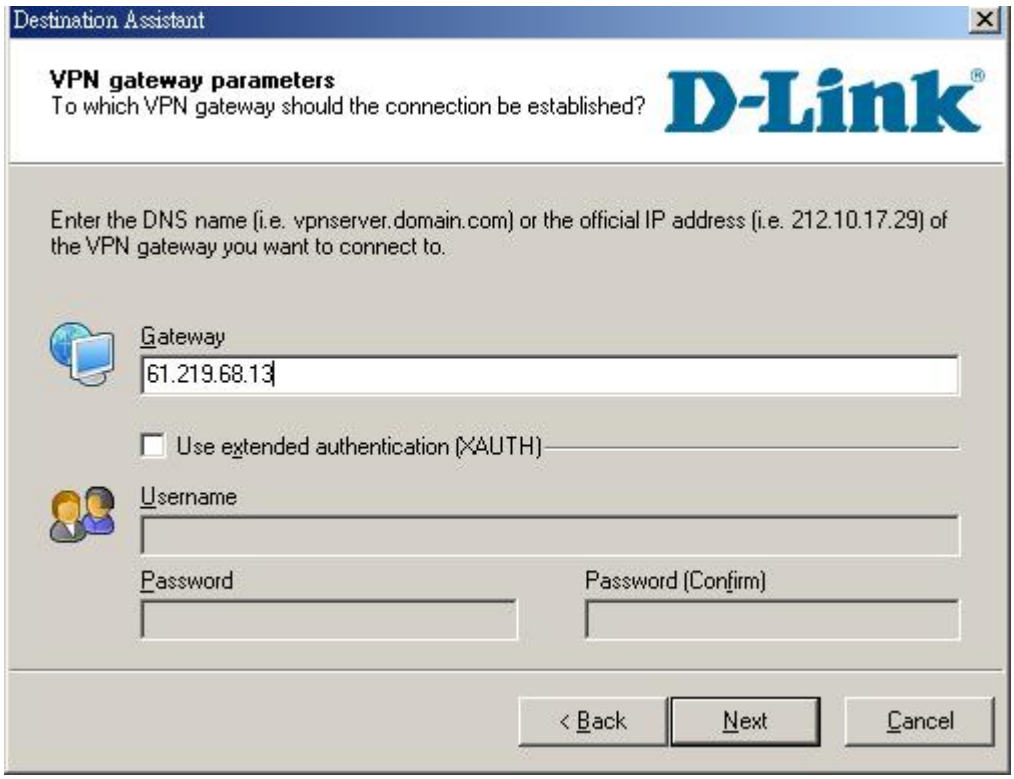
Setup2

Select Communication media as **LAN over IP** and click **Next** Button



Setup3

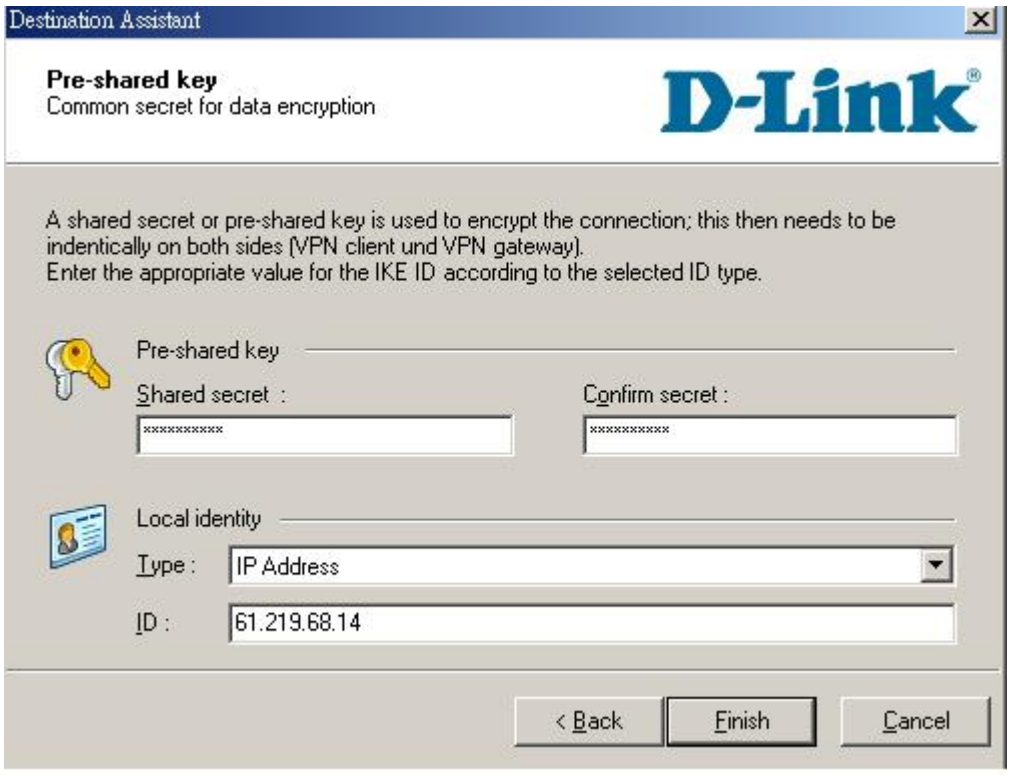
Input VPN gateway (**61.219.68.13**) and click **Next** button



Setup4

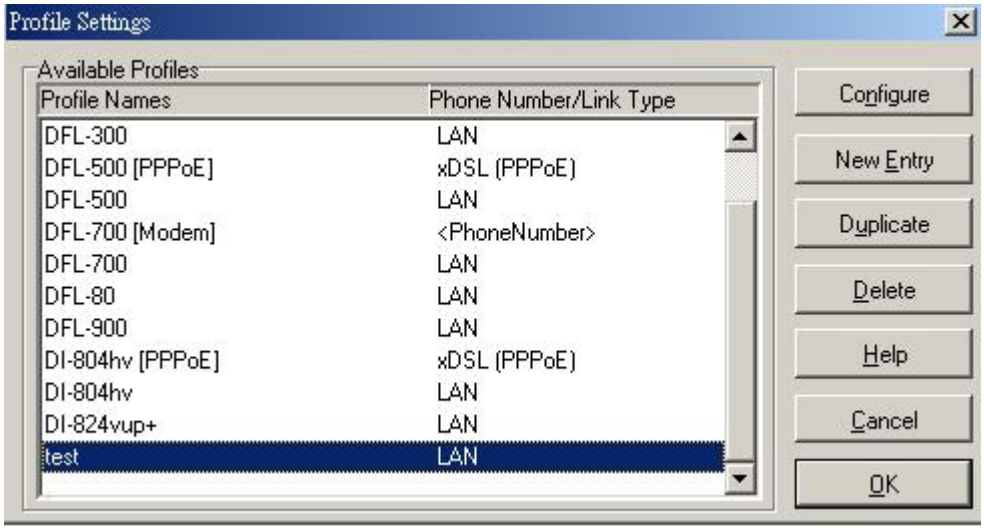
Input 1234567890 in the **Shared secret** and retype it in the **Confirm secret.**

Input your local IP address in the **Local identity,** and click **Finish** button.



Setup5

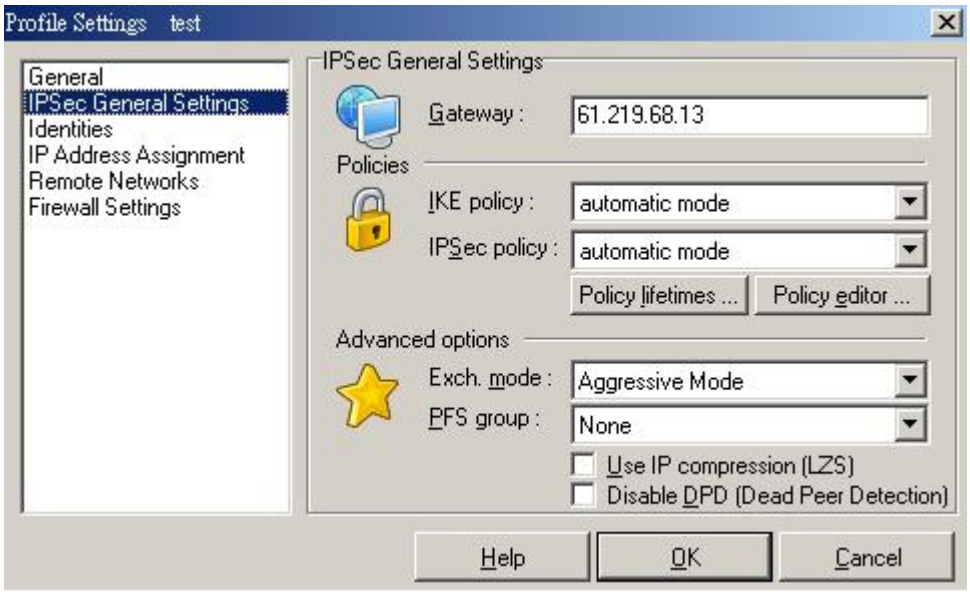
After finishing the previous wizard, you can find out that add a new profile here.

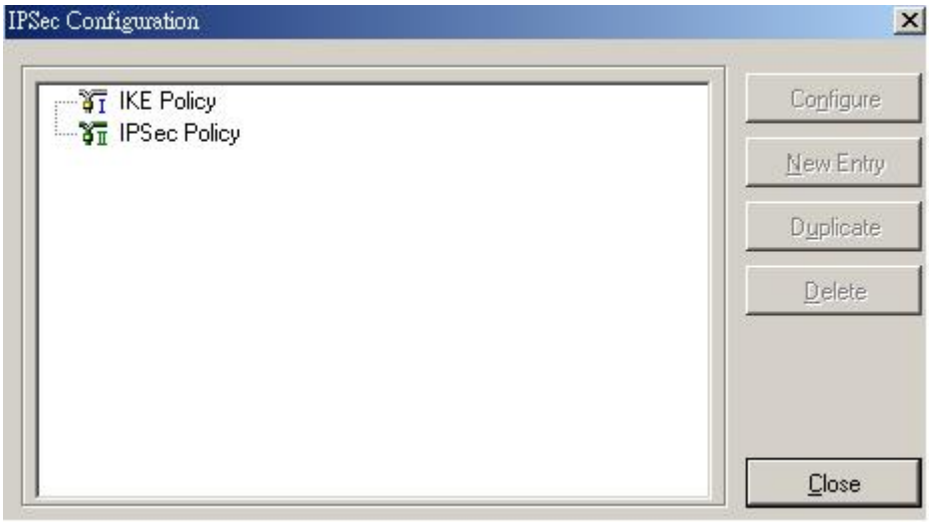


Setup6

Configuration->Profile settings->test->IPSec General Settings

Click **Policy editor** to edit IPSec and IKE policy

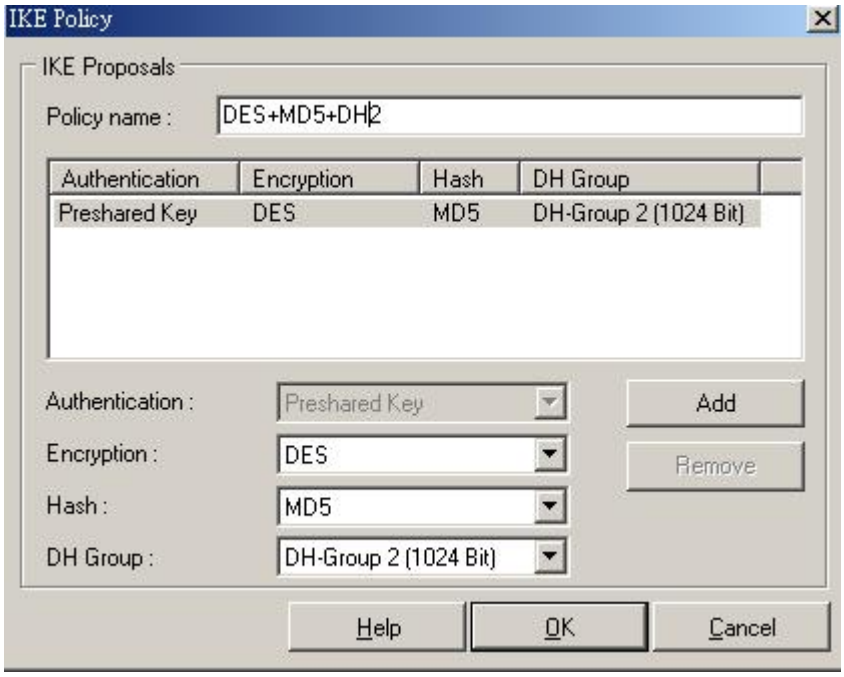




Setup7

Click **IKE Policy->New Entry**, enter DES+MD5+DH2 as the IKE policy name.

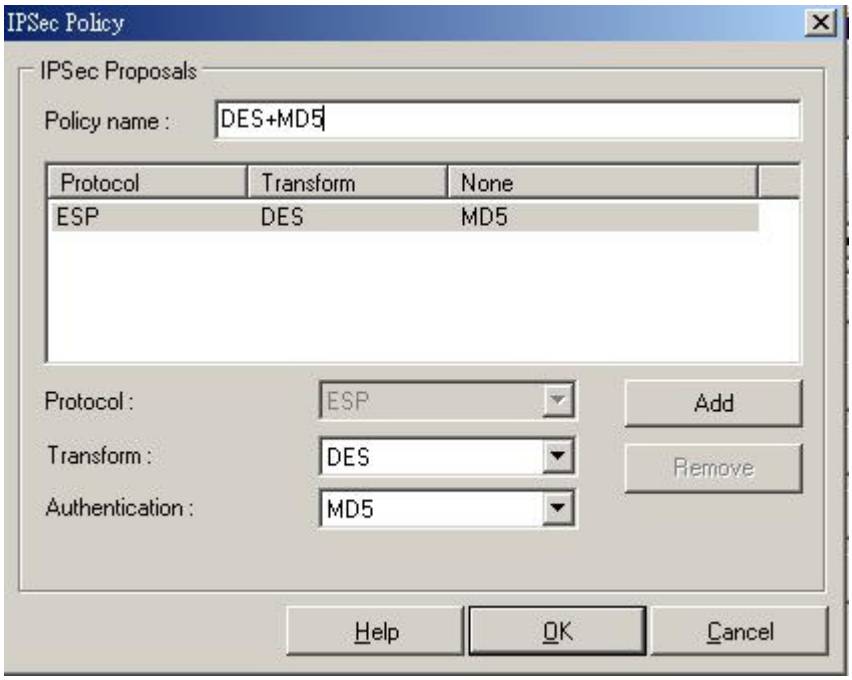
Select **Encryption** as DES, **Hash** as MD5, **DH group** as DH2 and click **OK** button.



