D-Link VPN Application

Quick Installation Guide

Contents

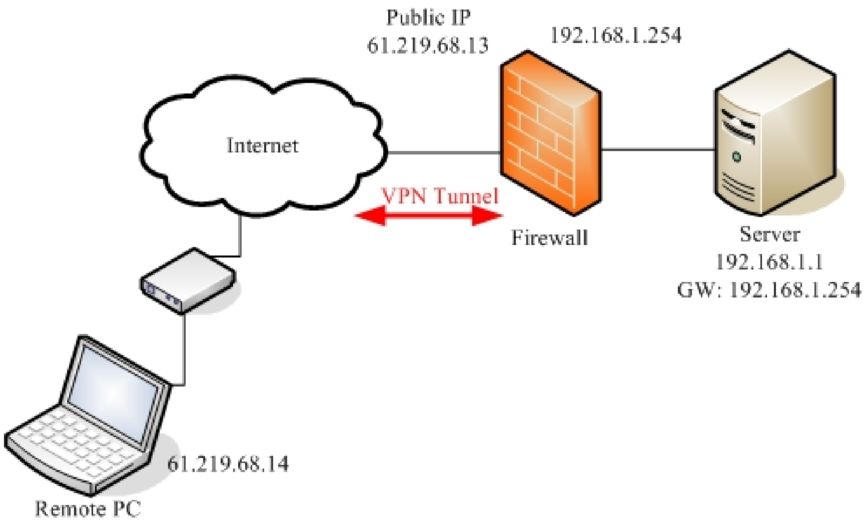
1. Remote Access

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

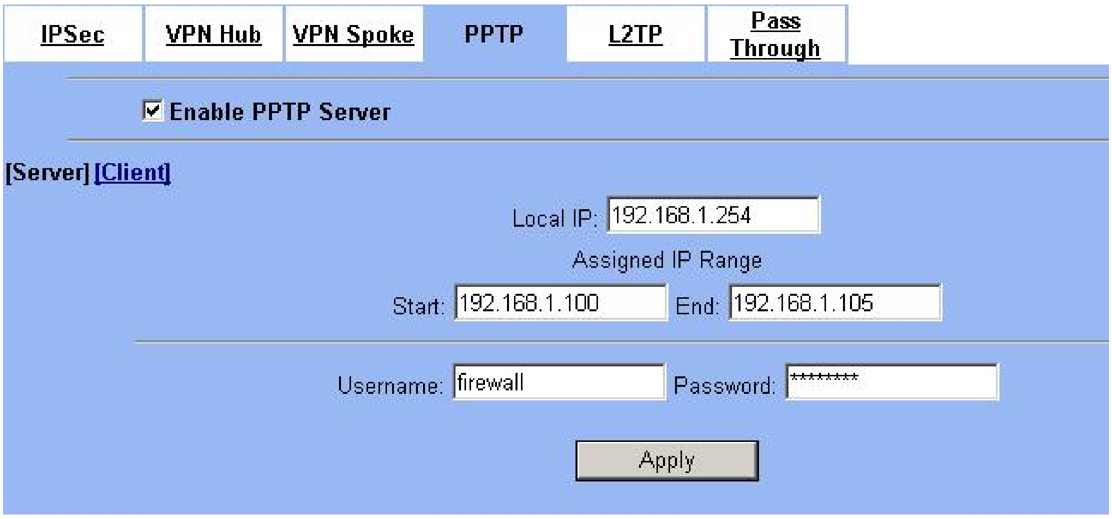
1-3-1 PPTP Server

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

Device setting page

DFL-1500

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



☑ Enable PPTP Server

Local IP: 192.168.1.254

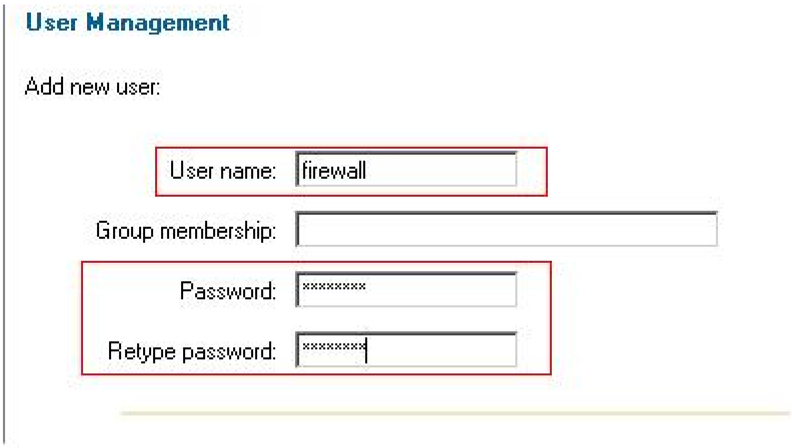
Assigned IP Range

Start: 192.168.1.100 End: 192.168.1.105

Username: firewall Password: *********

DFL-1100/700/200

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



Add new user:

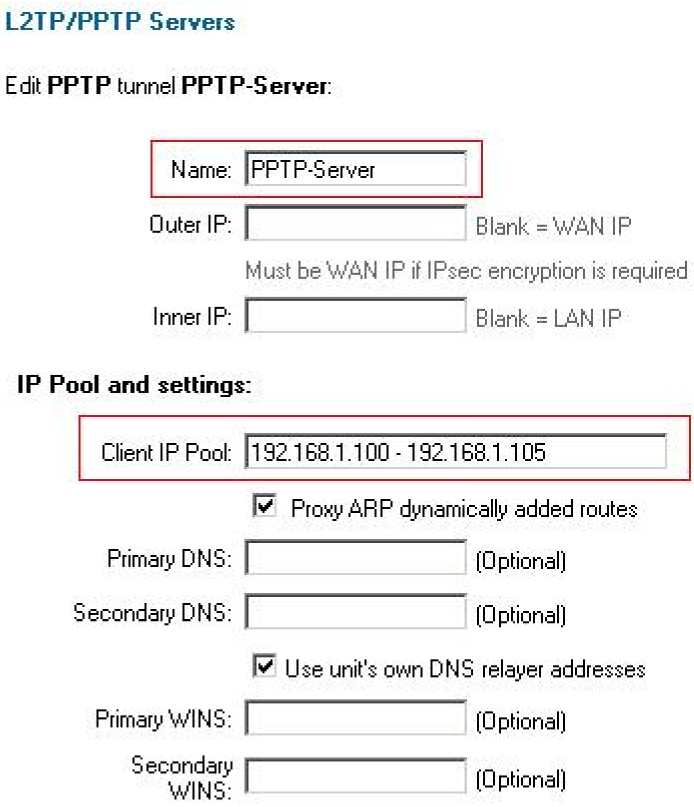
User name: firewall

Group membership:

Password: ********

Retype password: ********

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



L2TP/PPTP Servers

Edit **PPTP** tunnel **PPTP-Server**:

Name: PPTP-Server

Outer IP: Blank = WAN IP

Must be WAN IP if IPsec encryption is required

Inner IP: Blank = LAN IP

IP Pool and settings:

Client IP Pool: 192.168.1.100 - 192.168.1.105

☑ Proxy ARP dynamically added routes

Primary DNS: (Optional)

Secondary DNS: (Optional)

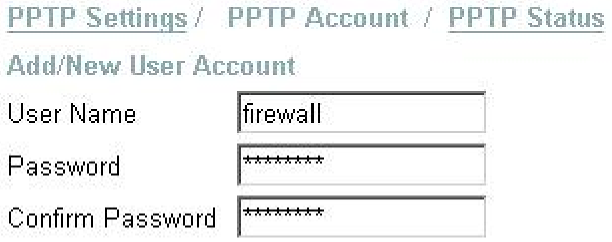
☑ Use unit's own DNS relayer addresses

Primary WINS: (Optional)

Secondary WINS: (Optional)

DFL-600

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



PPTP Settings / PPTP Account / PPTP Status

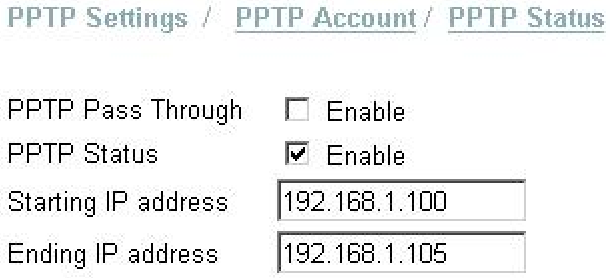
Add/New User Account

User Name: firewall

Password: ********

Confirm Password: ********

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



PPTP Settings / PPTP Account / PPTP Status

PPTP Pass Through □ Enable

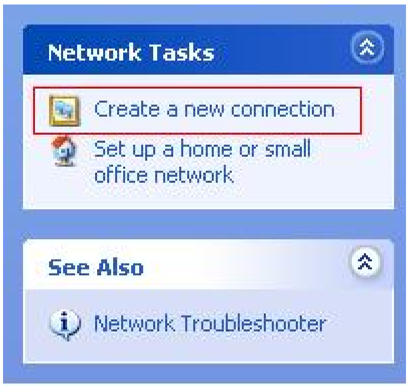
PPTP Status ☑ Enable

Starting IP address 192.168.1.100

Ending IP address 192.168.1.105

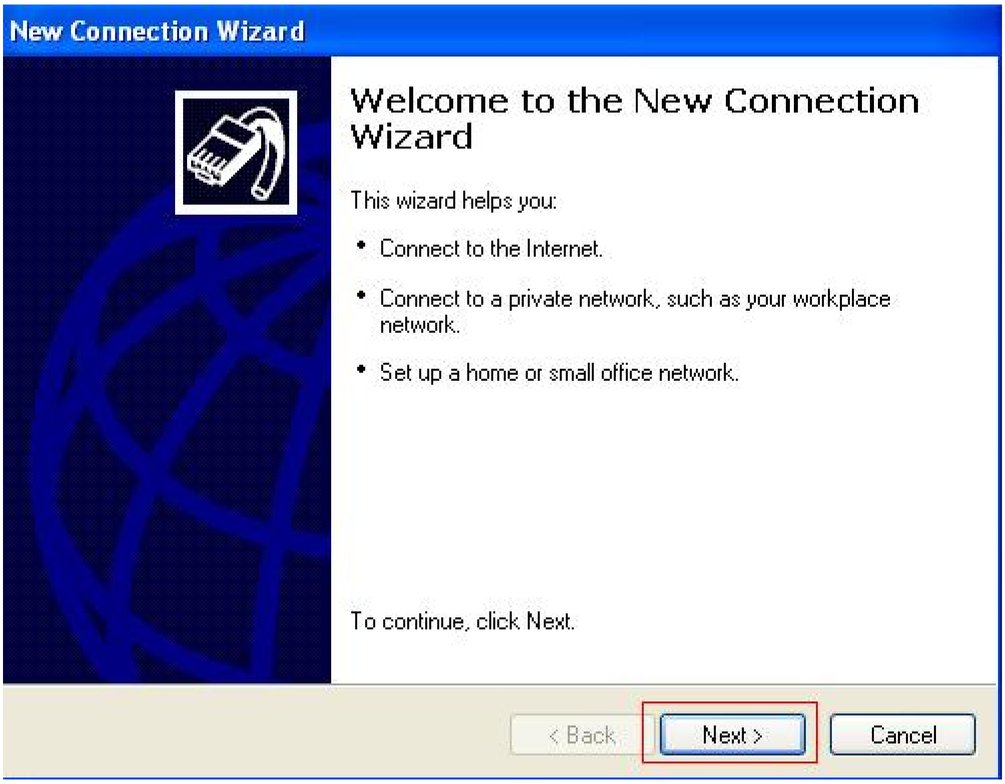
Configuring PPTP Client (Microsoft XP PRO's VPN adapter)
Setup1

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



Setup2

Click **Next** to the next step.