Setup8

Click **IPSec Policy->New Entry**, enter DES+MD5 as the IPSec policy name.

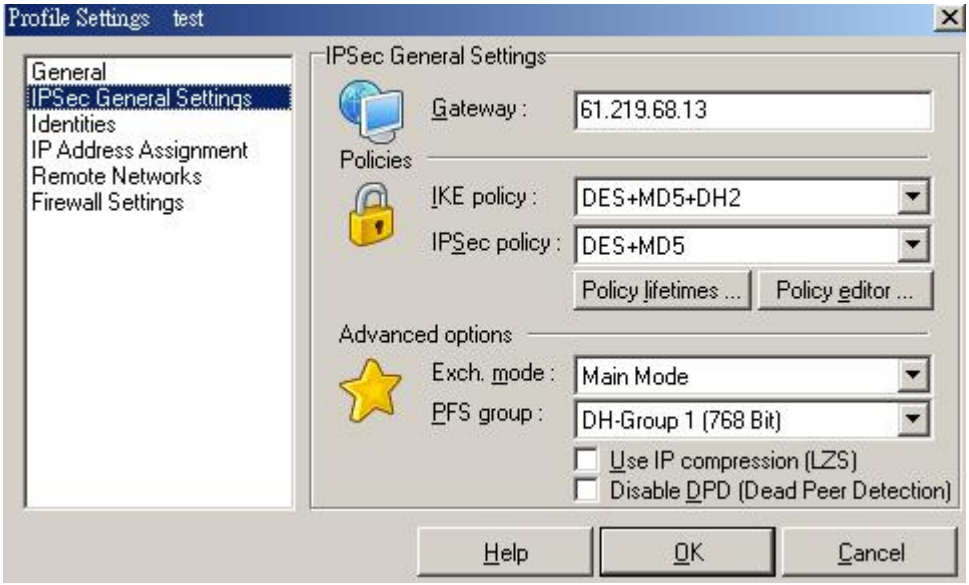
Select **Transform** as DES, **Authentication** as MD5 and click OK button.



Setup9

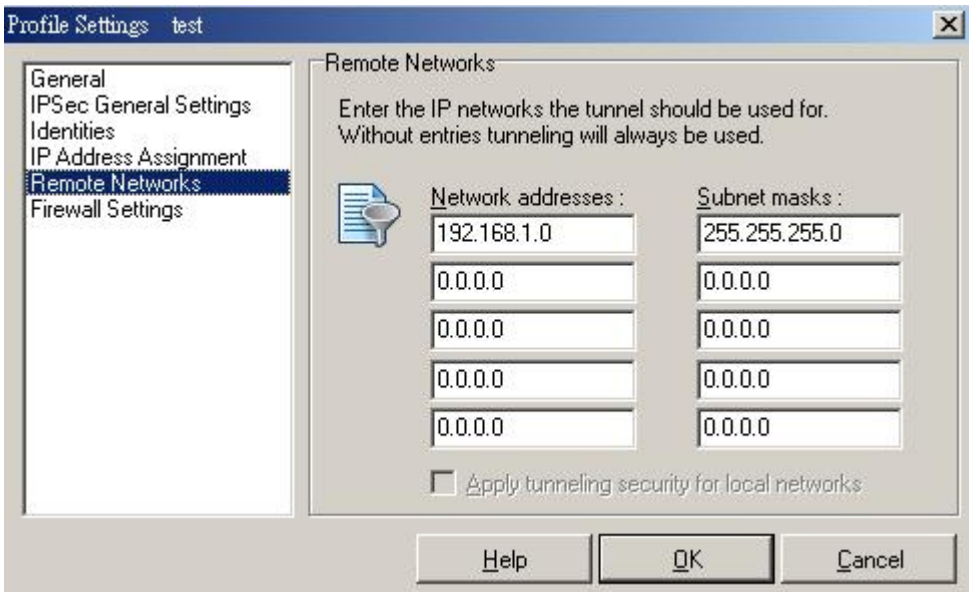
Configuration->Profile settings->test->IPSec General Settings

Select **IKE policy** as DES+MD5+DH2, **IPSec policy** as DES+MD5, **Exch. mode** as Main Mode, **PFS group** as DH-1



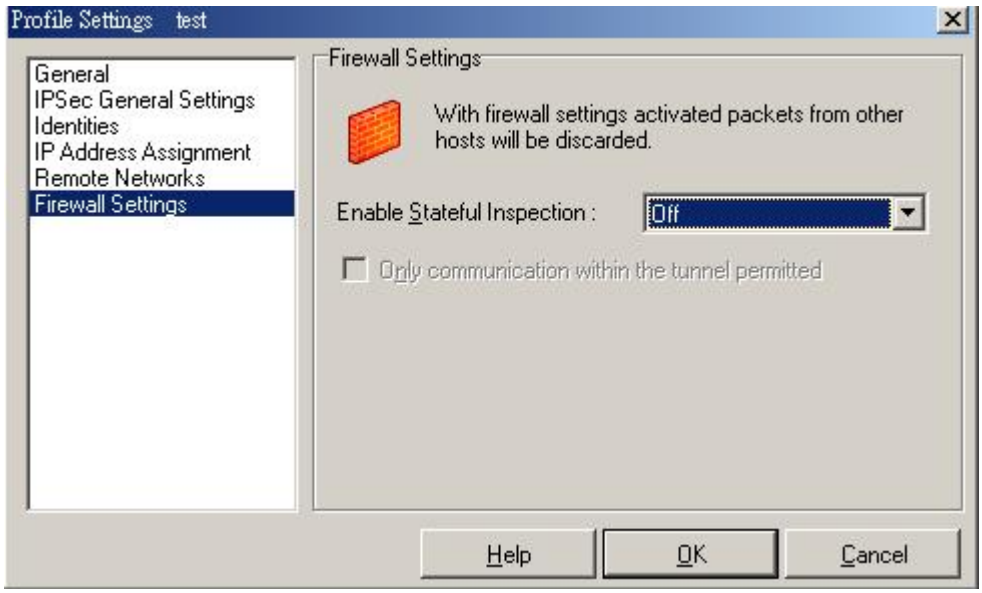
Setup10

Setup **Remote Networks**, enter **Network address** as 192.168.1.0 and **Subnet masks** as 255.255.255.0



Setup11

Setup Firewall settings, select **Enable Stateful Inspection** as off and click **OK** button.



Setup12

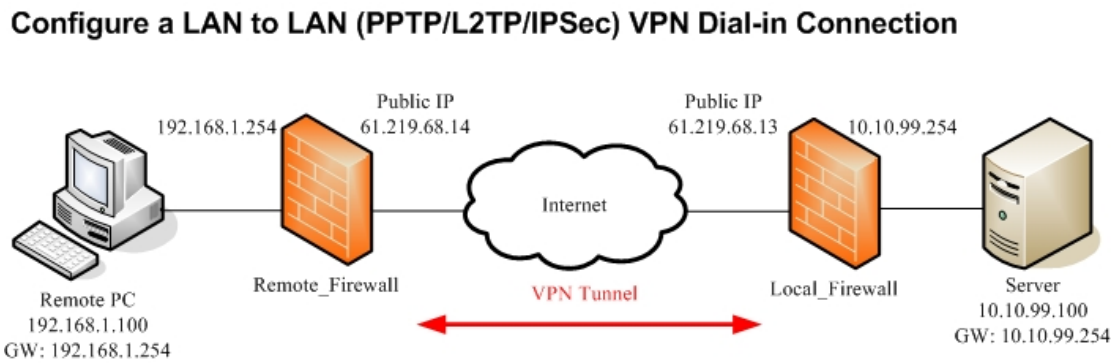
Click **Connect** button to establish IPSec tunnel

2. LAN to LAN

2-1 Objective:

When a branch office wants to connect with another branch office through the Internet.

2-2 Environment:



2-3 Setups:

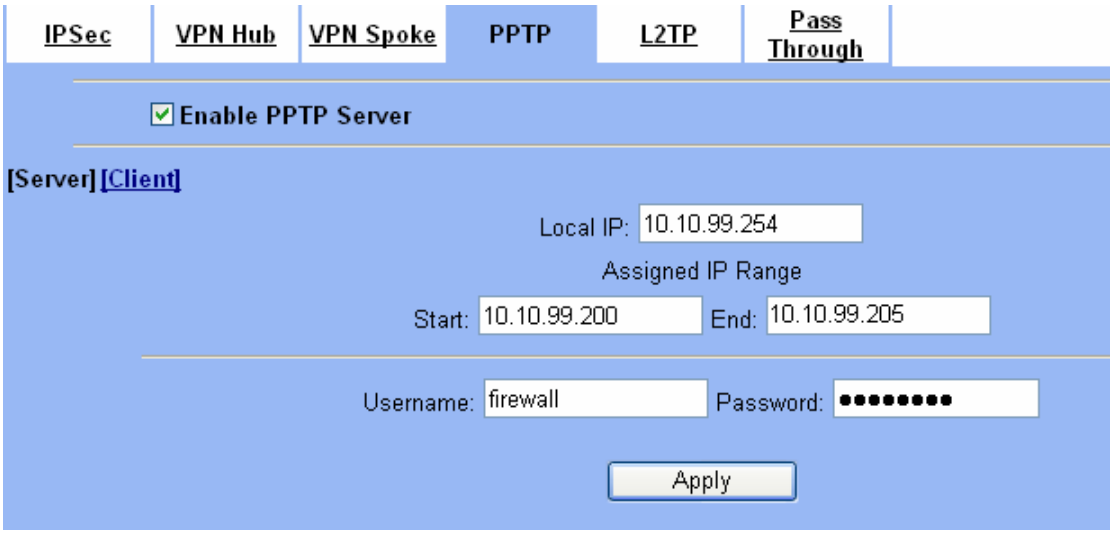
2-3-1 PPTP Server & PPTP Client

Remote_Firewall settings	Local_Firewall settings
01- Enable PPTP Client	01- Enable PPTP Server
02- Server IP address: 61.219.68.13	02- Local IP address: 10.10.99.254
03- Username: firewall	03- IP pool: 10.10.99.200-205
04- Password: firewall	04- Username: firewall
	05- Password: firewall

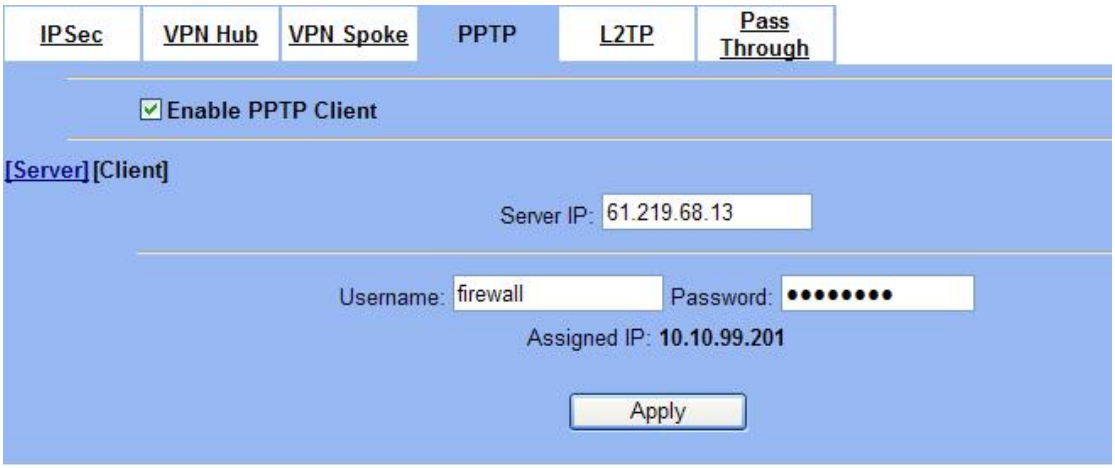
D-Link corporation

DFL-1500

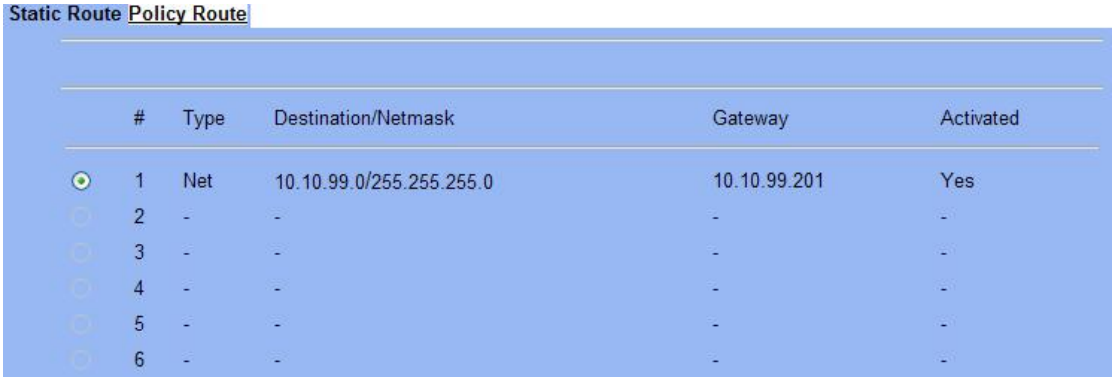
01- Enable PPTP Server (**Advanced settings -> VPN settings -> PPTP**)



02- Enable PPTP Client (**Advanced settings -> VPN settings -> PPTP -> Client**)