Welcome to the New Connection Wizard

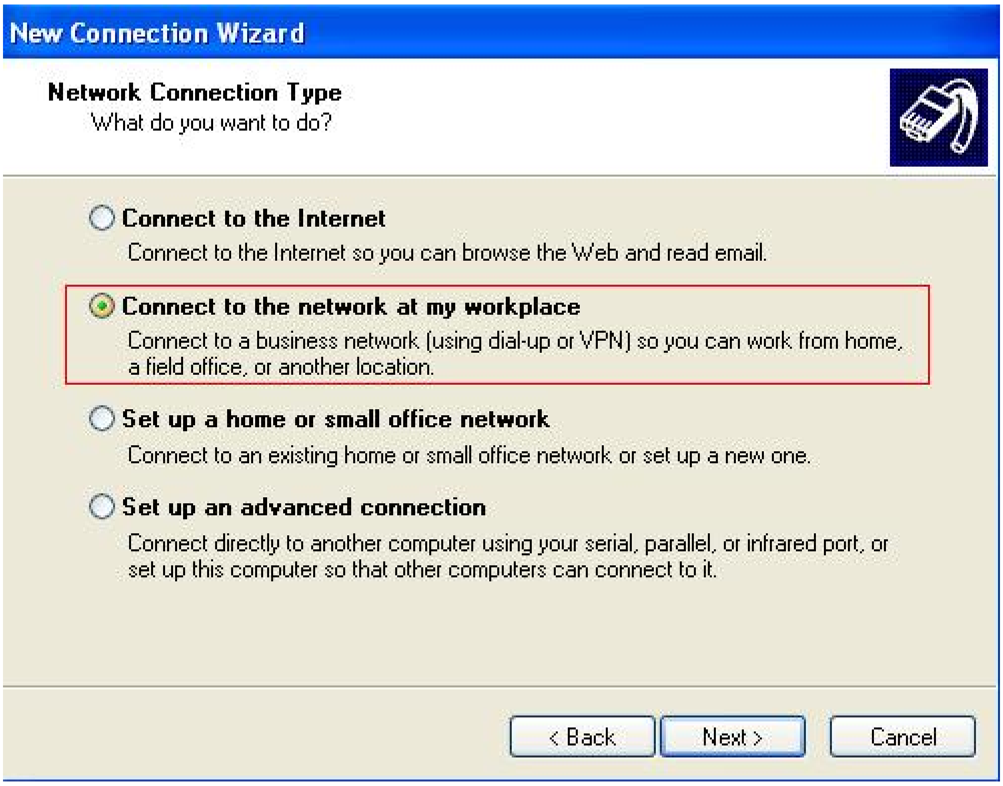
This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

Setup3

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



New Connection Wizard

Network Connection Type

What do you want to do?

○ **Connect to the Internet**

Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**

Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**

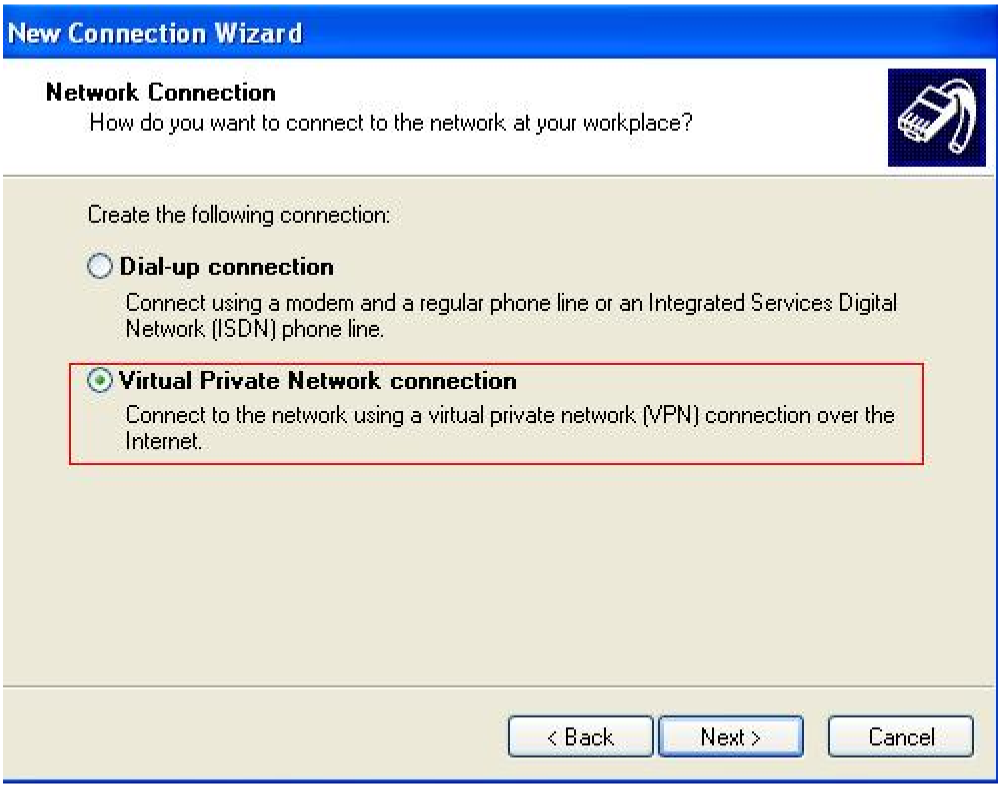
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**

Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Steup4

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



New Connection Wizard

Network Connection

How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**

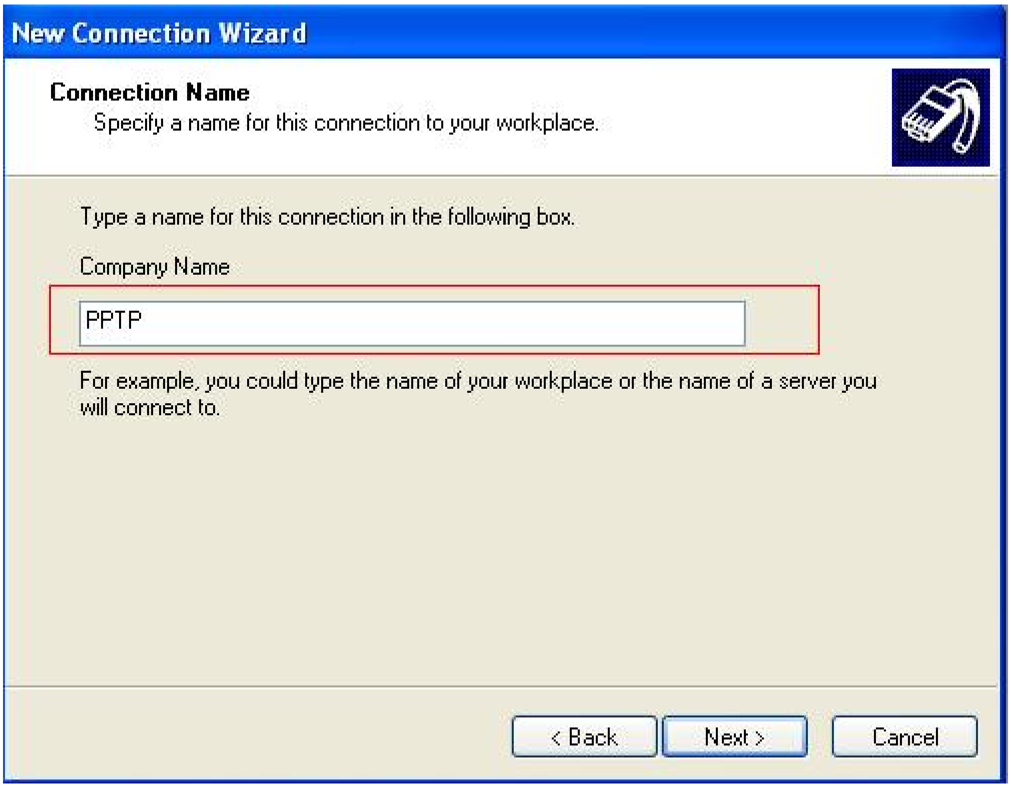
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**

Connect to the network using a virtual private network (VPN) connection over the Internet.

Step5

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



Connection Name

Specify a name for this connection to your workplace.

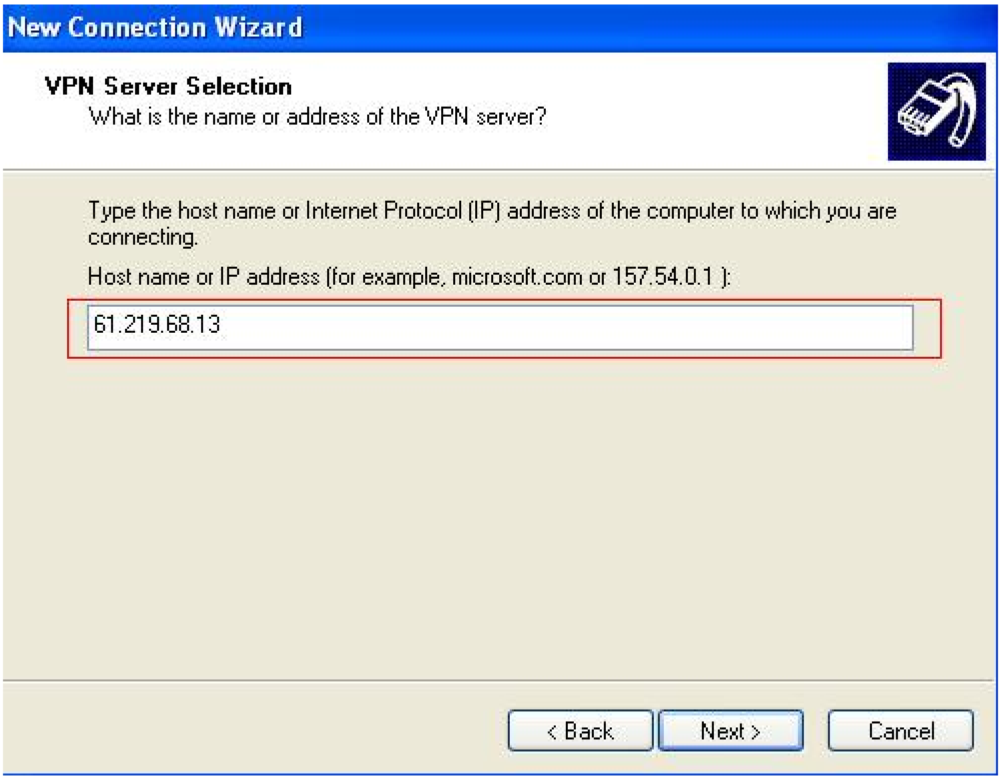
Type a name for this connection in the following box.

Company Name: PPTP

For example, you could type the name of your workplace or the name of a server you will connect to.

Step6

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



VPN Server Selection

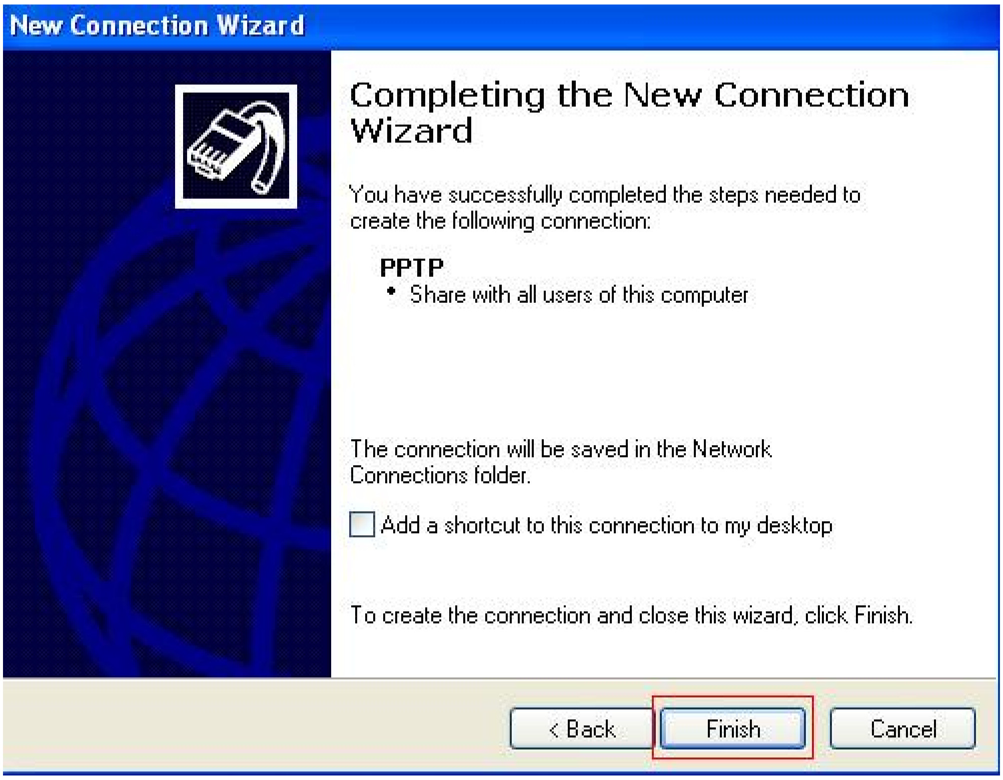
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1): 61.219.68.13

Step7

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



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

PPTP
- Share with all users of this computer

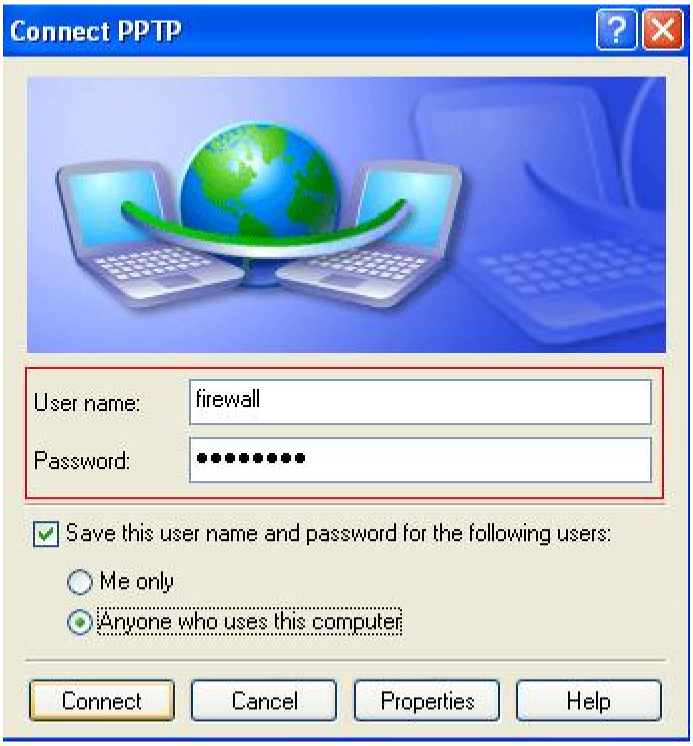
The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

Step8

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



Connect PPTP

User name: firewall

Password: ●●●●●●●●●

☑ Save this user name and password for the following users:

○ Me only

● Anyone who uses this computer

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

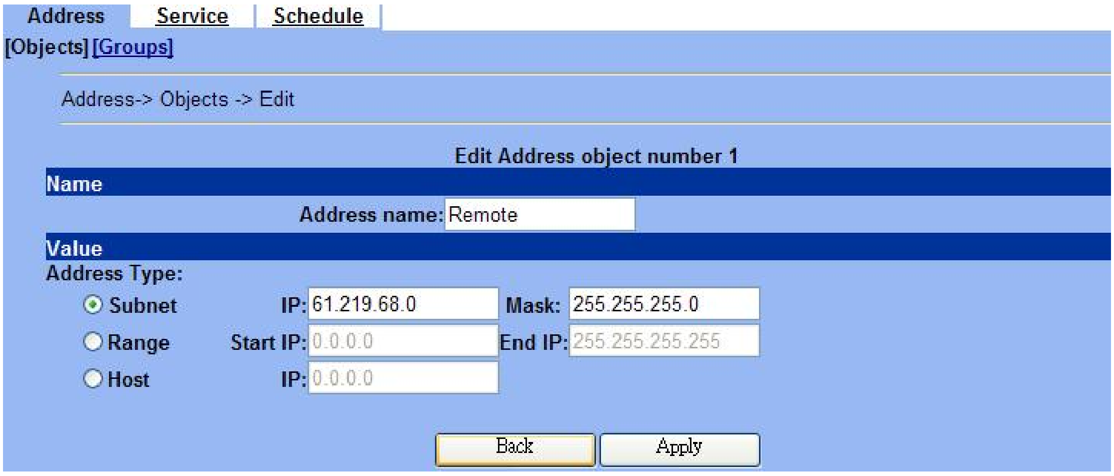
Remote PC settings	Firewall settings
01- Profile name: test 02- Communication media: LAN over IP 03- Gateway: 61.219.68.13 04- IKE policy: DES+MD5 05- IKE key group: DH2 06- IPSec policy: DES+MD5 (ESP) 07- IPSec key group: DH1 08- Exch_mode: Main 09- Local identity: IP address 10- ID: 61.219.68.14 11-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

Device settings

DFL-1500/900

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

WAN1:



Address | Service | Schedule

[Objects] [Groups]

Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: Remote

Value

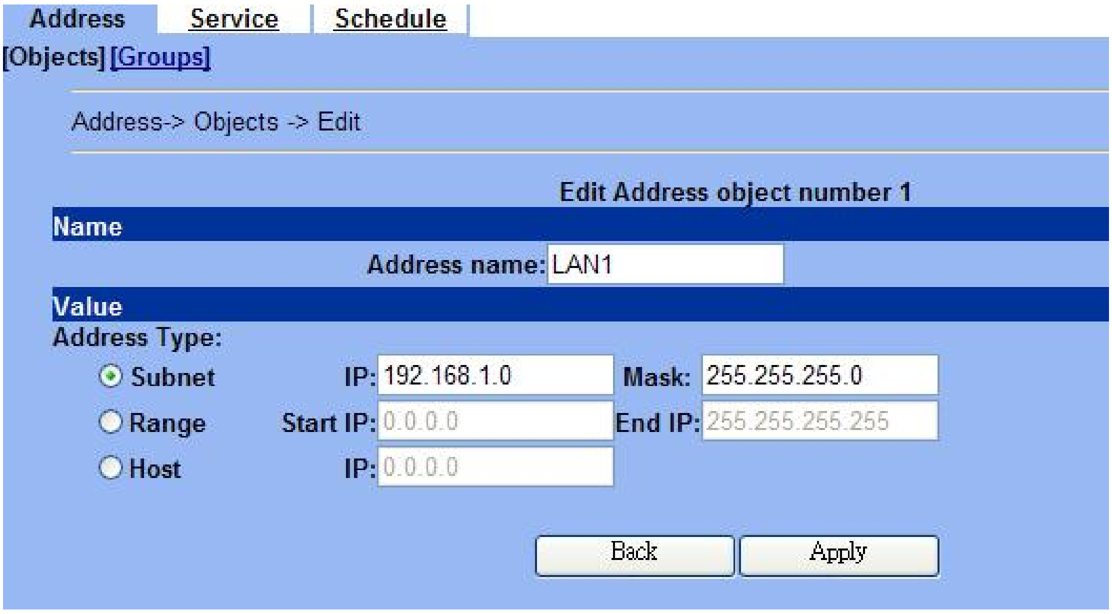
Address Type:

● Subnet IP: 61.219.68.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0

LAN1:



Address | Service | Schedule

[Objects] [Groups]

Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: LAN1

Value

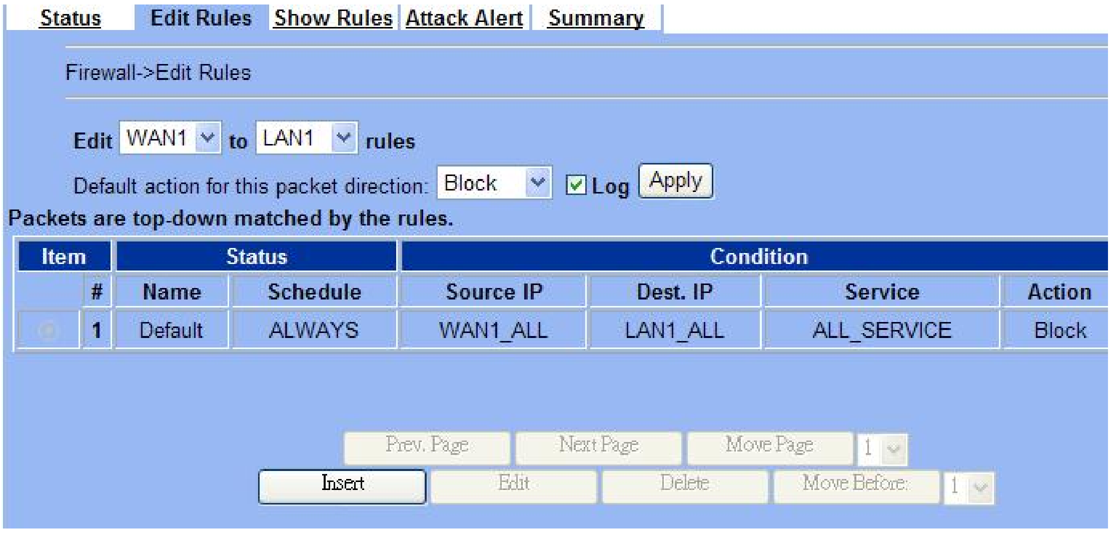
Address Type:

● Subnet IP: 192.168.1.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0

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



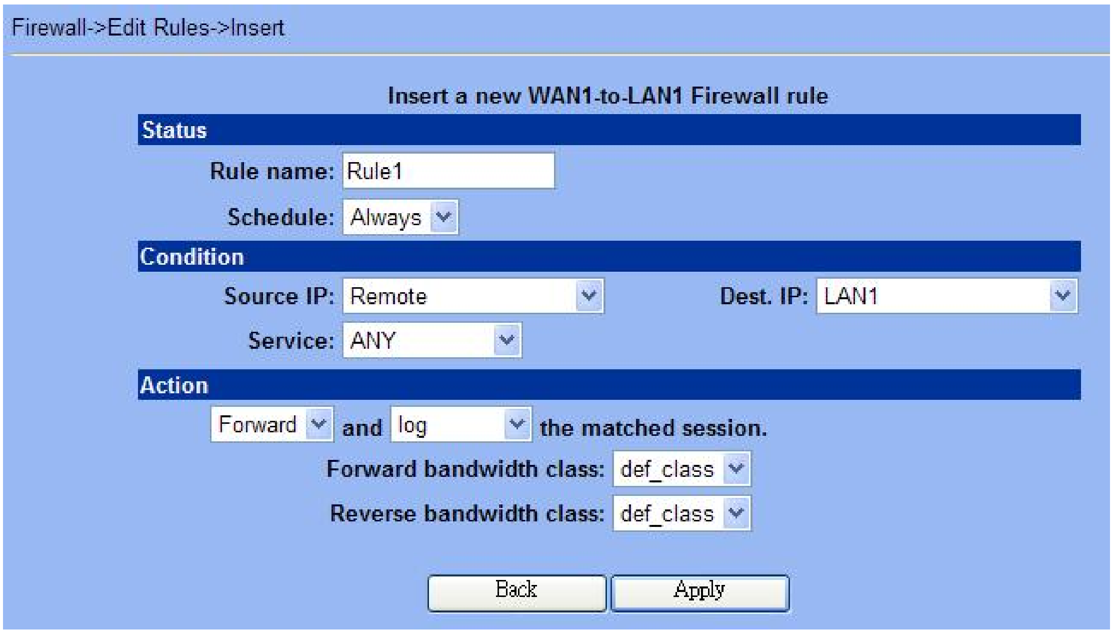
Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item	Status			Condition			
	#	Name	Schedule	Source IP	Dest. IP	Service	Action
○	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block


Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: Rule1

Schedule: Always

Condition

Source IP: Remote

Dest. IP: LAN1

Service: ANY

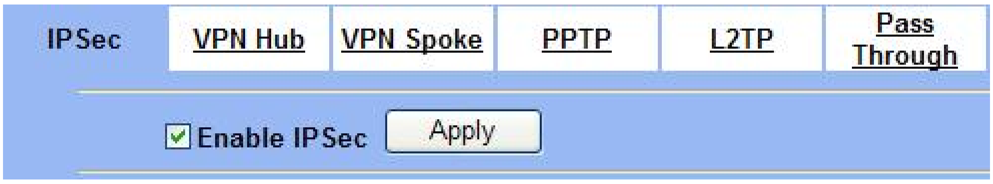
Action

Forward and log the matched session.

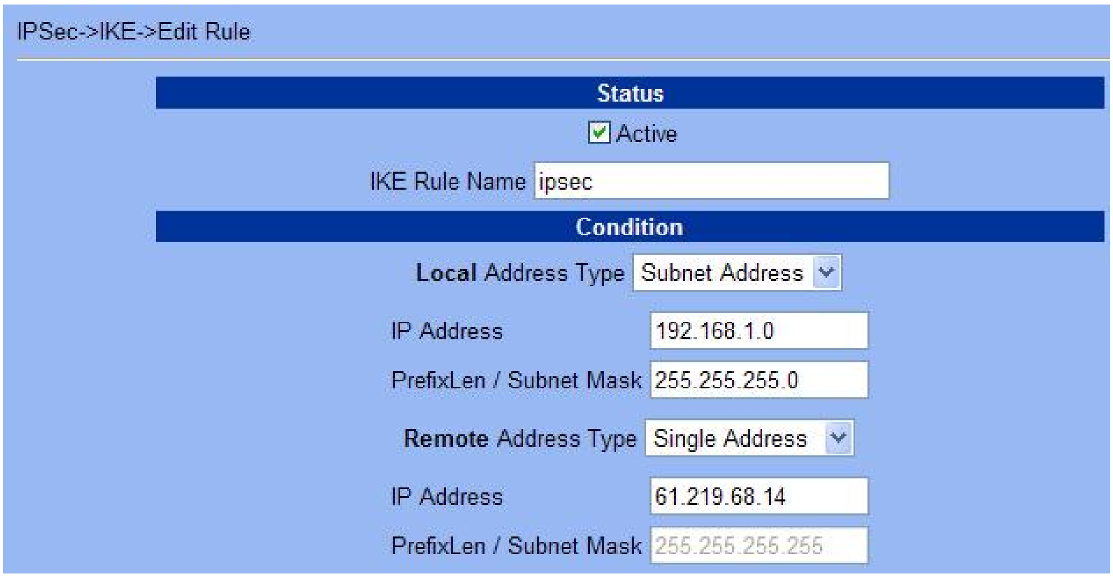
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