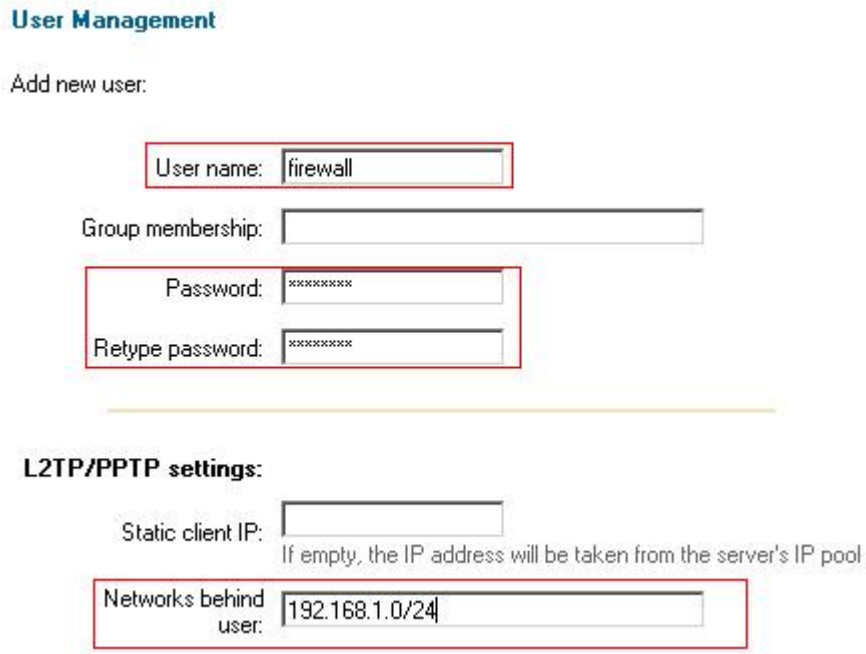
03- Add a static routing table (**Advanced settings -> Routing -> Static Route**)



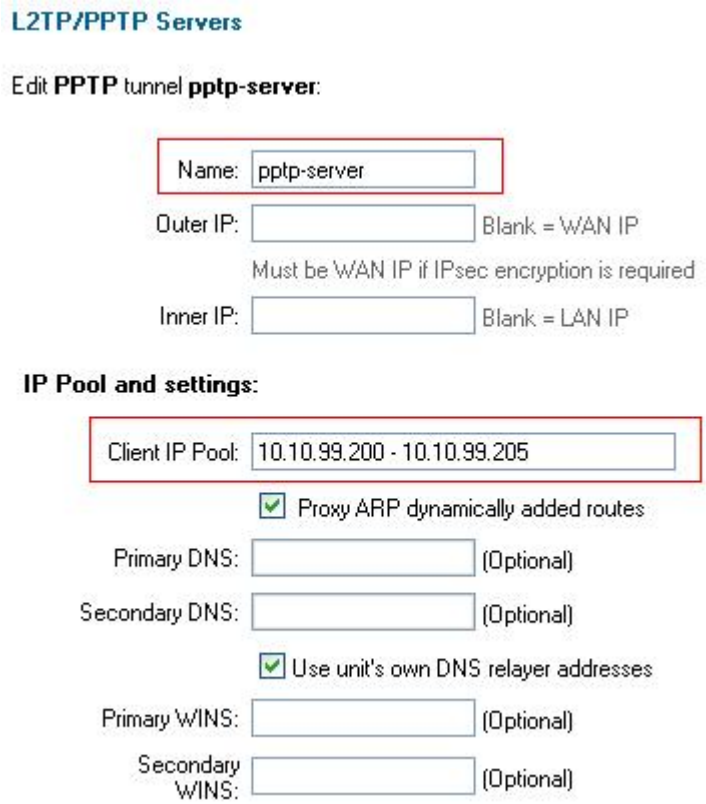
D-Link corporation

DFL-1100/700/200

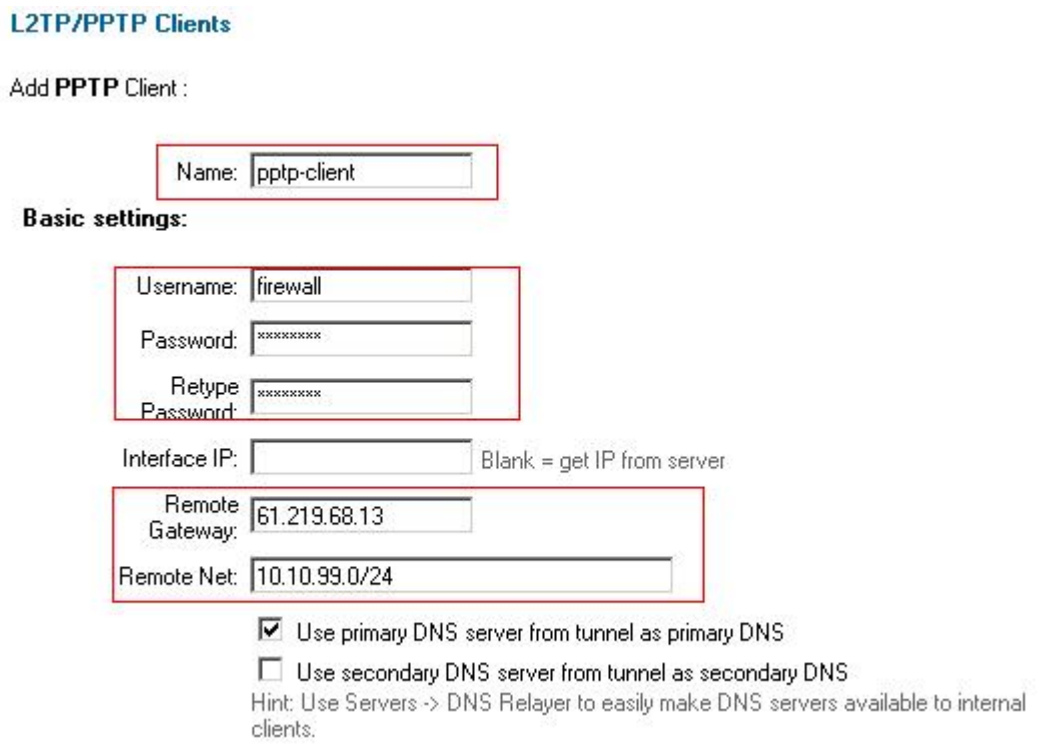
01- Add User (**Firewall -> Users**)



02- Enable PPTP Server (**Firewall -> VPN**)



03- Enable PPTP Client (**Firewall -> VPN**)



2-3-2 L2TP Server & L2TP Client

Remote_Firewall settings	Local_Firewall settings

2-3-3 IPSec

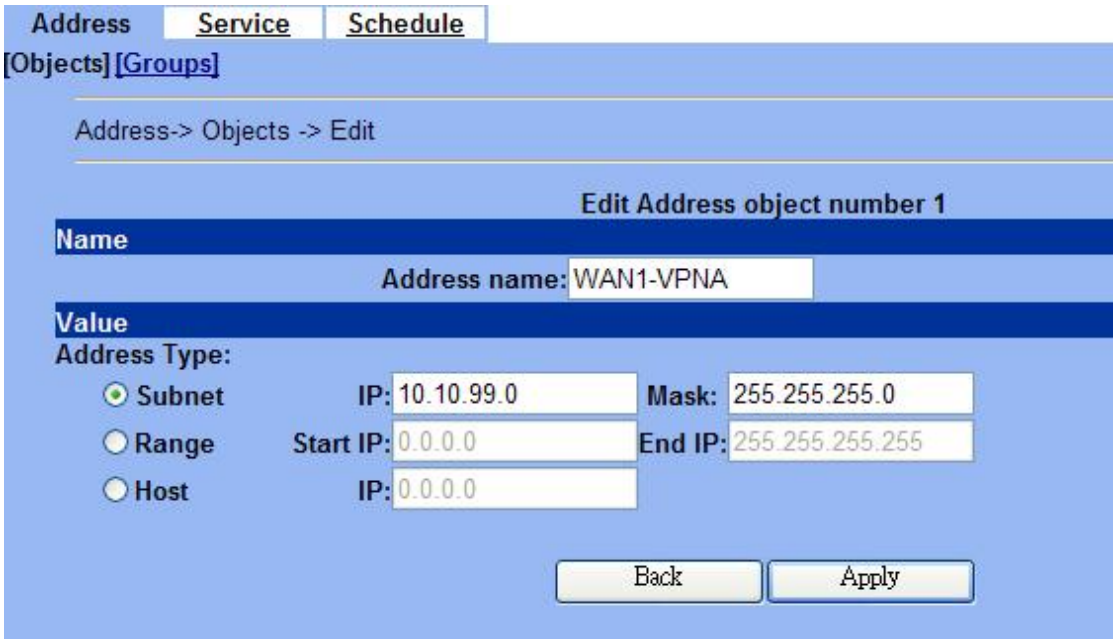
Remote_Firewall settings	Local_Firewall settings
01- Enable IPSec	01- Enable IPSec
02- Local IP address: 192.168.1.0/24	02- Local IP address: 10.10.99.0/24
03- Remote IP address: 10.10.99.0/24	03- Remote IP address: 192.168.1.0/24
04- Negotiation Mode: Main mode	04- Negotiation Mode: Main mode
05- Encapsulation Mode: Tunnel mode	05- Encapsulation Mode: Tunnel mode
06- Peer's IP address: 61.219.68.13	06- Peer's IP address: 61.219.68.14
07- PSK: 1234567890	07- PSK: 1234567890
08- IKE policy: DES+MD5	08- IKE policy: DES+MD5
09- IKE key group: DH2	09- IKE key group: DH2
10- IPSec policy: DES+MD5 (ESP)	10- IPSec policy: DES+MD5 (ESP)
11- IPSec key group: DH1	11- IPSec key group: DH1

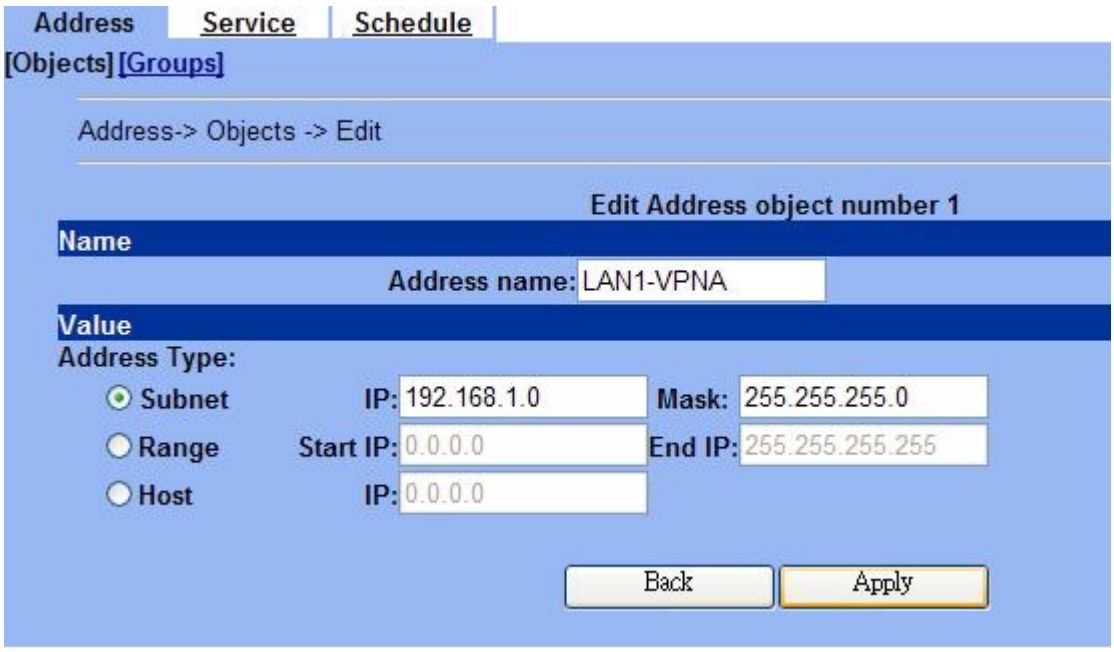
D-Link corporation

DFL-1500

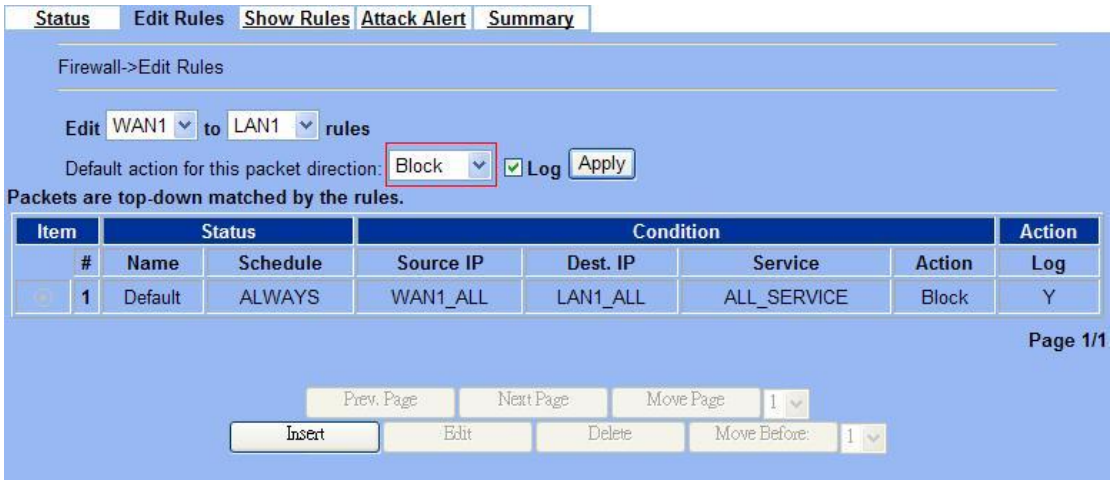
Remote_Firewall:

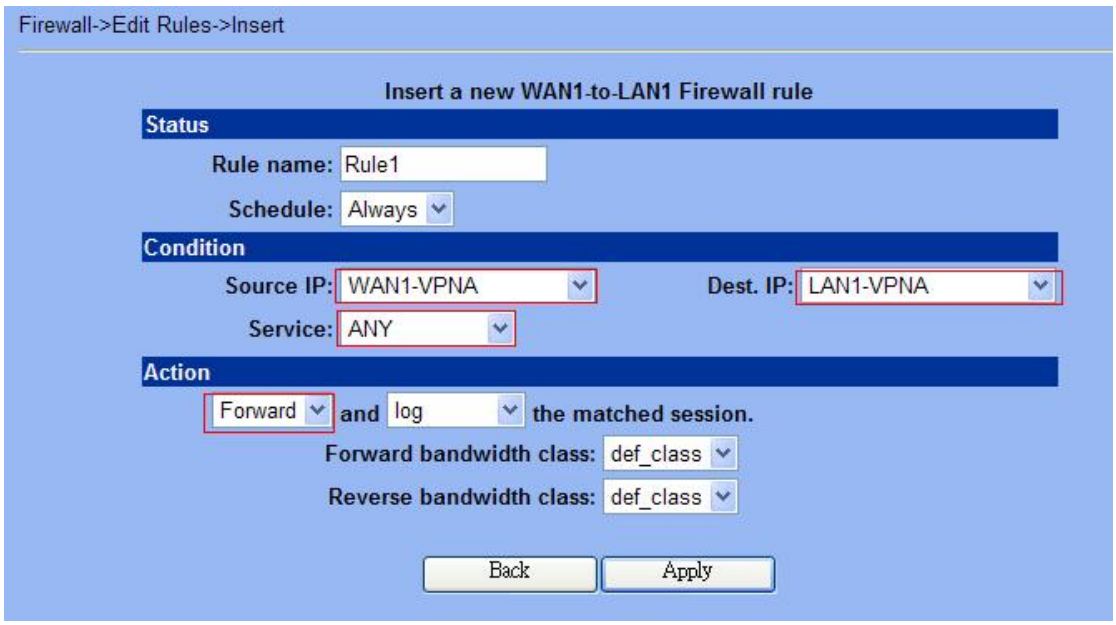
01- Add books (**Basic -> Books**)



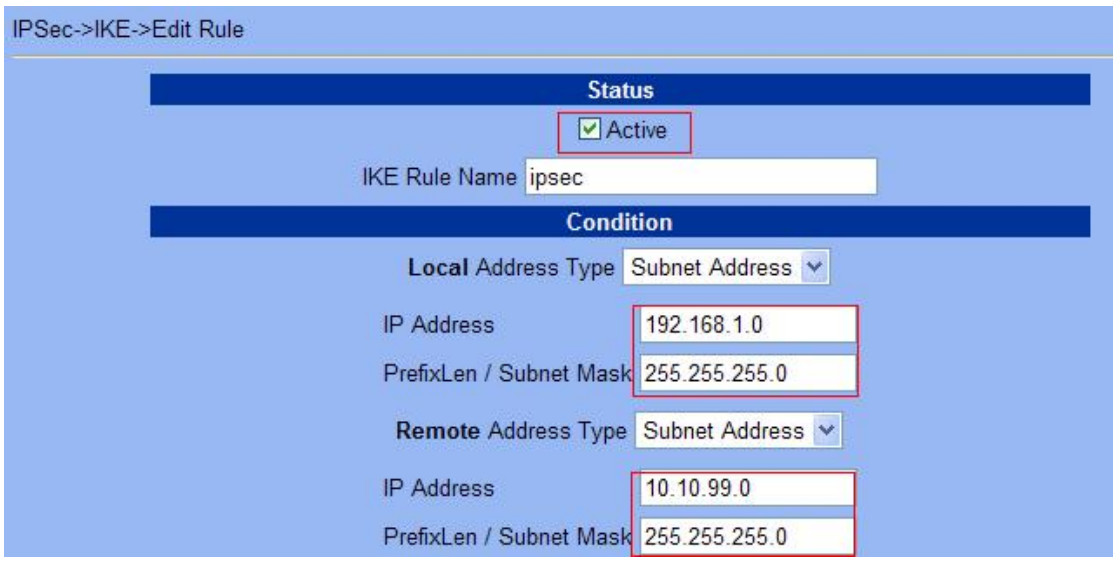


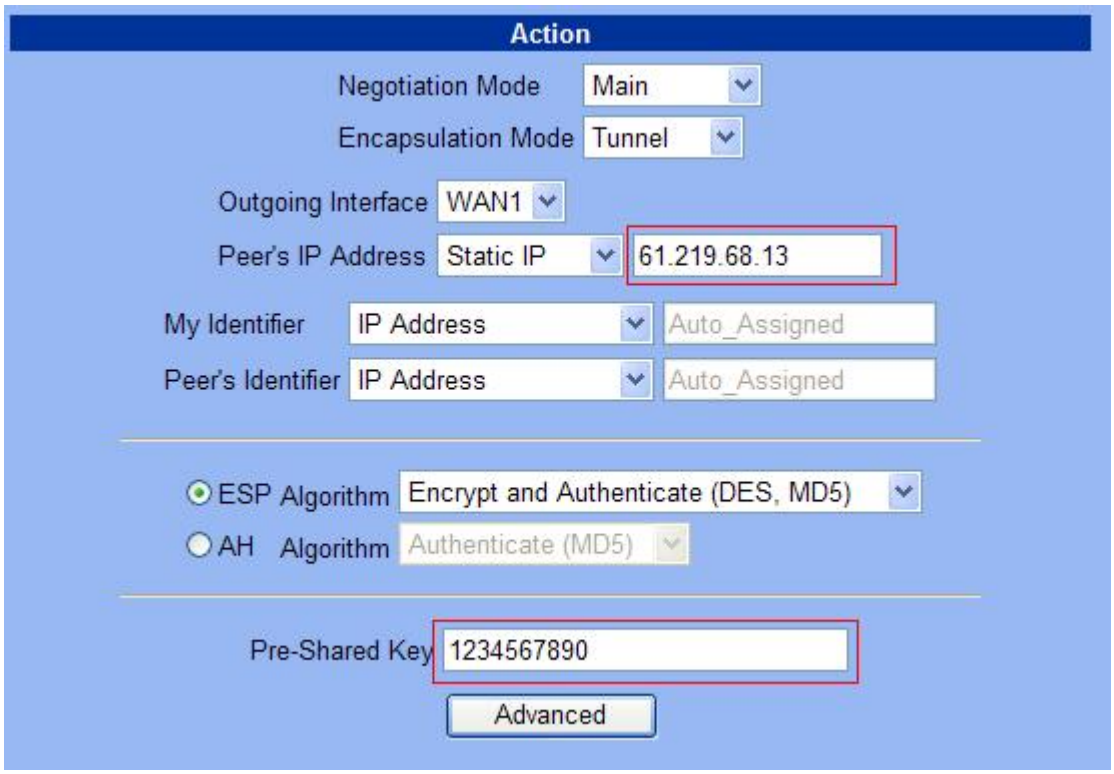
02- Edit Firewall rules (**Advanced Settings -> Firewall -> Edit Rules**)

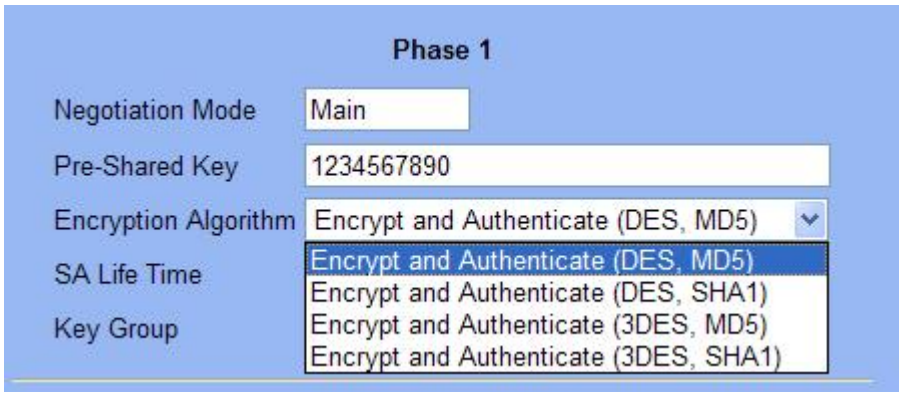


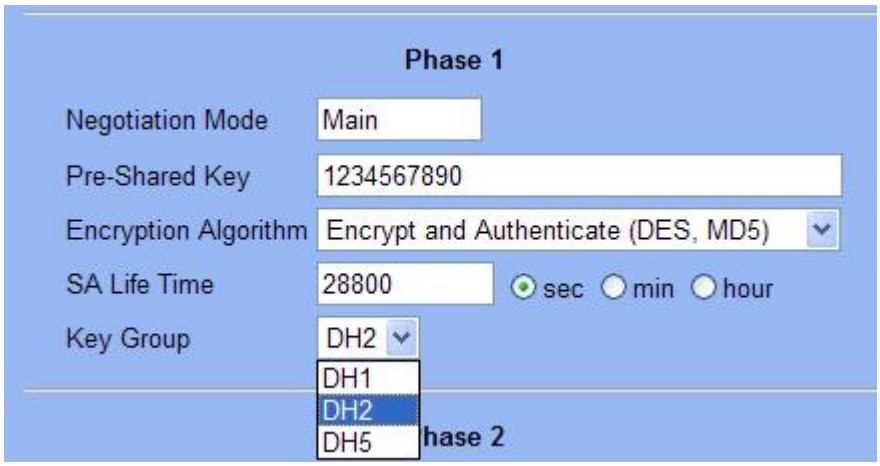


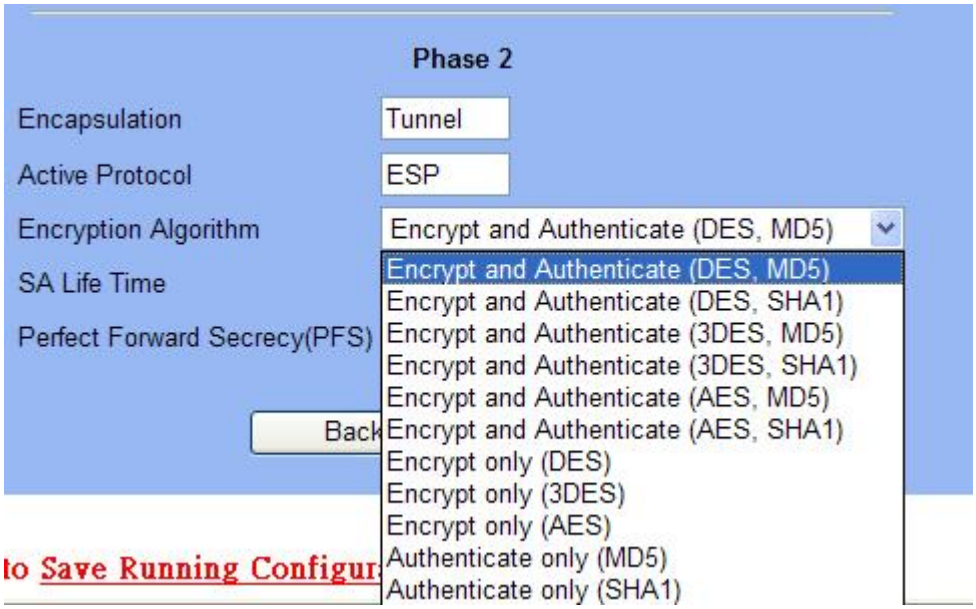
03- Enable IPSec and edit IPSec rule (**Advanced Settings -> VPN Settings**)

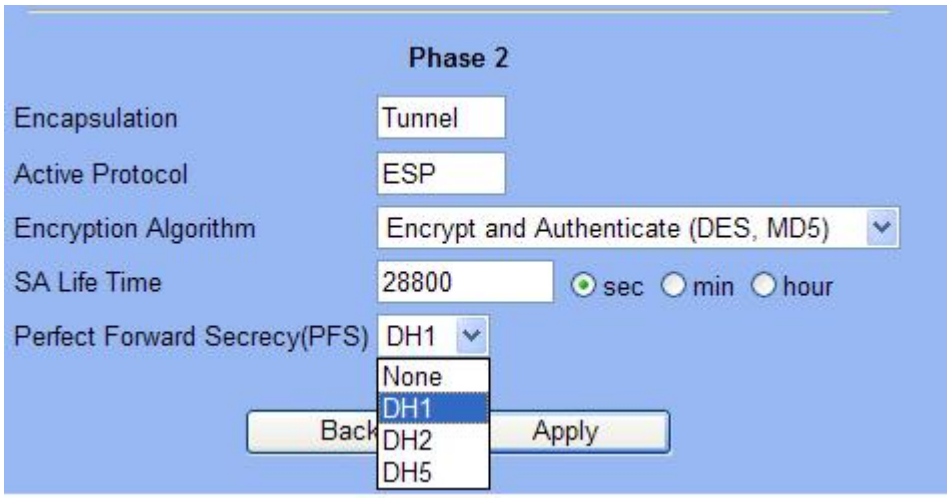

IPSec->IKE->Edit Rule
Status
Active
IKE Rule Name ipsec
Condition
Local Address Type Subnet Address
IP Address 192.168.1.0
PrefixLen / Subnet Mask 255.255.255.0
Remote Address Type Subnet Address
IP Address 10.10.99.0
PrefixLen / Subnet Mask 255.255.255.0


Action
Negotiation Mode Main
Encapsulation Mode Tunnel
Outgoing Interface WAN1
Peer's IP Address Static IP 61.219.68.13
My Identifier IP Address Auto_Assigned
Peer's Identifier IP Address Auto_Assigned
ESP Algorithm Encrypt and Authenticate (DES, MD5)
AH Algorithm Authenticate (MD5)
Pre-Shared Key 1234567890
Advanced


Phase 1
Negotiation Mode Main
Pre-Shared Key 1234567890
Encryption Algorithm Encrypt and Authenticate (DES, MD5)
SA Life Time
Key Group
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)

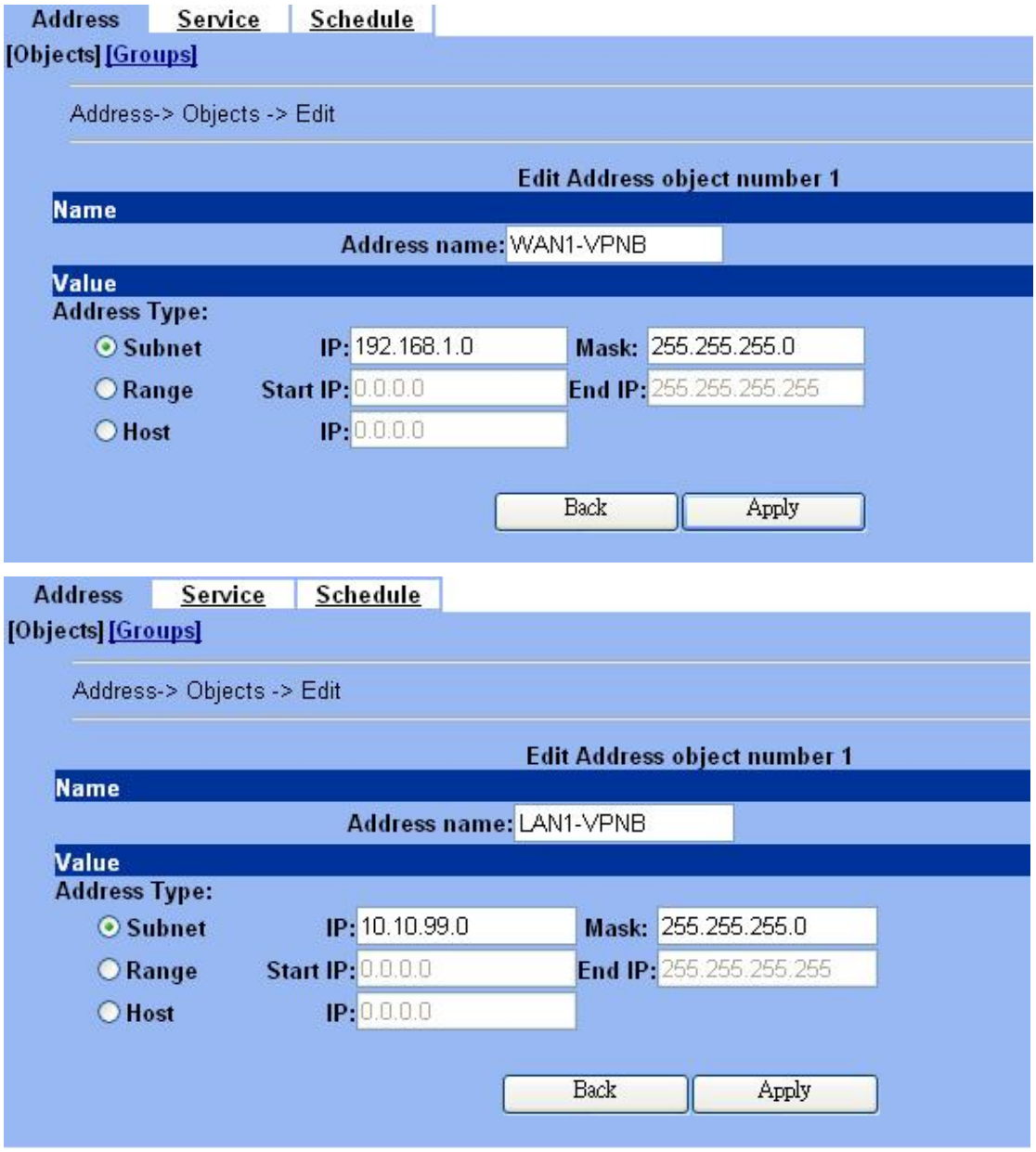




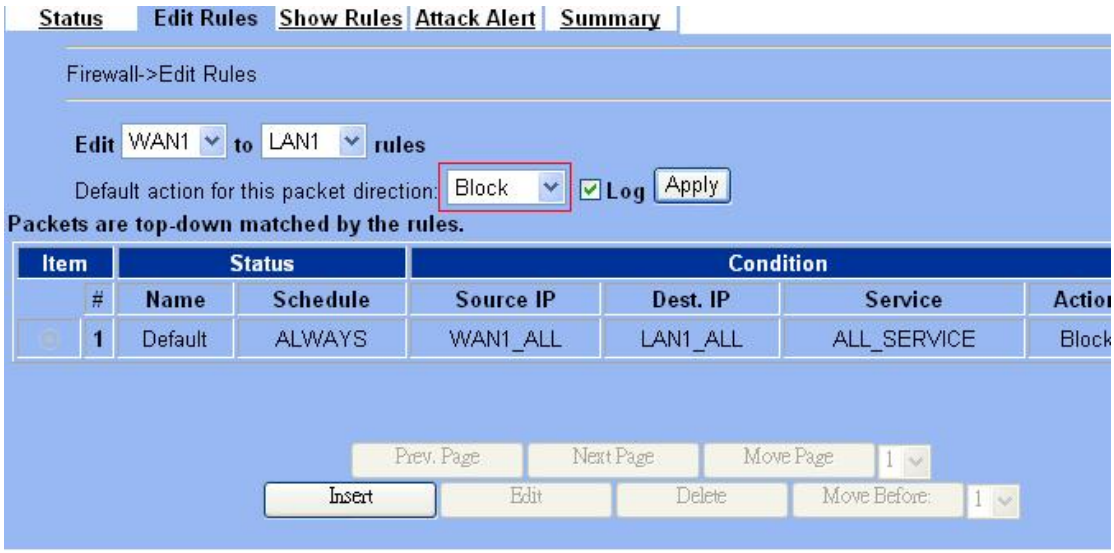


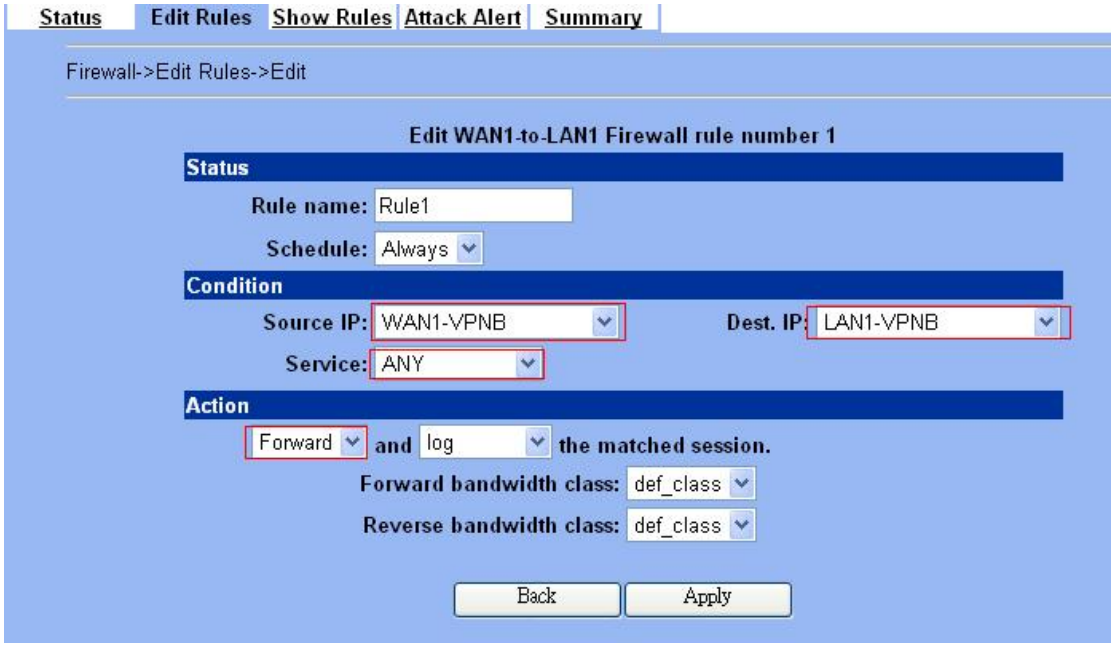
Local_Firewall:

01- Add books (**Basic -> Books**)

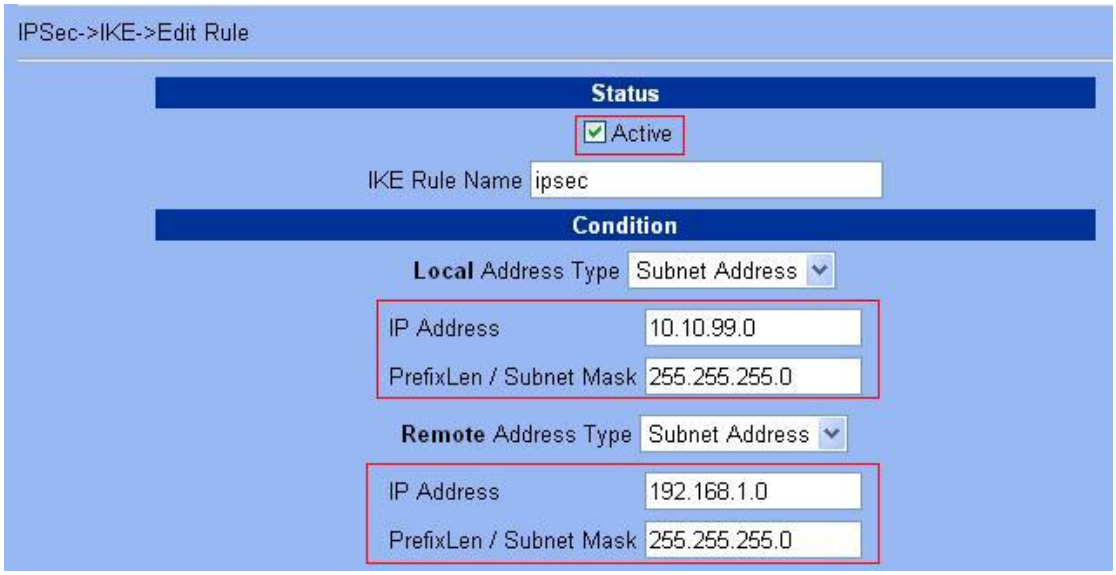


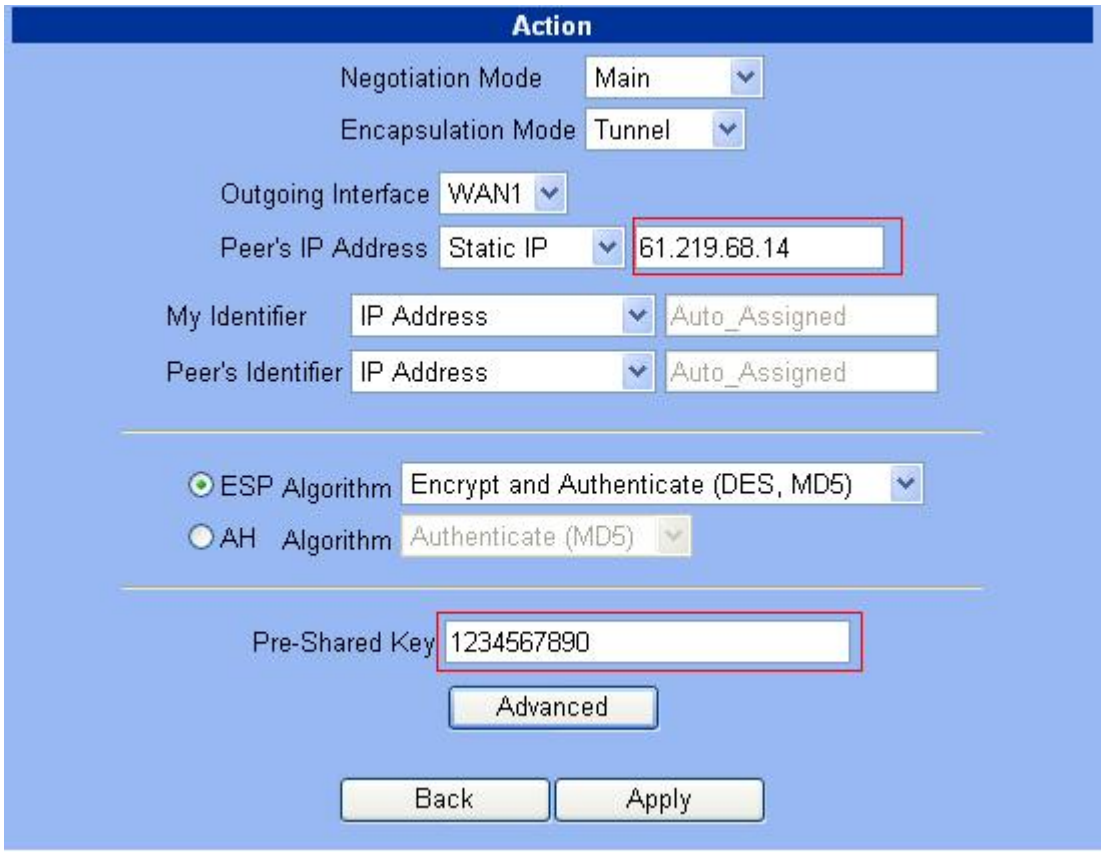
02- Edit Firewall rules (**Advanced Settings -> Firewall -> Edit Rules**)