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



☑ Enable IPSec



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: ipsec

Condition

Local Address Type: Subnet Address

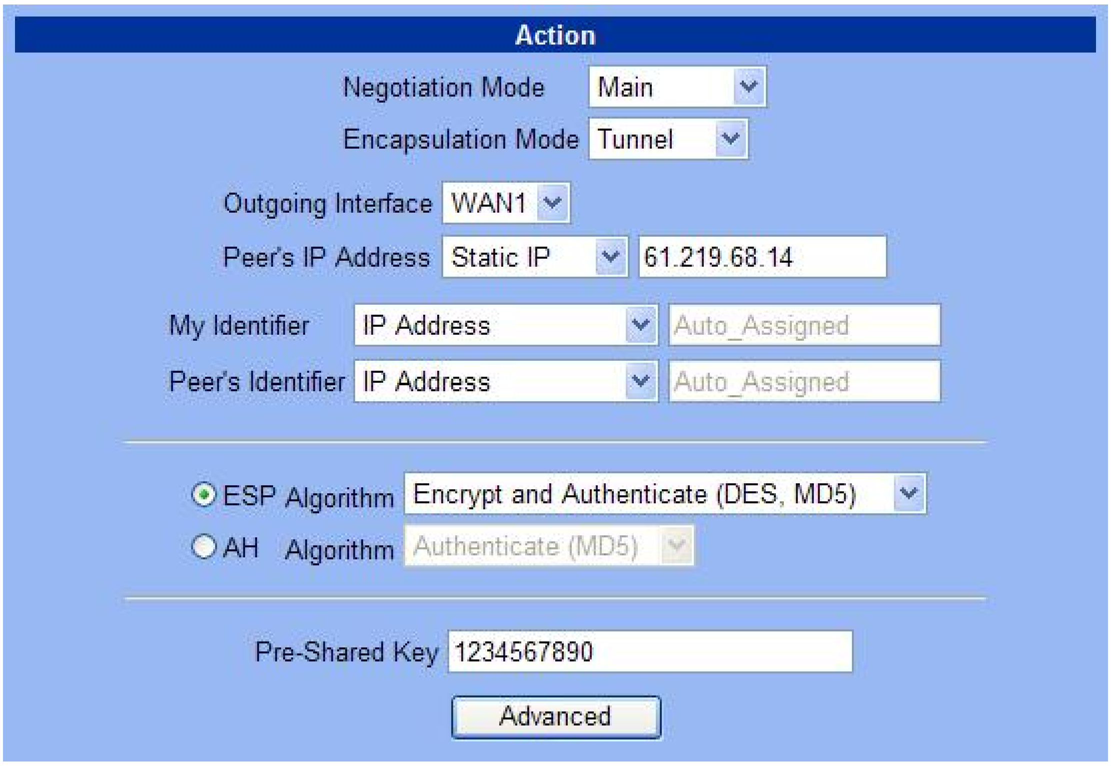
IP Address: 192.168.1.0

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

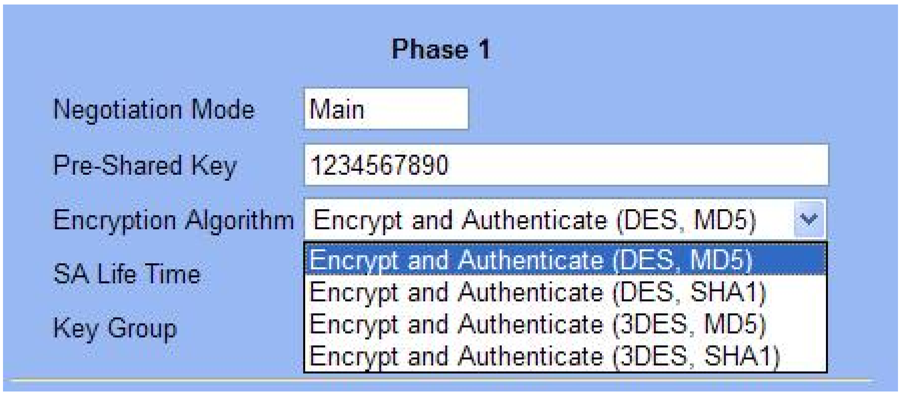
My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890



Phase 1

Negotiation Mode: Main

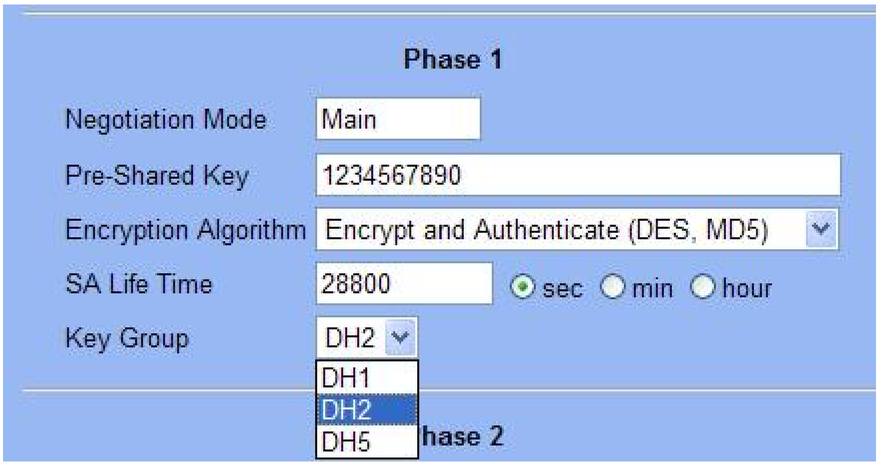
Pre-Shared Key: 1234567890

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

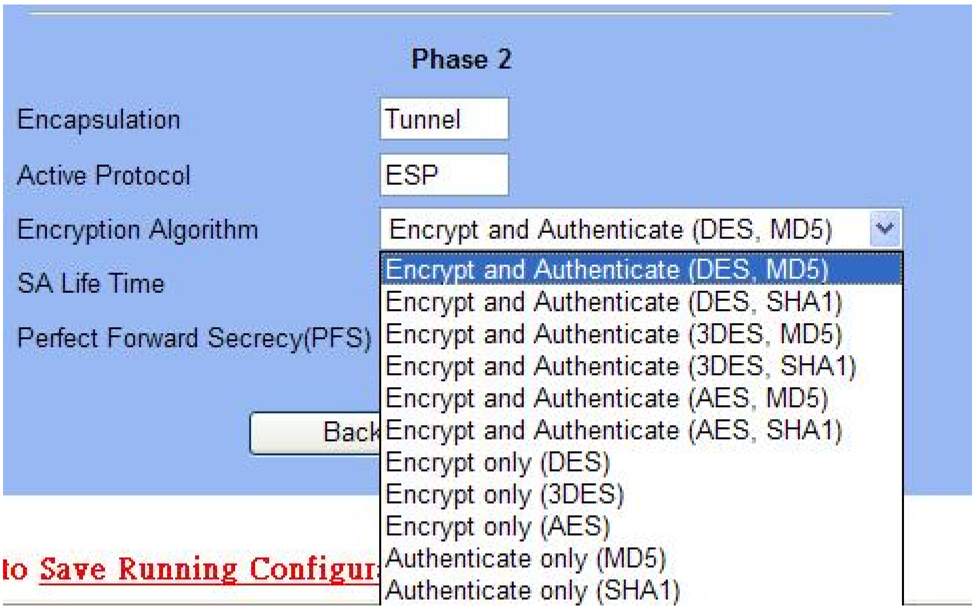
Negotiation Mode: Main

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Key Group: DH2



Phase 2

Encapsulation: Tunnel

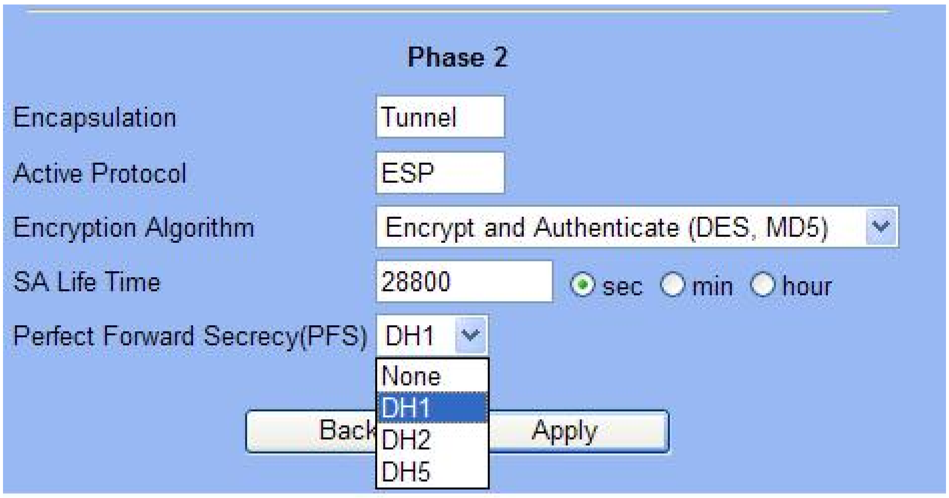
Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time

Perfect Forward Secrecy(PFS)

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)
Back
to Save Running Configur



Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

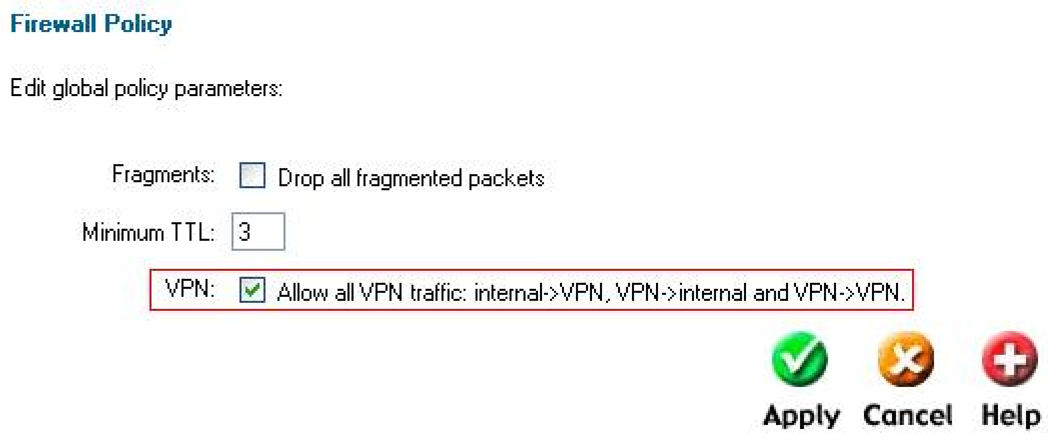
Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Perfect Forward Secrecy(PFS): DH1

DFL-1100/700/200

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



Firewall Policy

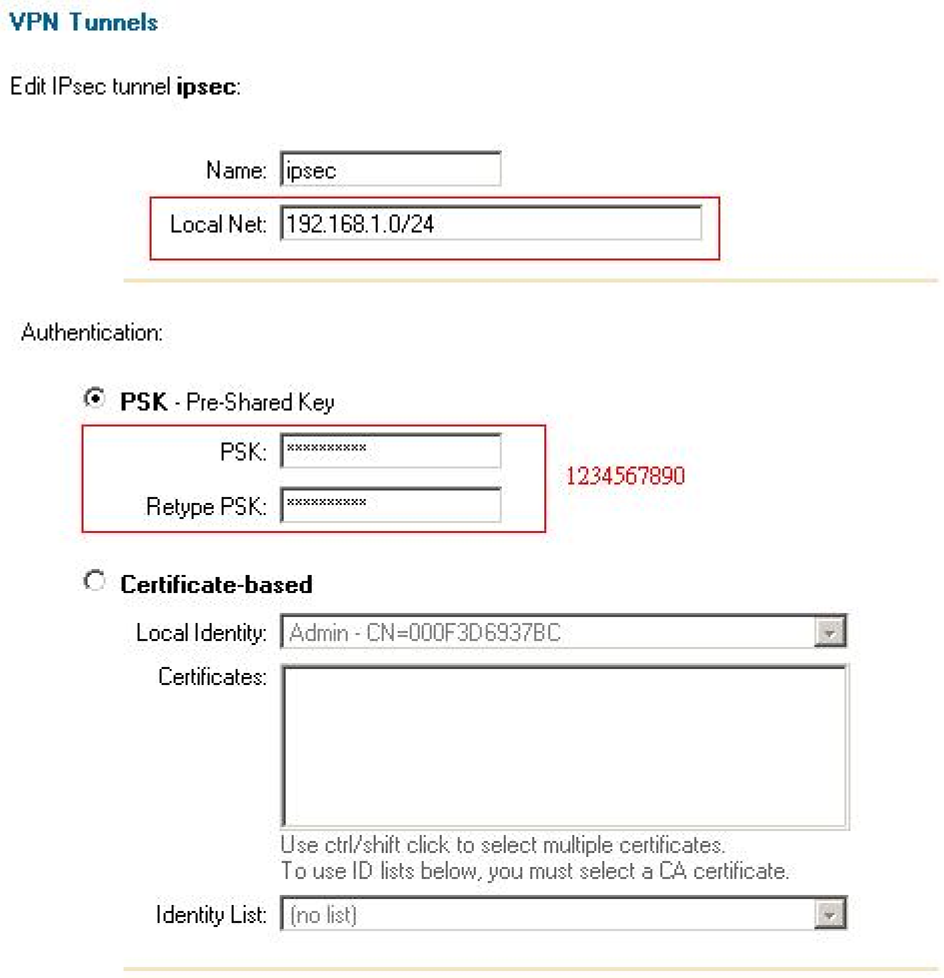
Edit global policy parameters:

Fragments: □ Drop all fragmented packets

Minimum TTL: 3

VPN: ☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

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



VPN Tunnels

Edit IPsec tunnel **ipsec**:

Name: ipsec

Local Net: 192.168.1.0/24

Authentication:

● **PSK** - Pre-Shared Key

PSK: **********

Retype PSK: **********

1234567890

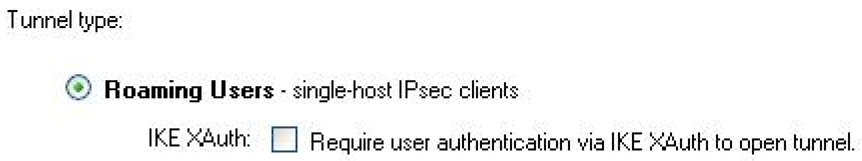
○ **Certificate-based**

Local Identity: Admin - CN=000F3D6937BC

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

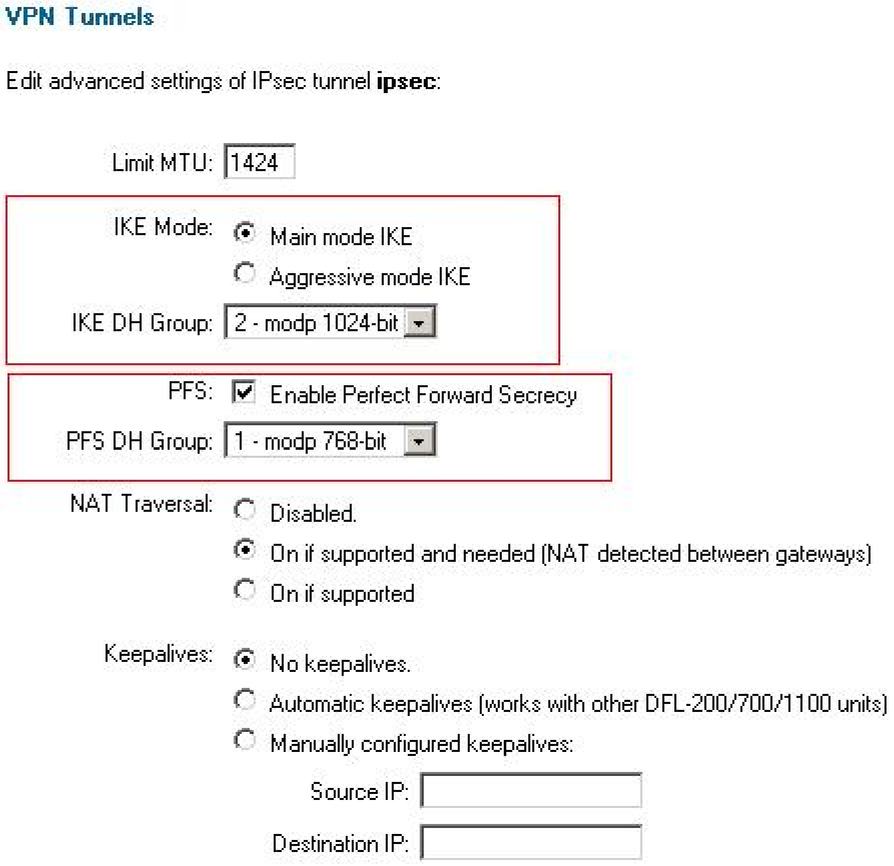
Identity List: (no list)



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

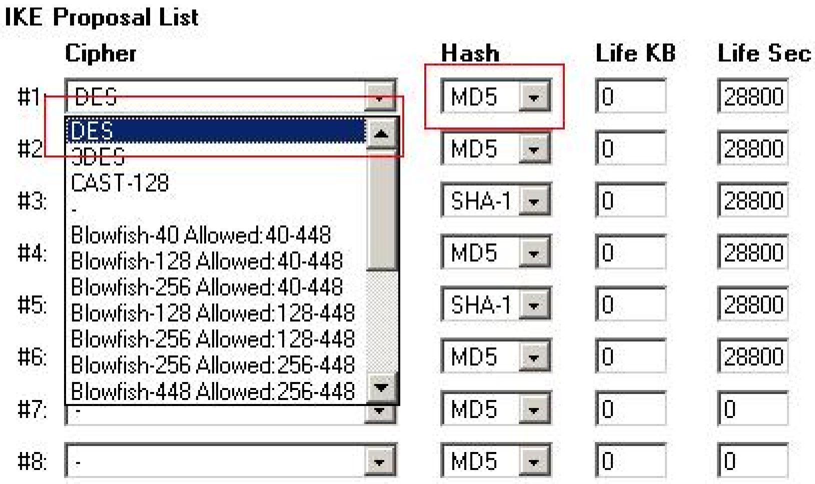
PFS DH Group: 1 - modp 768-bit

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:

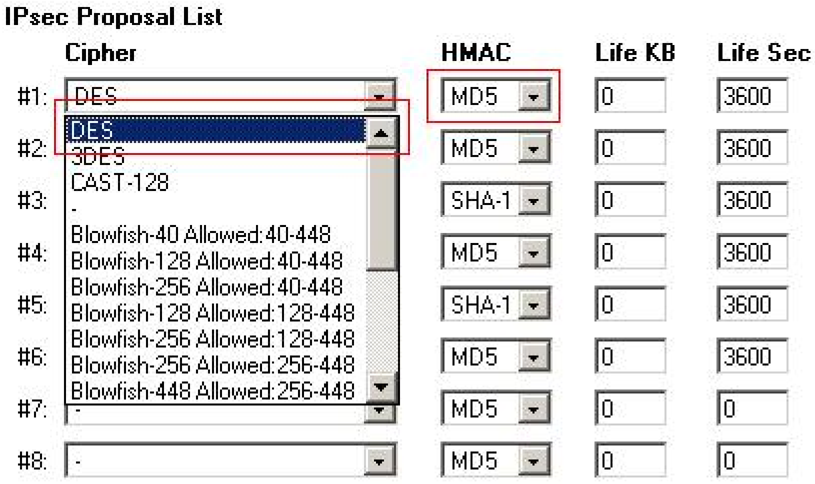
Destination IP:



IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1	DES	MD5	0	28800
#2		MD5	0	28800
#3:		SHA-1	0	28800
#4:		MD5	0	28800
#5:		SHA-1	0	28800
#6:		MD5	0	28800
#7:	-	MD5	0	0
#8:	-	MD5	0	0

DES
3DES
CAST-128
-
Blowfish-40 Allowed:40-448
Blowfish-128 Allowed:40-448
Blowfish-256 Allowed:40-448
Blowfish-128 Allowed:128-448
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448



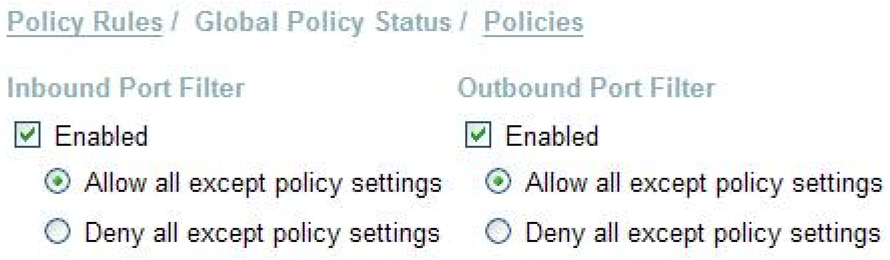
IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:		MD5	0	3600
#3:		SHA-1	0	3600
#4:		MD5	0	3600
#5:		SHA-1	0	3600
#6:		MD5	0	3600
#7:	-	MD5	0	0
#8:	-	MD5	0	0

DES
3DES
CAST-128
-
Blowfish-40 Allowed:40-448
Blowfish-128 Allowed:40-448
Blowfish-256 Allowed:40-448
Blowfish-128 Allowed:128-448
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

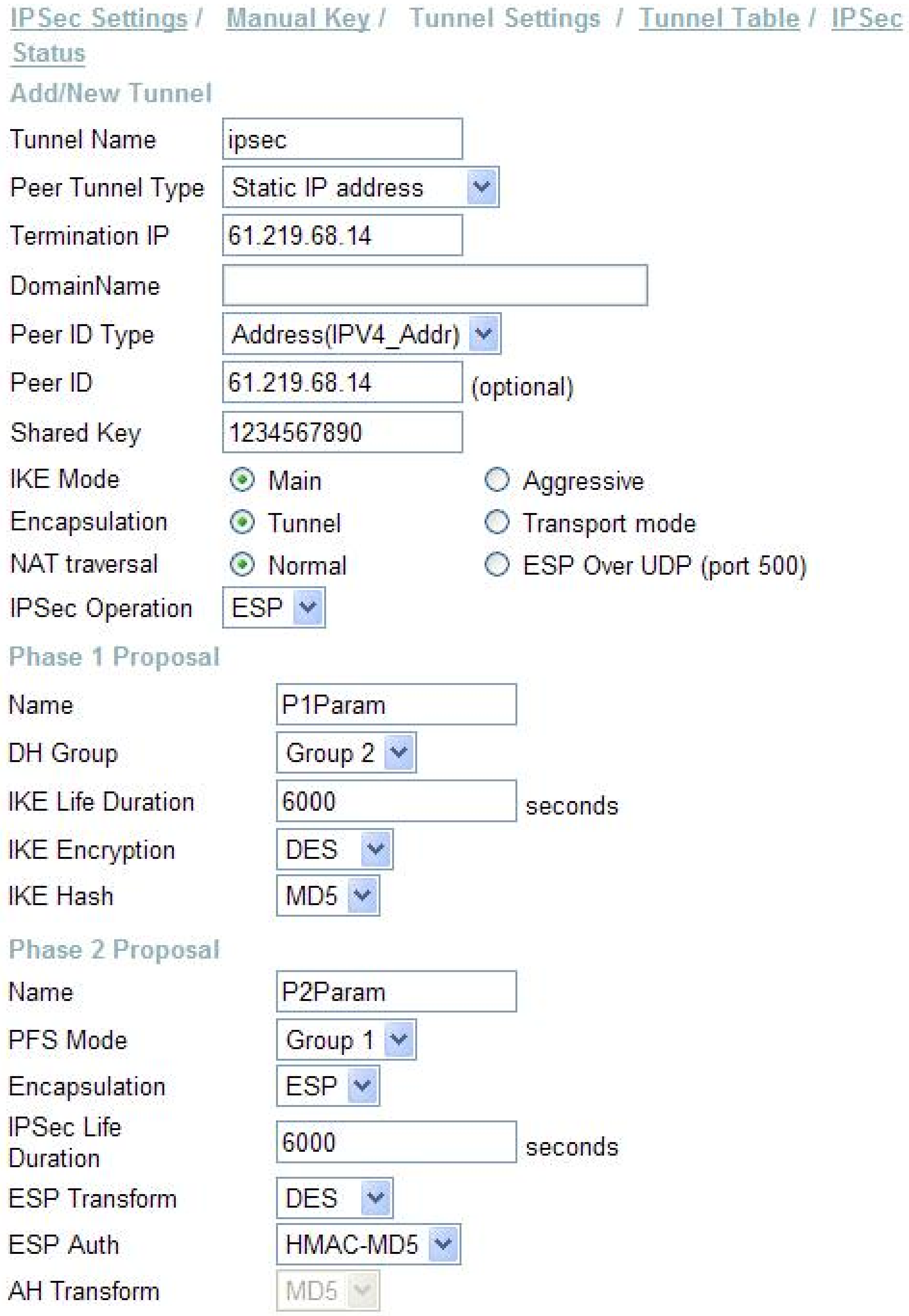
DFL-600

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



Inbound Port Filter	Outbound Port Filter
☑ Enabled	☑ Enabled
● Allow all except policy settings	● Allow all except policy settings
○ Deny all except policy settings	○ Deny all except policy settings

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



IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status

Add/New Tunnel

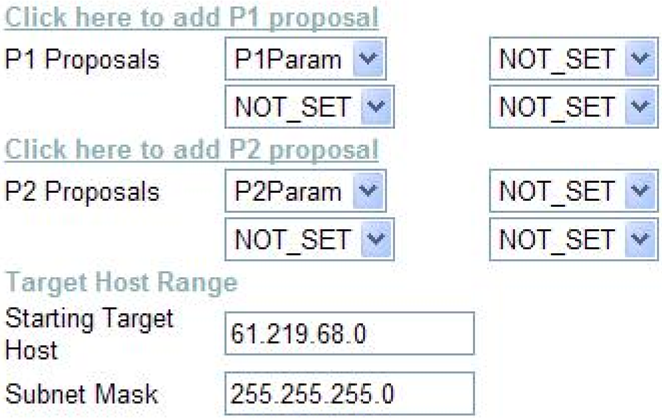
Tunnel Name	ipsec	
Peer Tunnel Type	Static IP address	
Termination IP	61.219.68.14	
DomainName		
Peer ID Type	Address(IPV4_Addr)	
Peer ID	61.219.68.14	(optional)
Shared Key	1234567890	
IKE Mode	● Main	○ Aggressive
Encapsulation	● Tunnel	○ Transport mode
NAT traversal	● Normal	○ ESP Over UDP (port 500)
IPSec Operation	ESP	