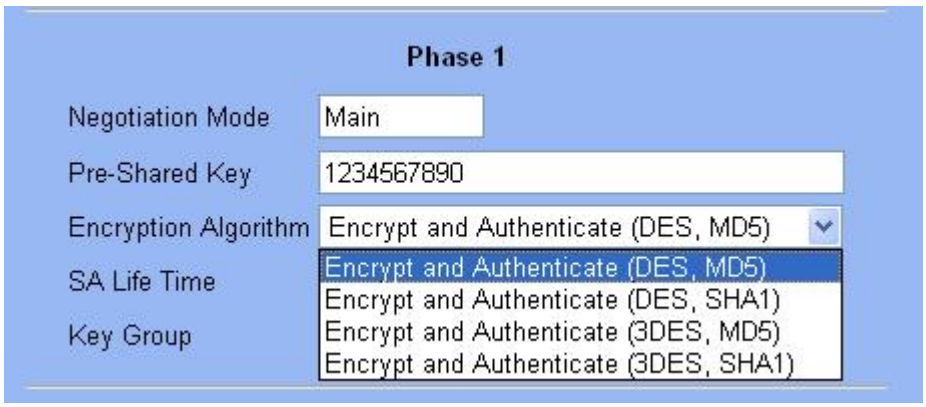


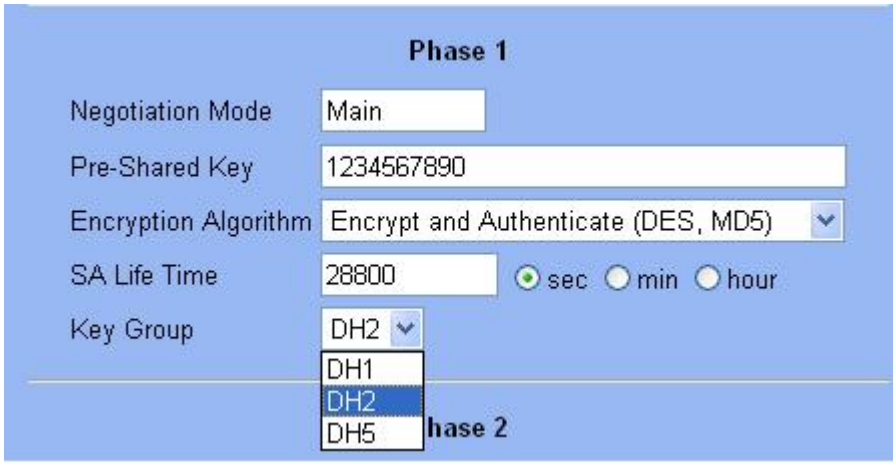


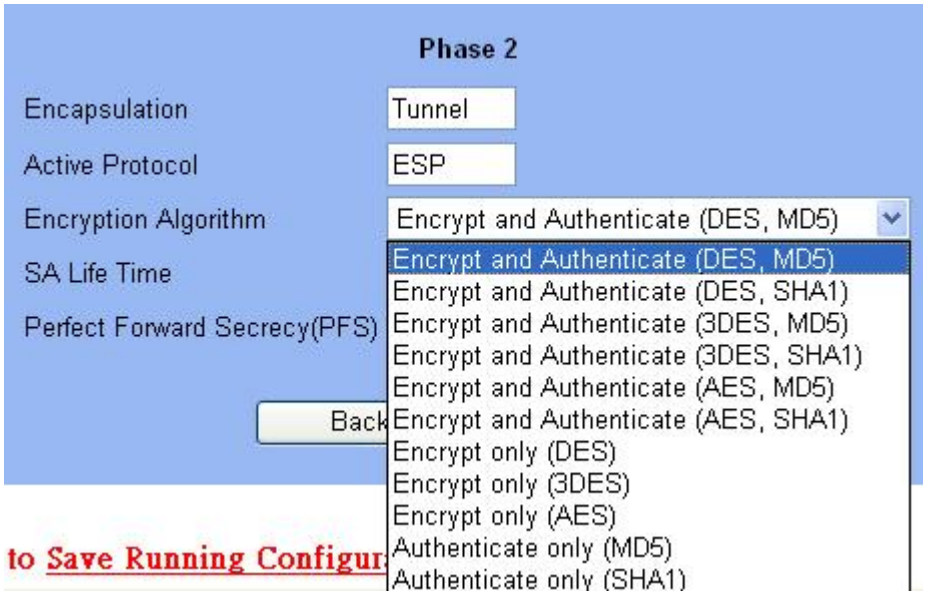
03- Enable IPSec and edit IPSec rule (**Advanced Settings -> VPN Settings**)

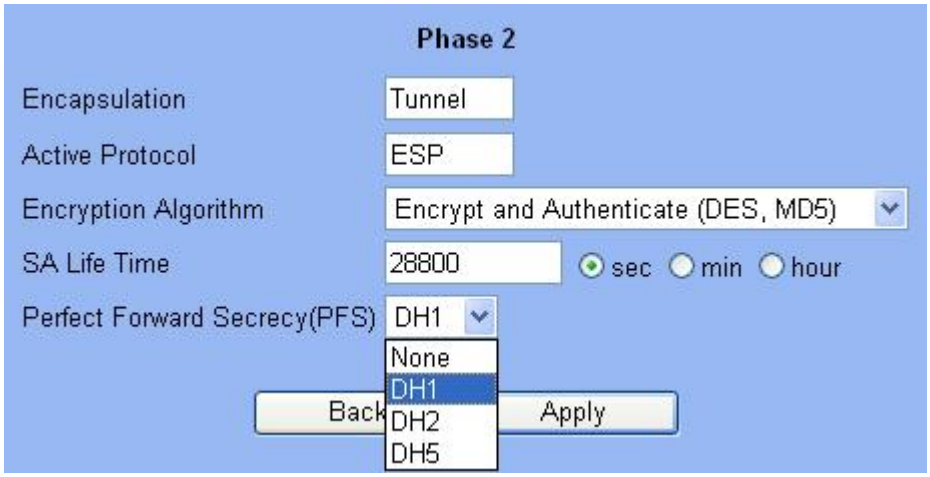

IPSec->IKE->Edit Rule
Status
Active
IKE Rule Name ipsec
Condition
Local Address Type Subnet Address
IP Address 10.10.99.0
PrefixLen / Subnet Mask 255.255.255.0
Remote Address Type Subnet Address
IP Address 192.168.1.0
PrefixLen / Subnet Mask 255.255.255.0


Action
Negotiation Mode Main
Encapsulation Mode Tunnel
Outgoing Interface WAN1
Peer's IP Address Static IP 61.219.68.14
My Identifier IP Address Auto_Assigned
Peer's Identifier IP Address Auto_Assigned
ESP Algorithm Encrypt and Authenticate (DES, MD5)
AH Algorithm Authenticate (MD5)
Pre-Shared Key 1234567890
Advanced
Back
Apply


Phase 1
Negotiation Mode Main
Pre-Shared Key 1234567890
Encryption Algorithm Encrypt and Authenticate (DES, MD5)
SA Life Time
Key Group
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)



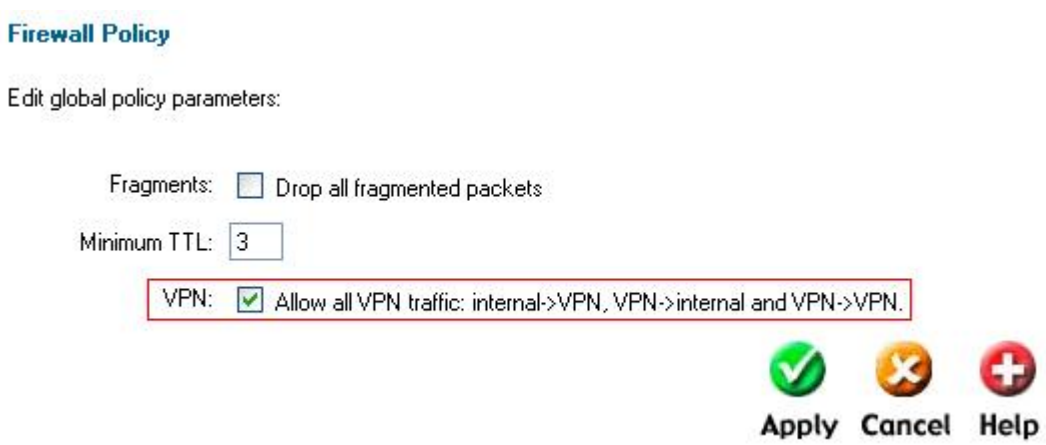




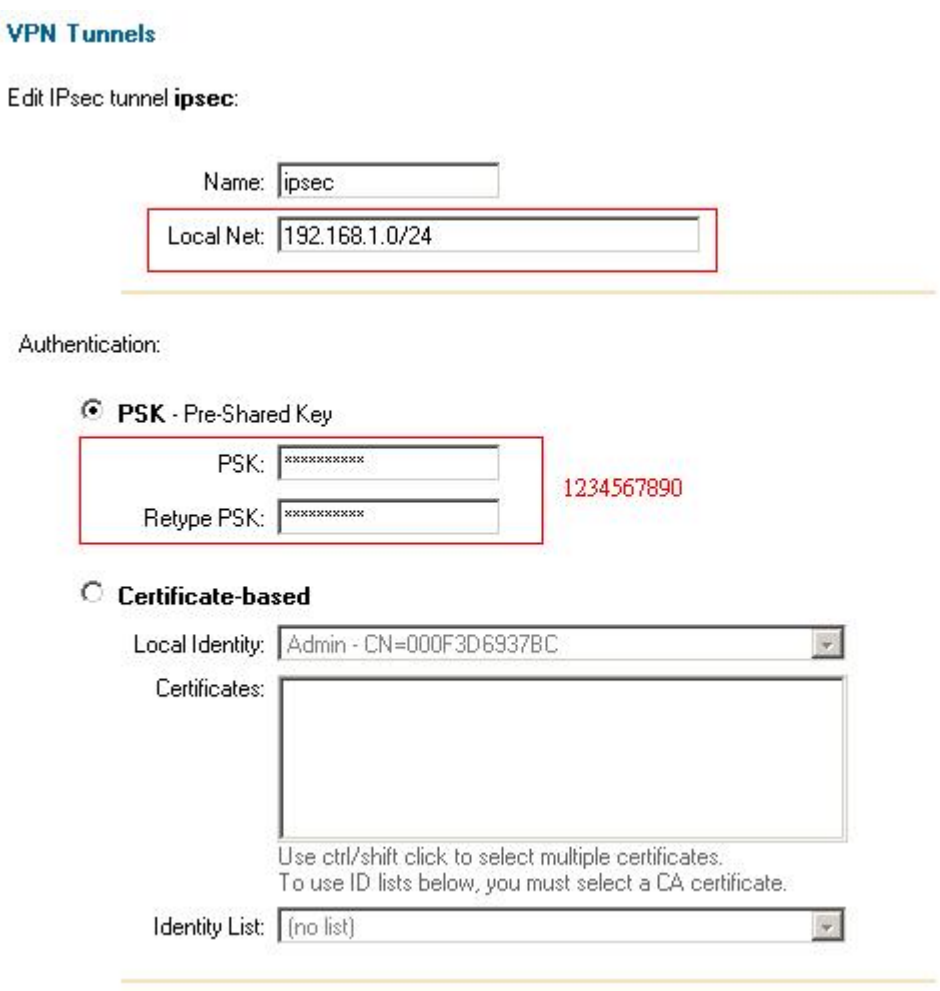
DFL-1100/700/200

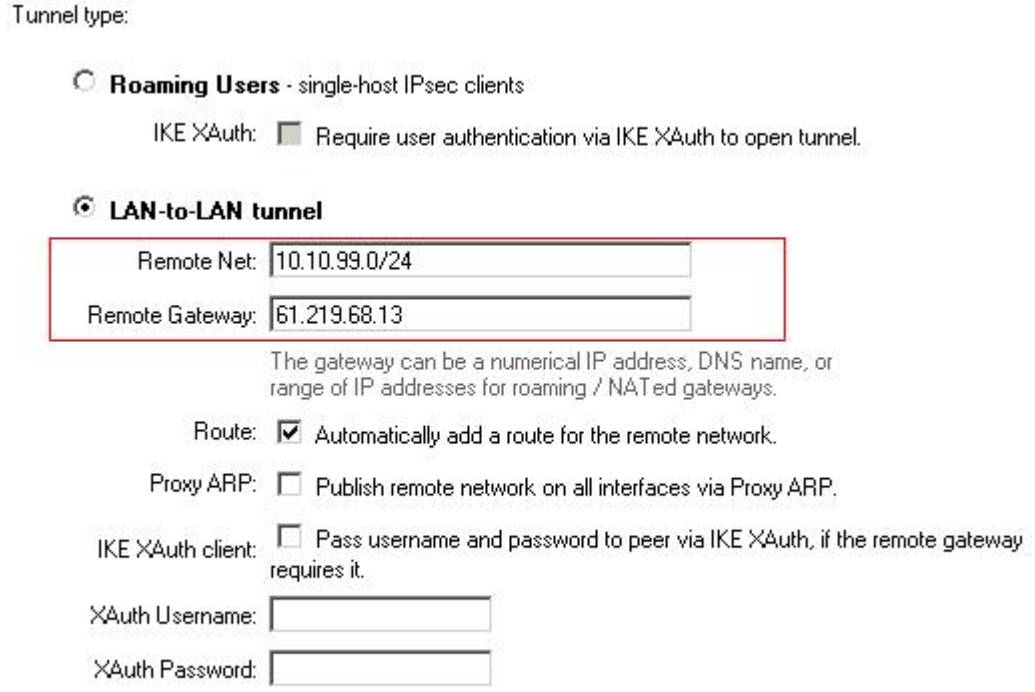
Remote_Firewall:

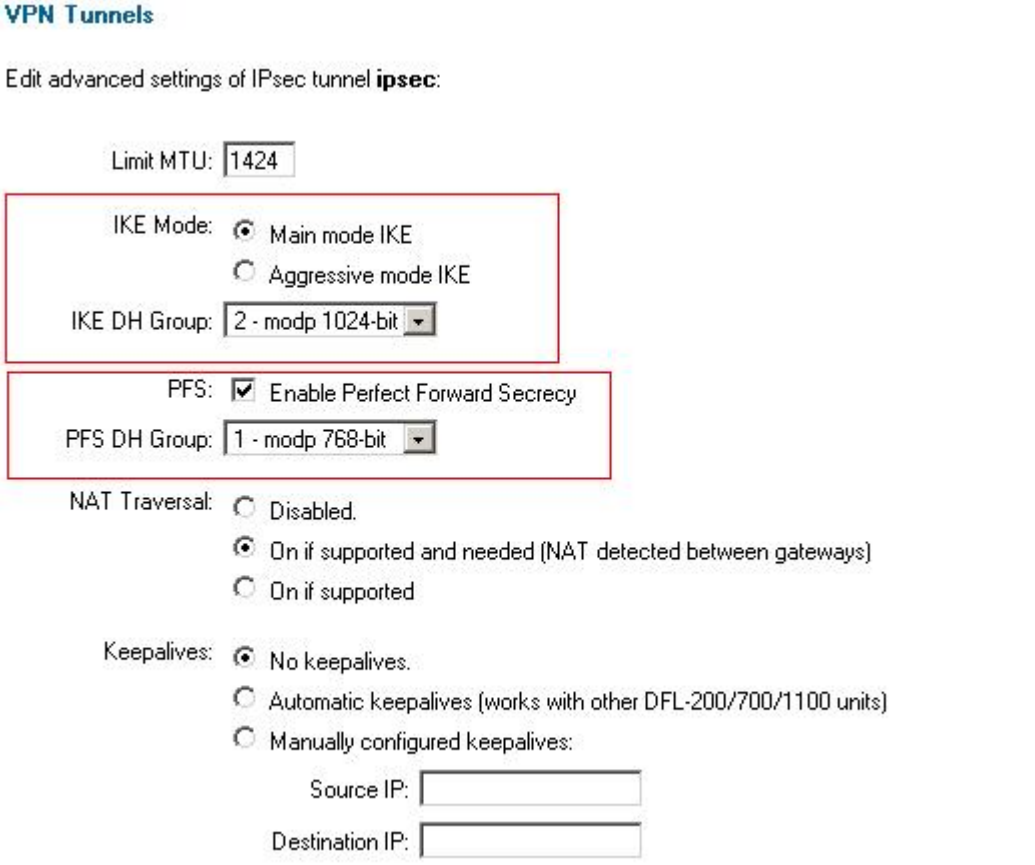
01- Enable allow all VPN traffic (**Firewall -> Policy**)