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

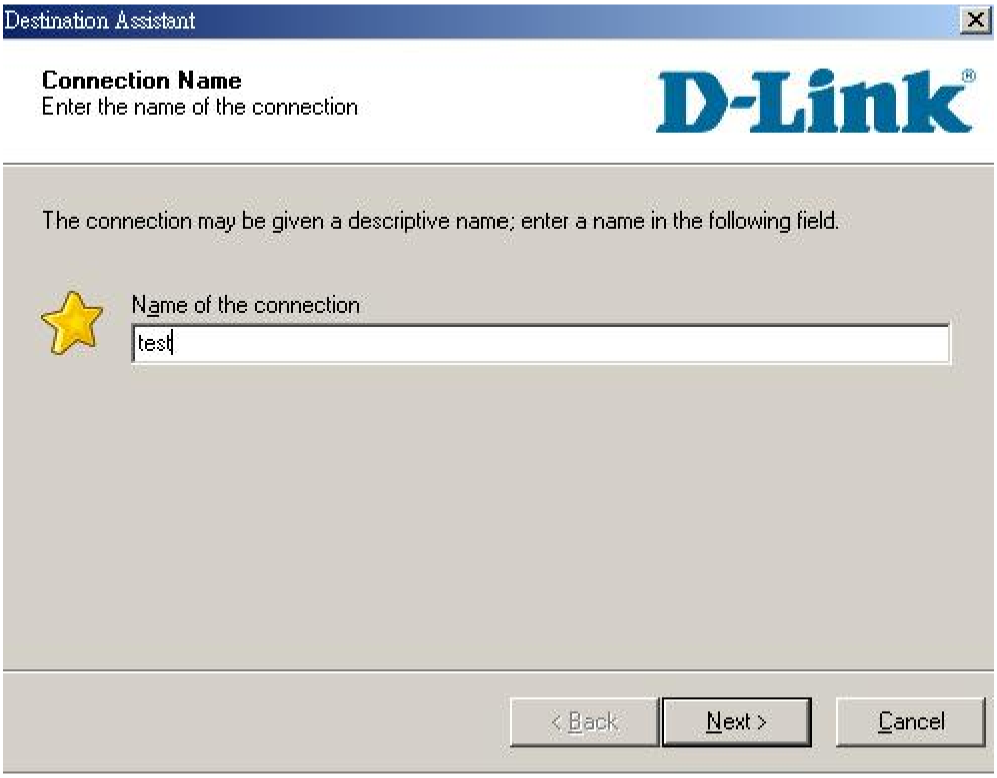
Target Host Range

Starting Target Host	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

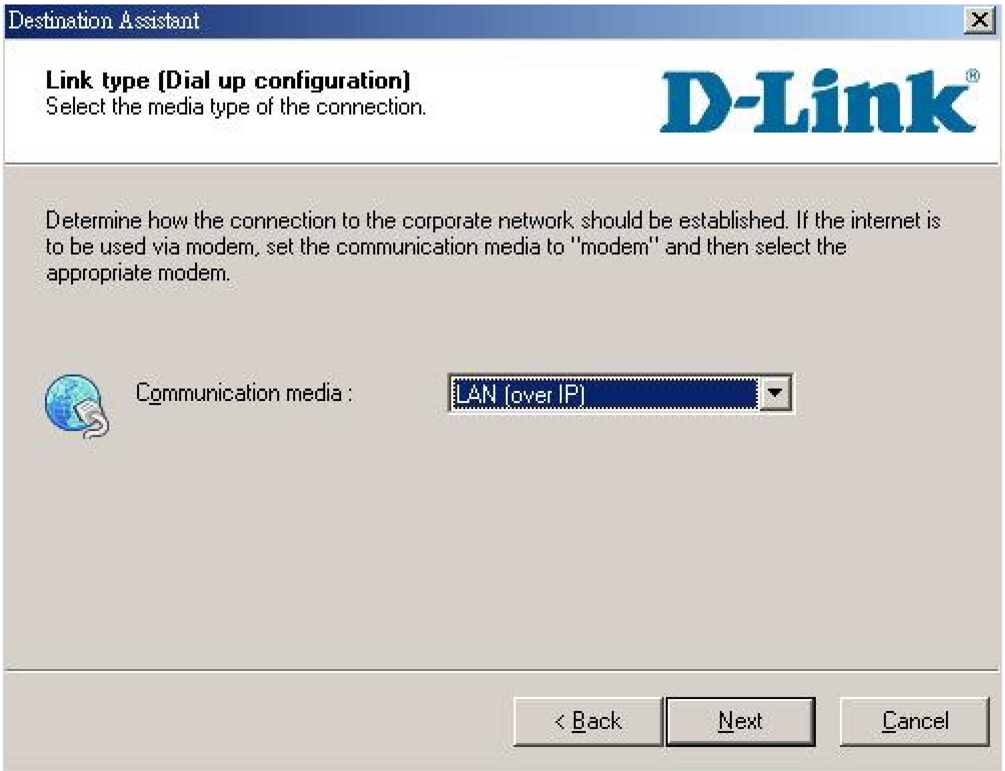


The connection may be given a descriptive name; enter a name in the following field.

Name of the connection: test

Setup2

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



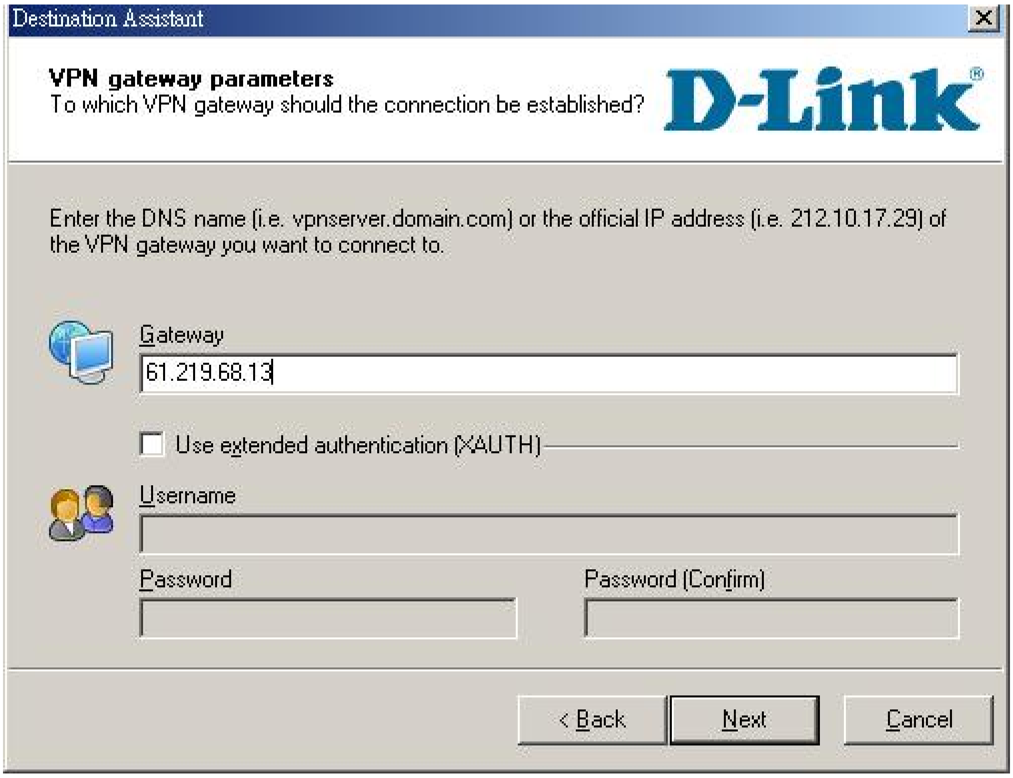
Destination Assistant
Link type (Dial up configuration)
Select the media type of the connection.
D-Link

Determine how the connection to the corporate network should be established. If the internet is to be used via modem, set the communication media to "modem" and then select the appropriate modem.

Communication media : LAN (over IP)

Setup3

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



Destination Assistant

VPN gateway parameters

To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.

Gateway: 61.219.68.13

□ Use extended authentication (XAUTH)

Username:

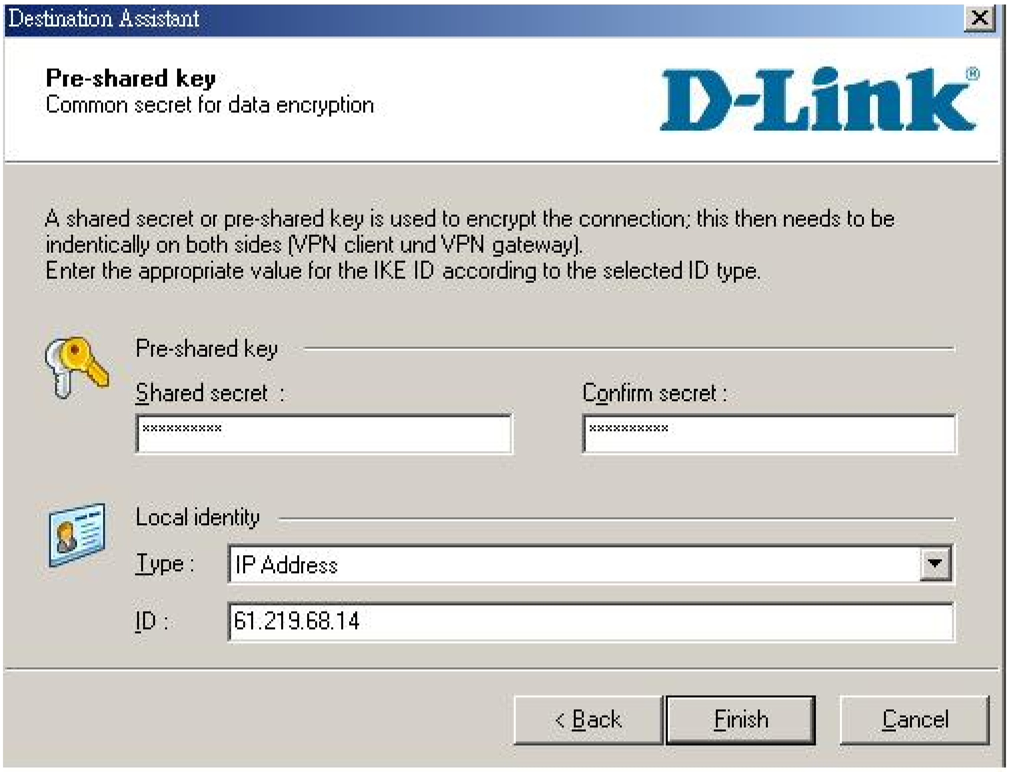
Password:

Password (Confirm):

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.



Destination Assistant

Pre-shared key

Common secret for data encryption

A shared secret or pre-shared key is used to encrypt the connection; this then needs to be indentically on both sides (VPN client und VPN gateway).
Enter the appropriate value for the IKE ID according to the selected ID type.

Pre-shared key

Shared secret : **********

Confirm secret : **********

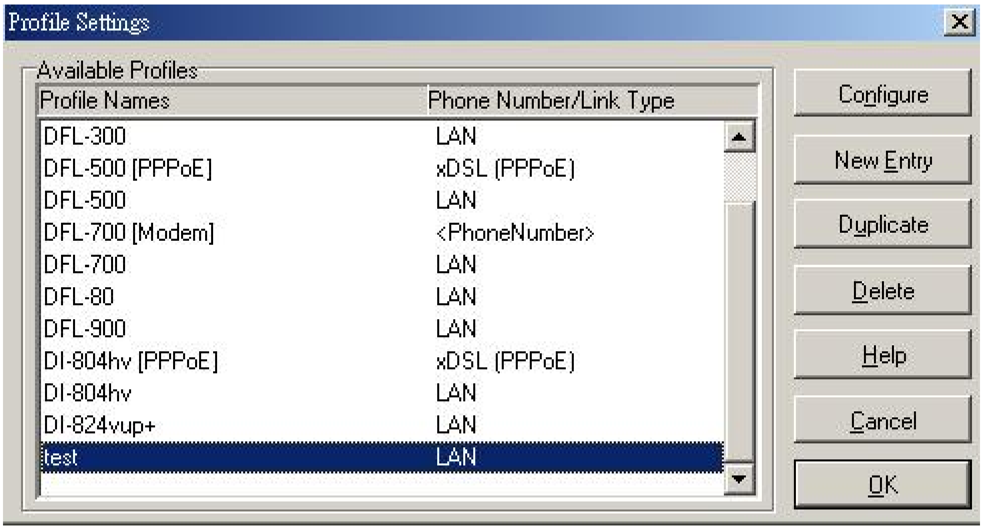
Local identity

Type : IP Address

ID : 61.219.68.14

Setup5

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



Profile Settings

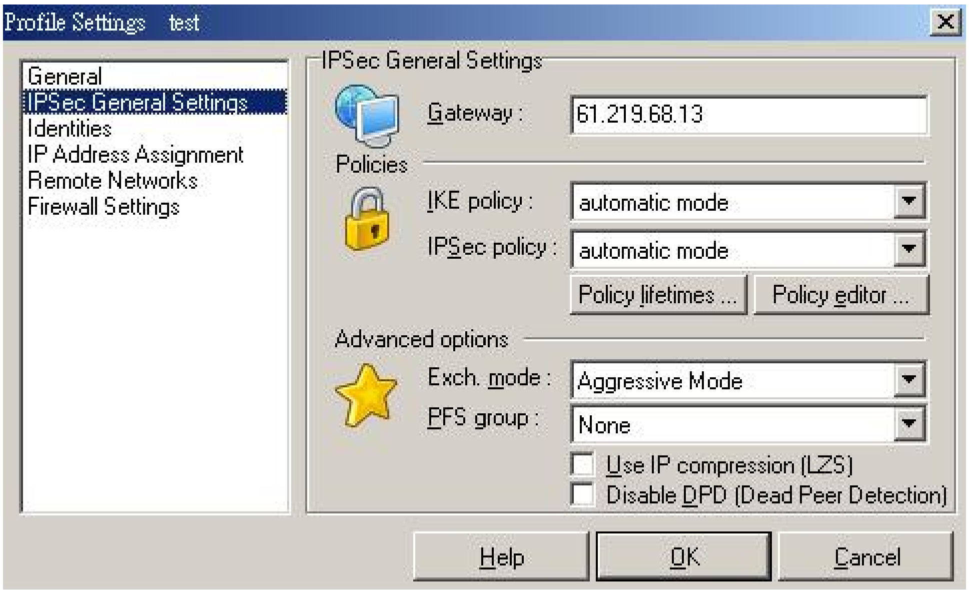
Available Profiles

Profile Names	Phone Number/Link Type
DFL-300	LAN
DFL-500 [PPPoE]	xDSL (PPPoE)
DFL-500	LAN
DFL-700 [Modem]	<PhoneNumber>
DFL-700	LAN
DFL-80	LAN
DFL-900	LAN
DI-804hv [PPPoE]	xDSL (PPPoE)
DI-804hv	LAN
DI-824vup+	LAN
test	LAN

Setup6

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

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



Profile Settings test

General
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Firewall Settings

IPSec General Settings

Gateway : 61.219.68.13

Policies

IKE policy : automatic mode

IPSec policy : automatic mode

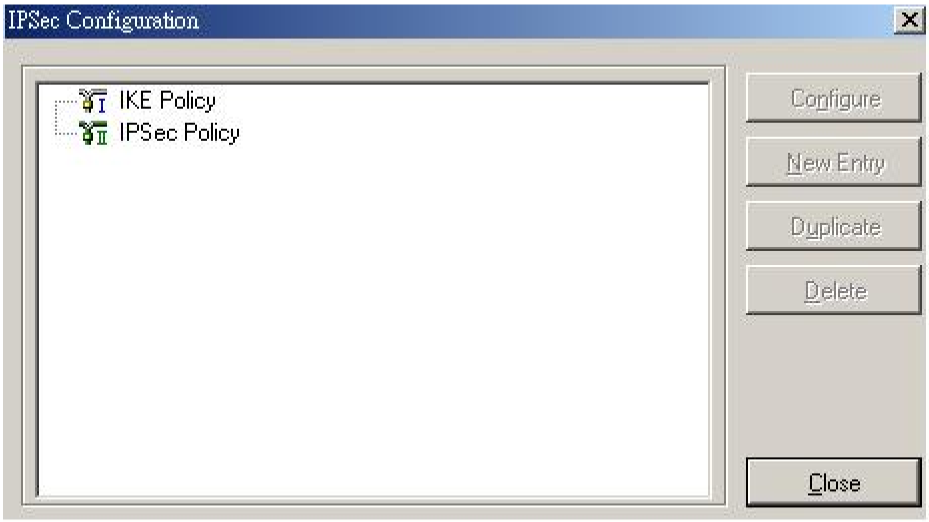
Advanced options

Exch. mode : Aggressive Mode

PFS group : None

□ Use IP compression (LZS)

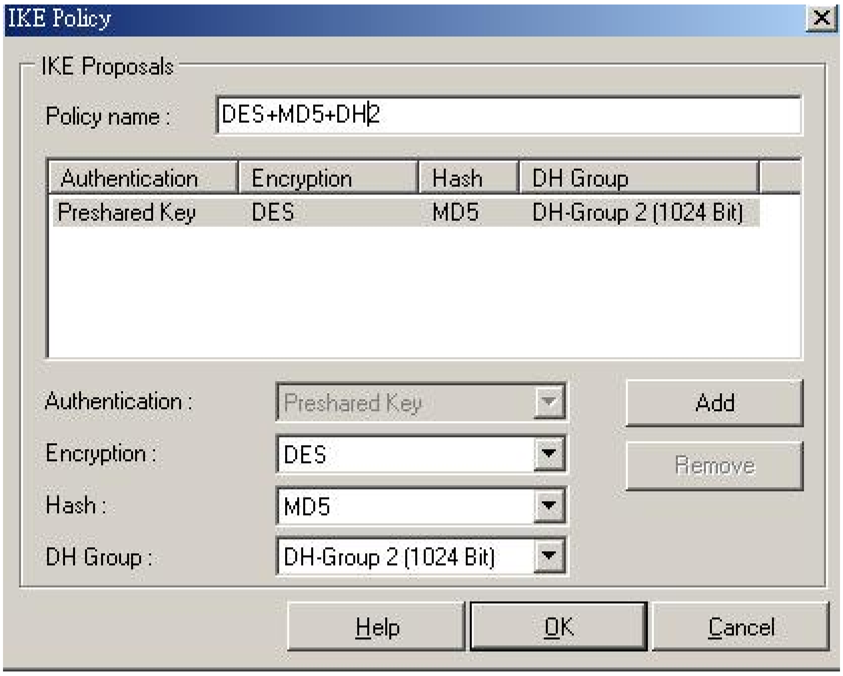
□ Disable DPD (Dead Peer Detection)



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.



Policy name : DES+MD5+DH2

Authentication	Encryption	Hash	DH Group
Preshared Key	DES	MD5	DH-Group 2 (1024 Bit)

Authentication : Preshared Key

Encryption : DES

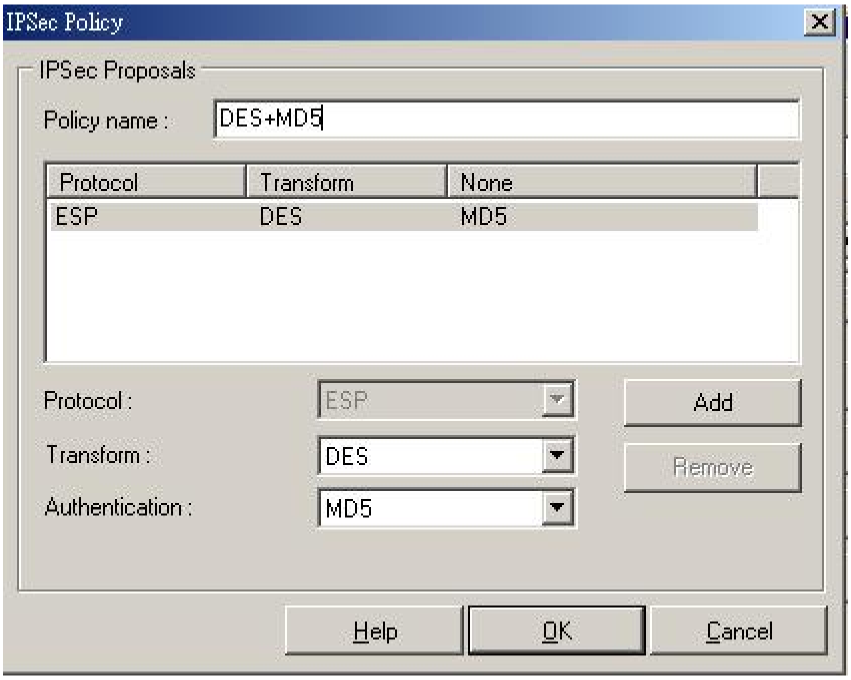
Hash : MD5

DH Group : DH-Group 2 (1024 Bit)

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.



IPSec Policy

IPSec Proposals

Policy name : DES+MD5

Protocol	Transform	None
ESP	DES	MD5

Protocol : ESP

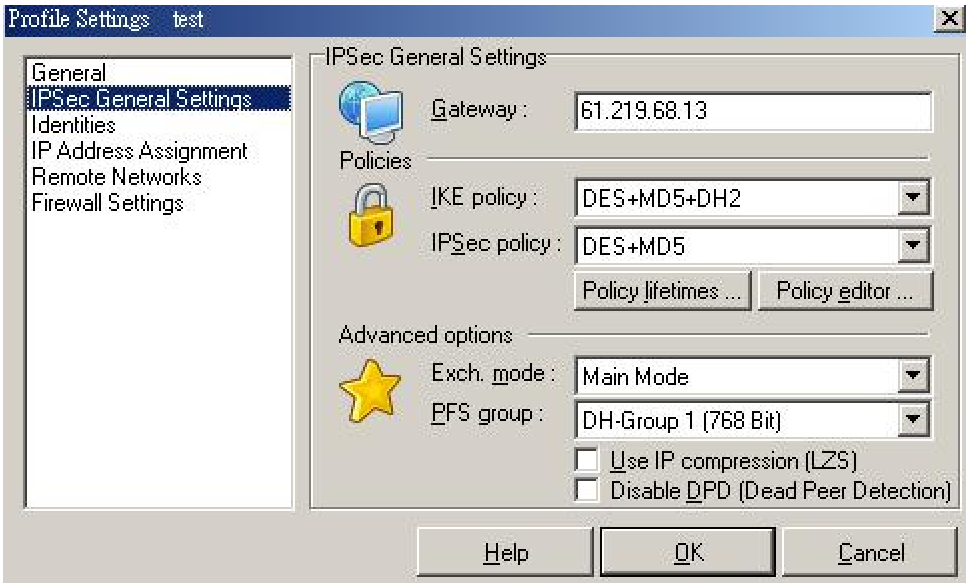
Transform : DES

Authentication : MD5

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



Profile Settings test

IPSec General Settings

Gateway : 61.219.68.13

Policies

IKE policy : DES+MD5+DH2

IPSec policy : DES+MD5

Advanced options

Exch. mode : Main Mode

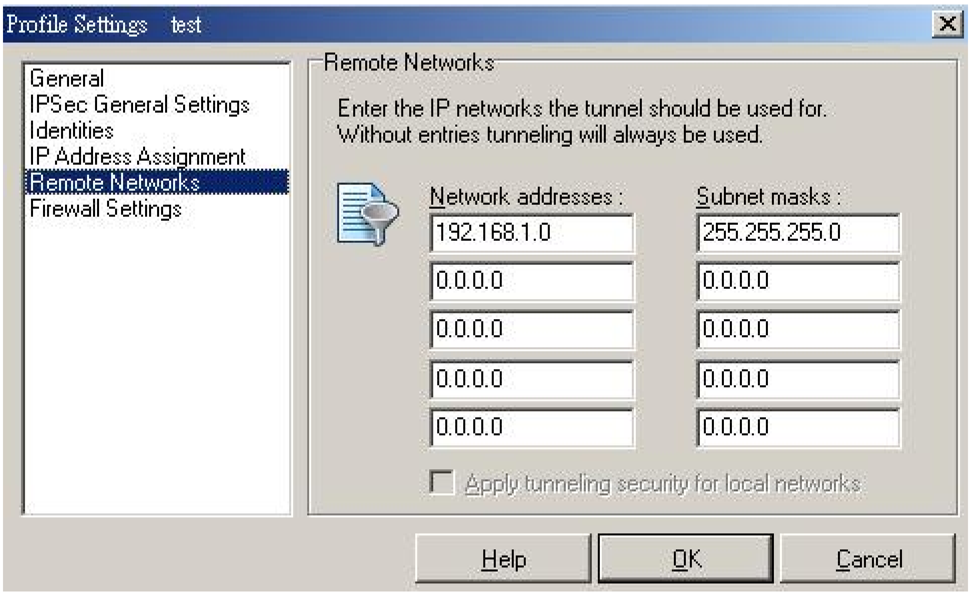
PFS group : DH-Group 1 (768 Bit)

□ Use IP compression (LZS)

□ Disable DPD (Dead Peer Detection)