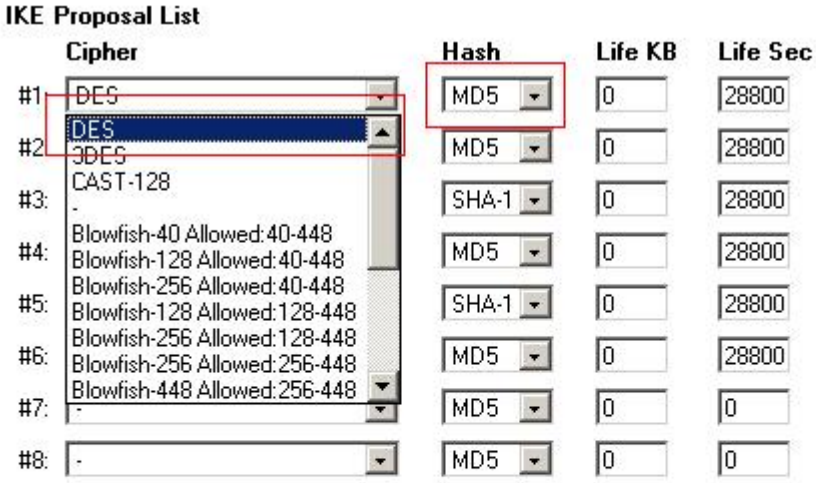


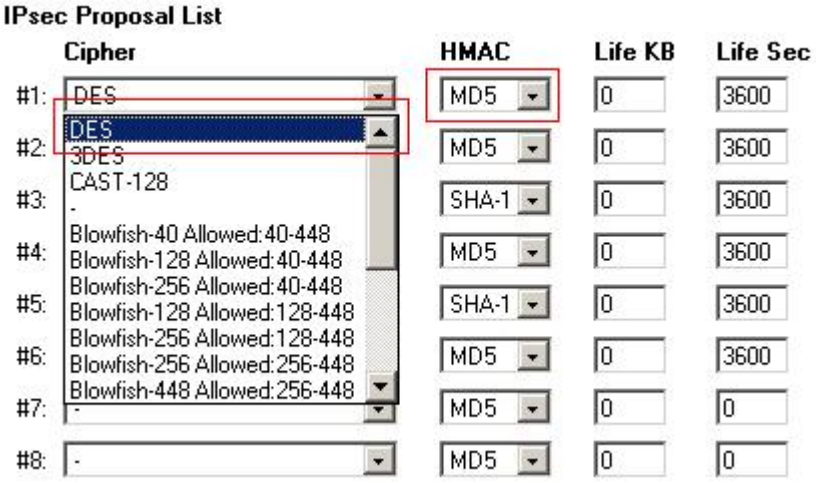
02- Enable IPSec and edit IPSec rule (**Firewall -> VPN -> IPSec Tunnels**)




Tunnel type:
Roaming Users - single-host IPsec clients
IKE XAuth:
Require user authentication via IKE XAuth to open tunnel.
LAN-to-LAN tunnel
Remote Net:
10.10.99.0/24
Remote Gateway:
61.219.68.13
The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.
Route:
Automatically add a route for the remote network.
Proxy ARP:
Publish remote network on all interfaces via Proxy ARP.
IKE XAuth client:
Pass username and password to peer via IKE XAuth, if the remote gateway requires it.
XAuth Username:
XAuth Password:

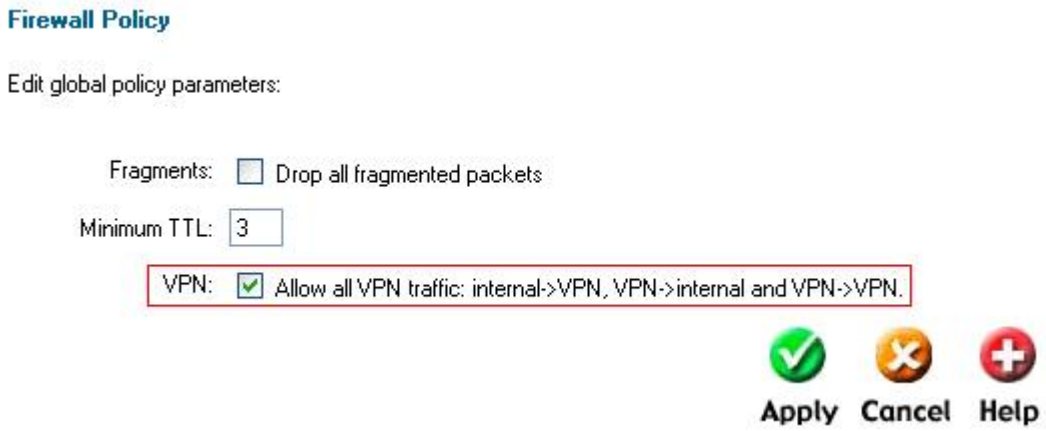

VPN Tunnels
Edit advanced settings of IPsec tunnel ipsec:
Limit MTU:
1424
IKE Mode:
Main mode IKE
Aggressive mode IKE
IKE DH Group:
2 - modp 1024-bit
PFS:
Enable Perfect Forward Secrecy
PFS DH Group:
1 - modp 768-bit
NAT Traversal:
Disabled.
On if supported and needed (NAT detected between gateways)
On if supported
Keepalives:
No keepalives.
Automatic keepalives (works with other DFL-200/700/1100 units)
Manually configured keepalives:
Source IP:
Destination IP:



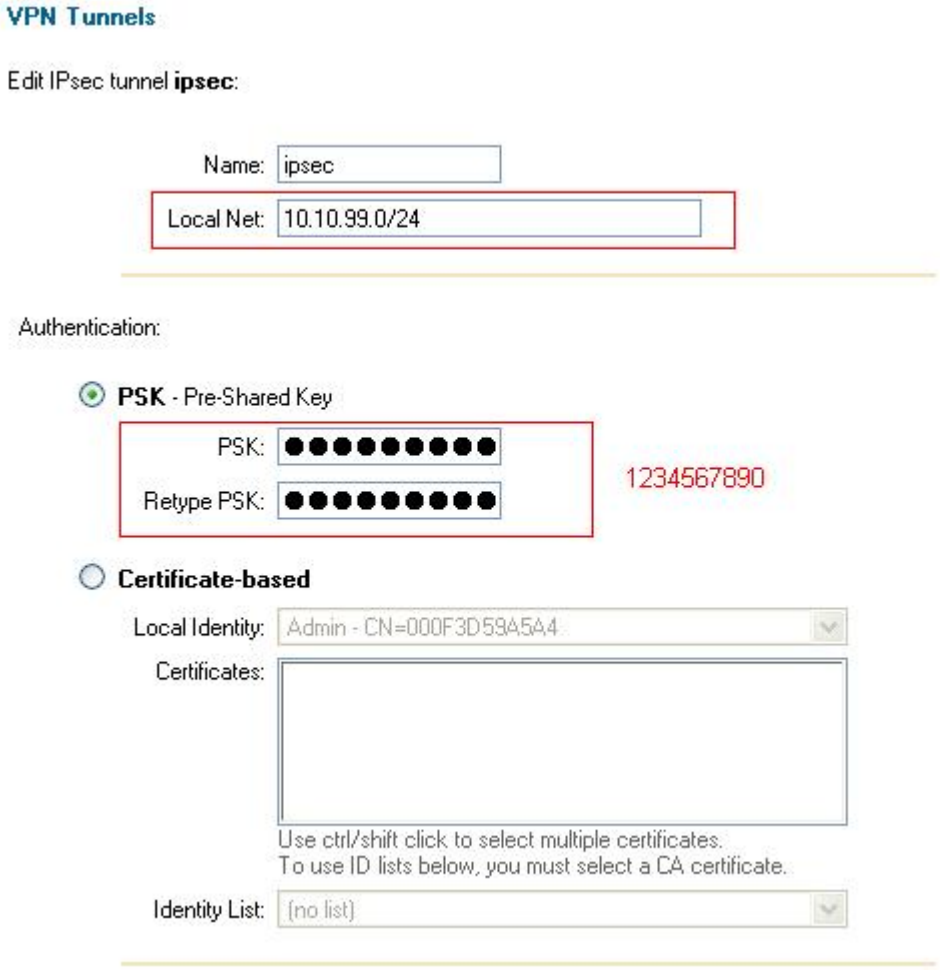


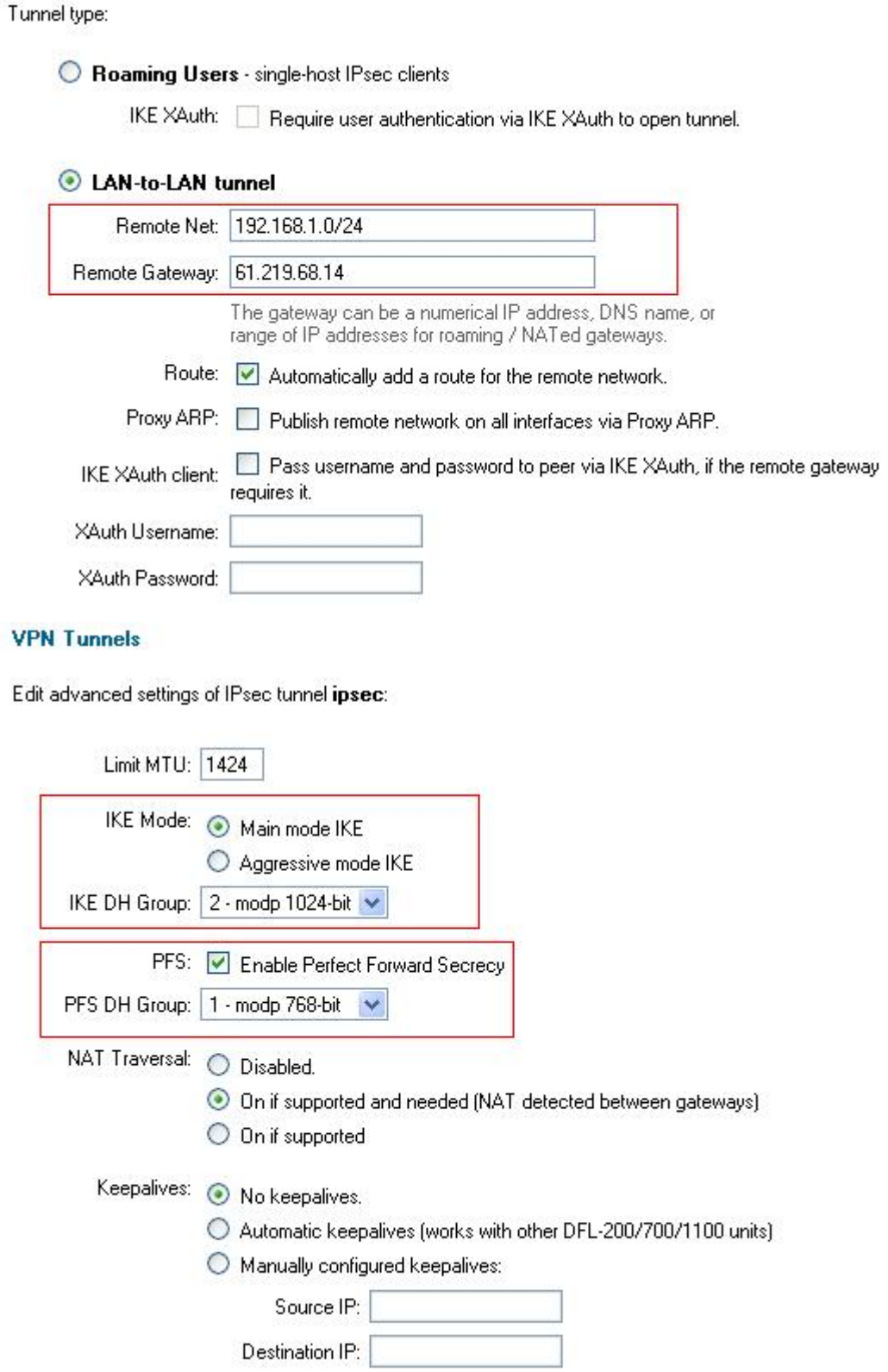
Local_Firewall:

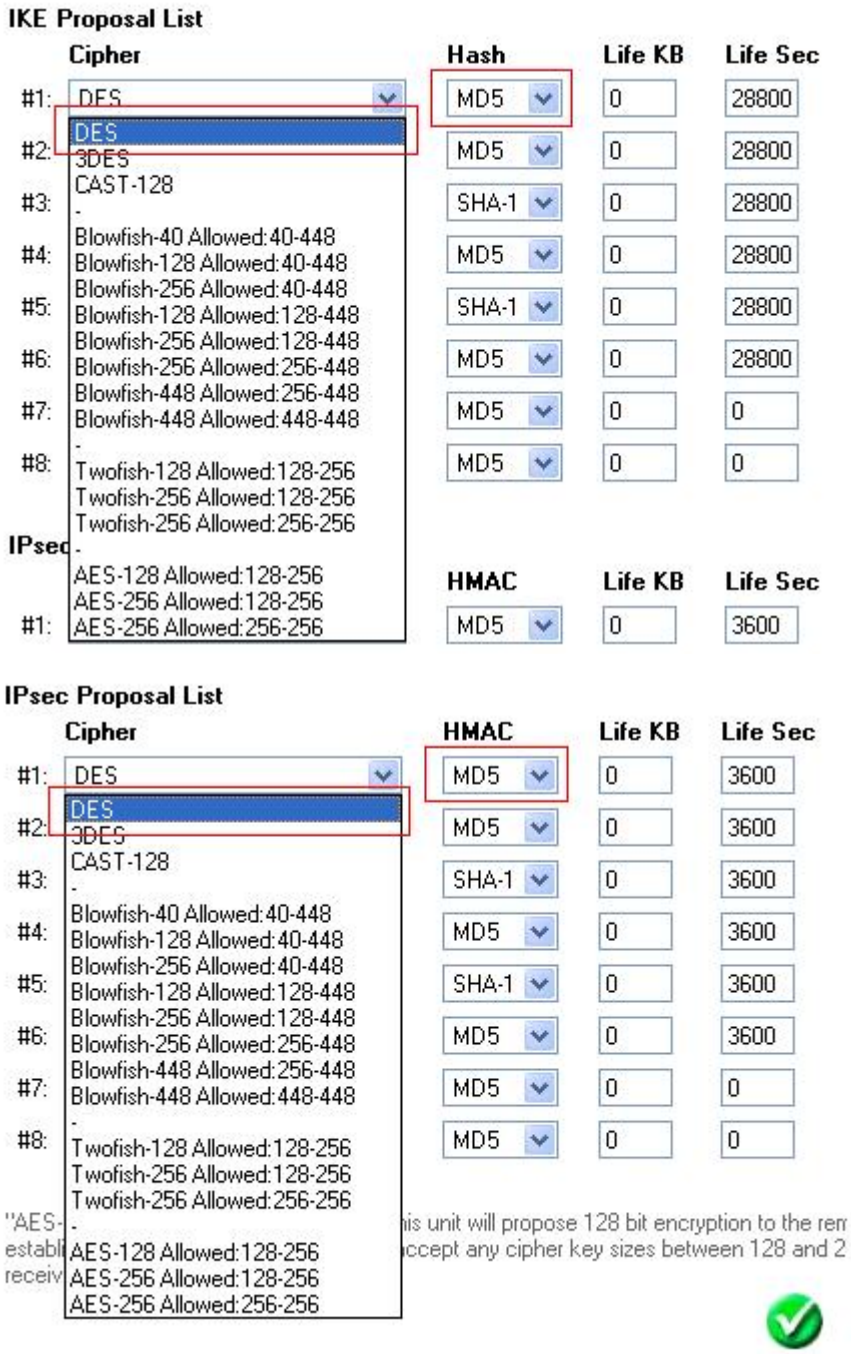
01-Enable allow all VPN traffic (**Firewall -> Policy**)



02- Enable IPSec and edit IPSec rule (**Firewall -> VPN -> IPSec Tunnels**)




Tunnel type:
Roaming Users - single-host IPsec clients
IKE XAuth:
Require user authentication via IKE XAuth to open tunnel.
LAN-to-LAN tunnel
Remote Net:
192.168.1.0/24
Remote Gateway:
61.219.68.14
The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.
Route:
Automatically add a route for the remote network.
Proxy ARP:
Publish remote network on all interfaces via Proxy ARP.
IKE XAuth client:
Pass username and password to peer via IKE XAuth, if the remote gateway requires it.
XAuth Username:
XAuth Password:
VPN Tunnels
Edit advanced settings of IPsec tunnel ipsec:
Limit MTU:
1424
IKE Mode:
Main mode IKE
Aggressive mode IKE
IKE DH Group:
2 - modp 1024-bit
PFS:
Enable Perfect Forward Secrecy
PFS DH Group:
1 - modp 768-bit
NAT Traversal:
Disabled.
On if supported and needed (NAT detected between gateways)
On if supported
Keepalives:
No keepalives.
Automatic keepalives (works with other DFL-200/700/1100 units)
Manually configured keepalives:
Source IP:
Destination IP:

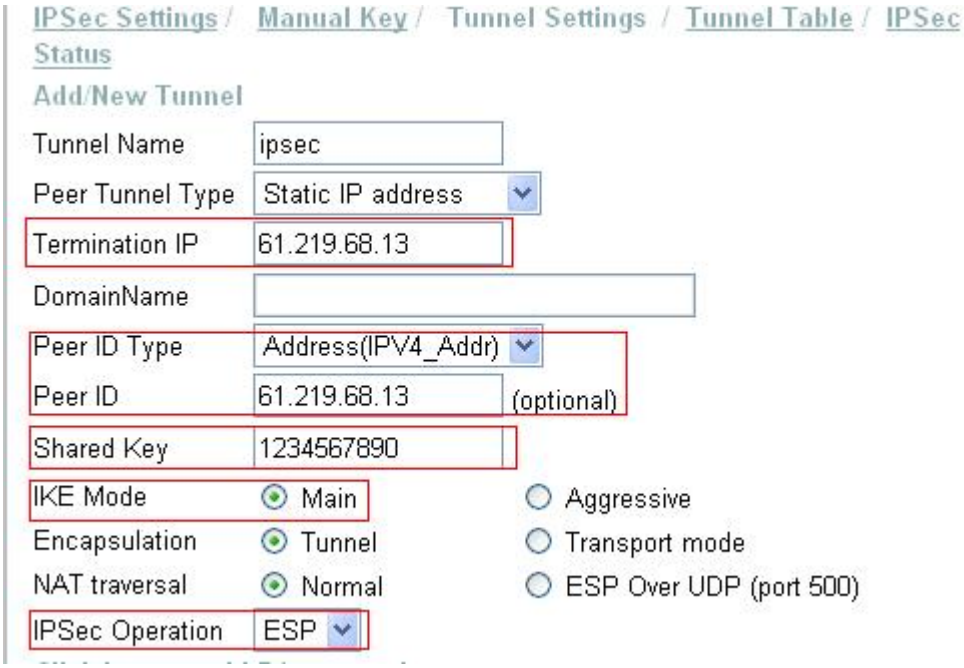


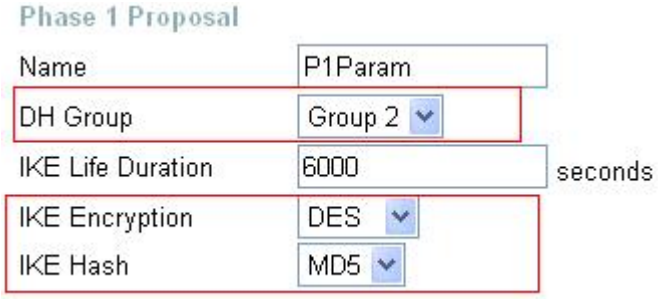
DFL-600

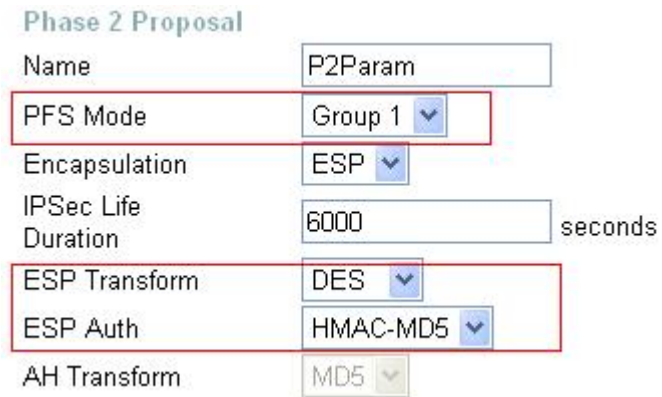
Remote_Firewall:

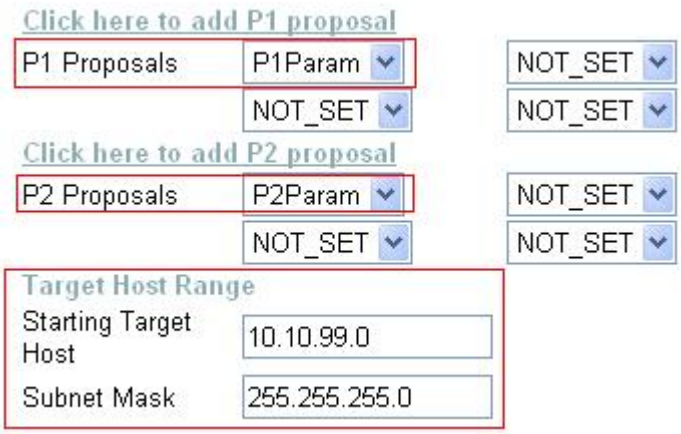
01- Enable allow all VPN traffic (**Advanced -> Policy -> Global Policy Status)**

02- Enable IPSec and edit IPSec rule (**Advanced -> VPN-IPSec -> Tunnel Settings**)





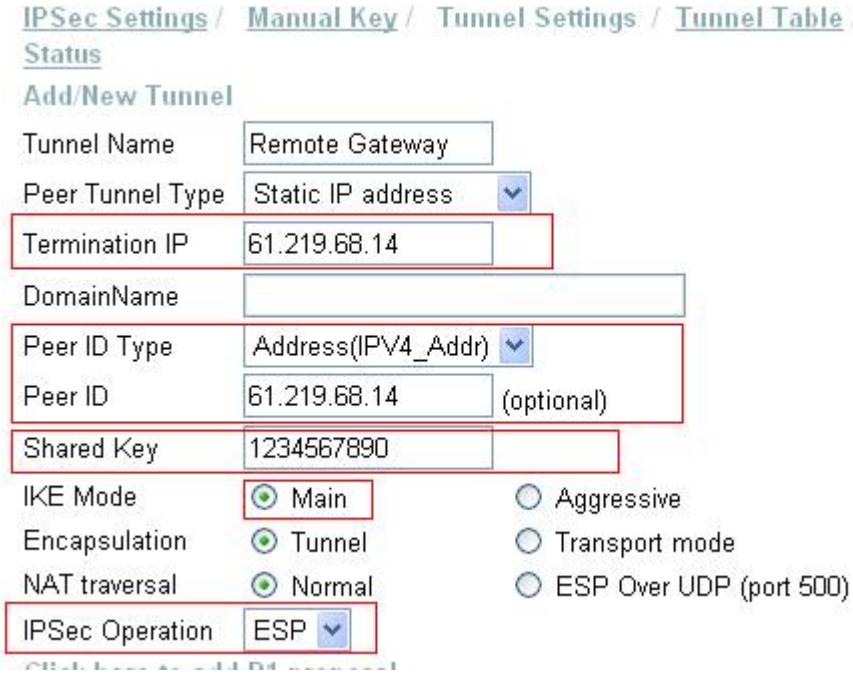


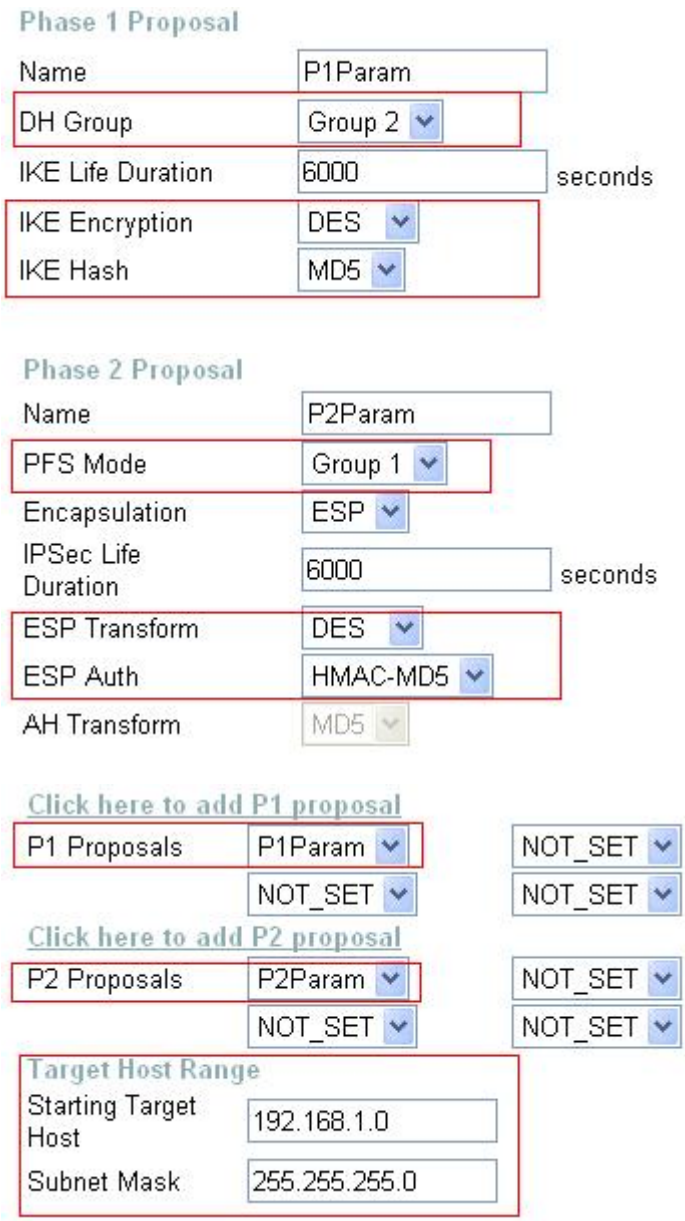


Local_Firewall:

01- Enable allow all VPN traffic (**Advanced -> Policy -> Global Policy Status)**

02- Enable IPSec and edit IPSec rule (**Advanced -> VPN-IPSec -> Tunnel Settings**)




Phase 1 Proposal
Name
P1Param
DH Group
Group 2
IKE Life Duration
6000
seconds
IKE Encryption
DES
IKE Hash
MD5
Phase 2 Proposal
Name
P2Param
PFS Mode
Group 1
Encapsulation
ESP
IPSec Life Duration
6000
seconds
ESP Transform
DES
ESP Auth
HMAC-MD5
AH Transform
MD5
Click here to add P1 proposal
P1 Proposals
P1Param
NOT_SET
NOT_SET
NOT_SET
Click here to add P2 proposal
P2 Proposals
P2Param
NOT_SET
NOT_SET
NOT_SET
Target Host Range
Starting Target Host
192.168.1.0
Subnet Mask
255.255.255.0