Setup10

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



Remote Networks

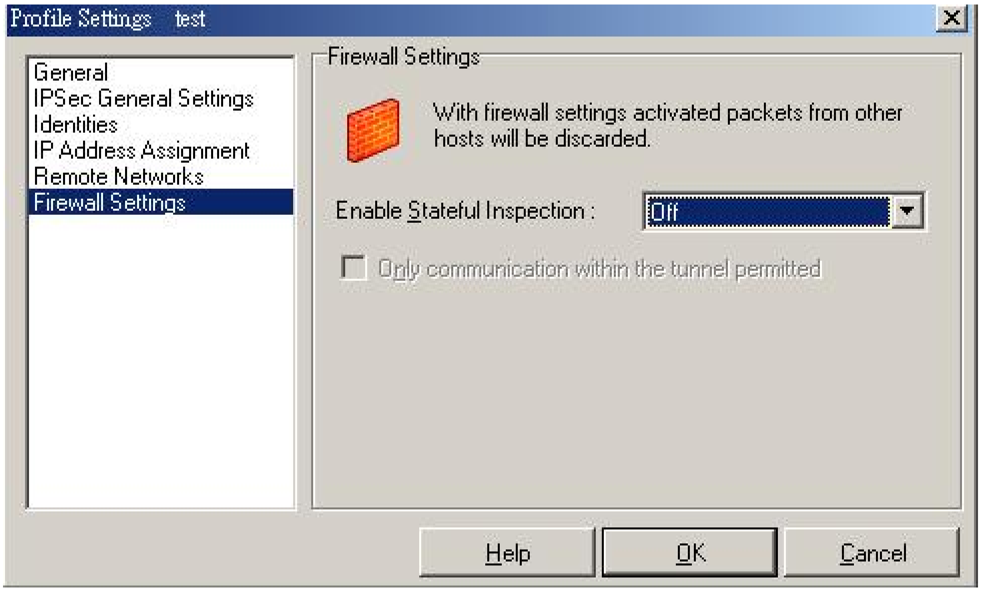
Enter the IP networks the tunnel should be used for.
Without entries tunneling will always be used.

Network addresses :	Subnet masks :
192.168.1.0	255.255.255.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

□ Apply tunneling security for local networks

Setup11

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



Firewall Settings

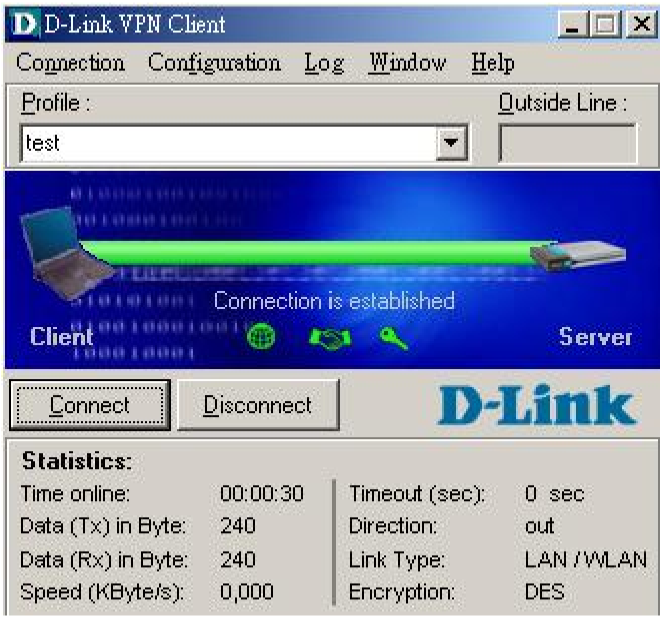
With firewall settings activated packets from other hosts will be discarded.

Enable Stateful Inspection : Off

□ Only communication within the tunnel permitted

Setup12

Click **Connect** button to establish IPSec tunnel



Profile : test

Connection is established

Statistics:

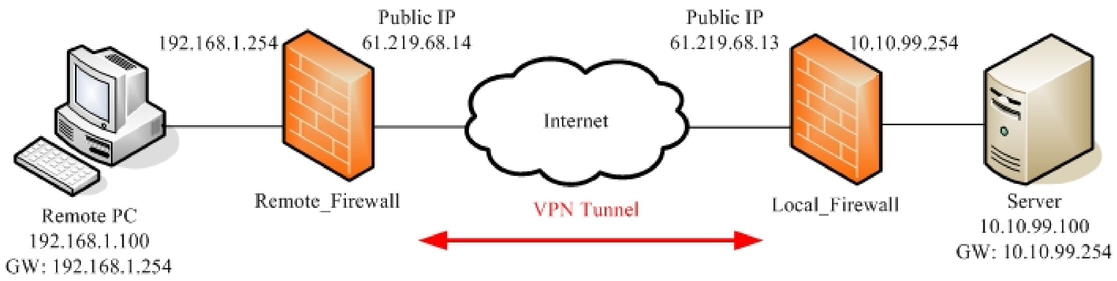
Time online:	00:00:30	Timeout (sec):	0 sec
Data (Tx) in Byte:	240	Direction:	out
Data (Rx) in Byte:	240	Link Type:	LAN / WLAN
Speed (KByte/s):	0,000	Encryption:	DES

2. LAN to LAN

2-1 Objective:

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

2-2 Environment:



Configure a LAN to LAN (PPTP/L2TP/IPSec) VPN Dial-in Connection

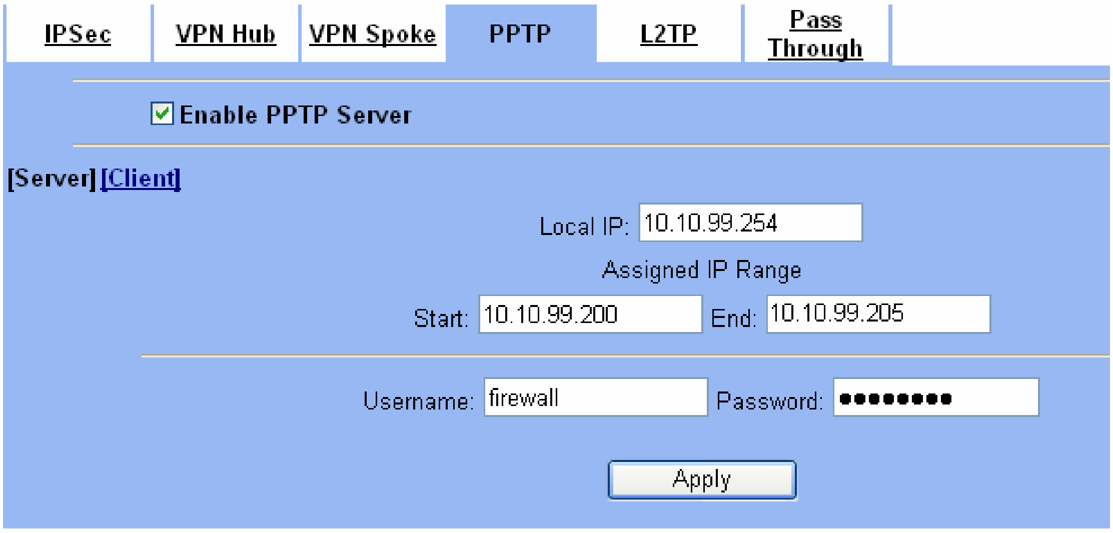
2-3 Setups:

2-3-1 PPTP Server & PPTP Client

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

DFL-1500

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



☑ Enable PPTP Server

[Server] [Client]

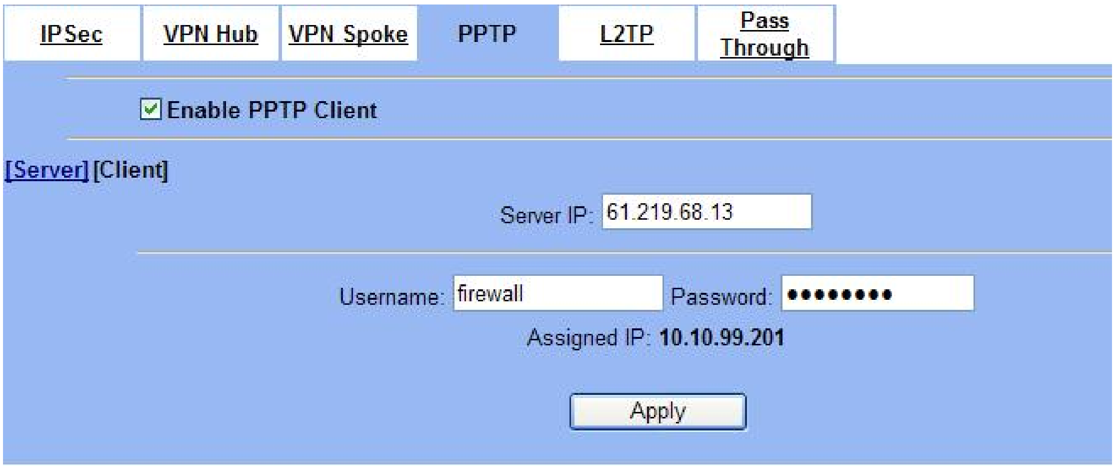
Local IP: 10.10.99.254

Assigned IP Range

Start: 10.10.99.200 End: 10.10.99.205

Username: firewall Password: ●●●●●●●●●

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



☑ Enable PPTP Client

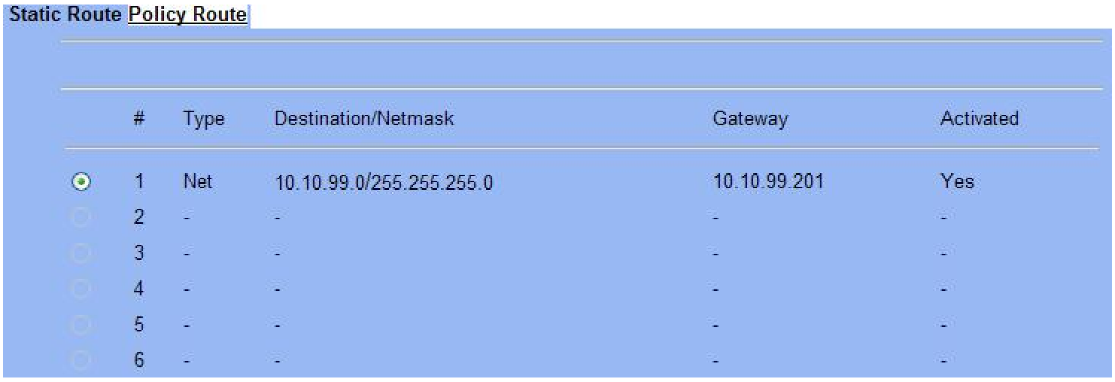
[Server] [Client]

Server IP: 61.219.68.13

Username: firewall Password: ●●●●●●●●

Assigned IP: **10.10.99.201**

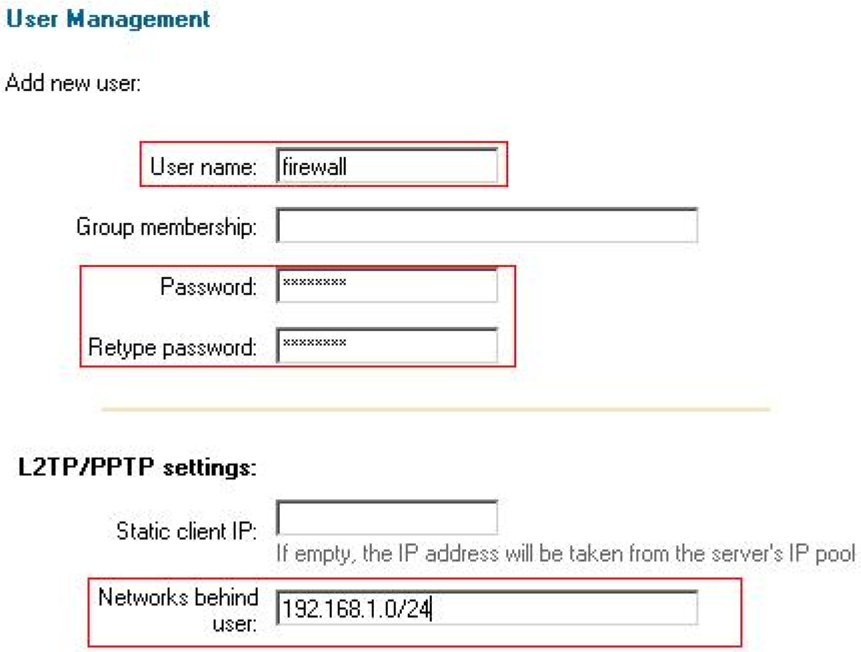
03- Add a static routing table (**Advanced settings -> Routing -> Static Route**)



	#	Type	Destination/Netmask	Gateway	Activated
●	1	Net	10.10.99.0/255.255.255.0	10.10.99.201	Yes
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-	-	-
○	6	-	-	-	-

DFL-1100/700/200

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



User Management

Add new user:

User name: firewall

Group membership:

Password: ********

Retype password: ********

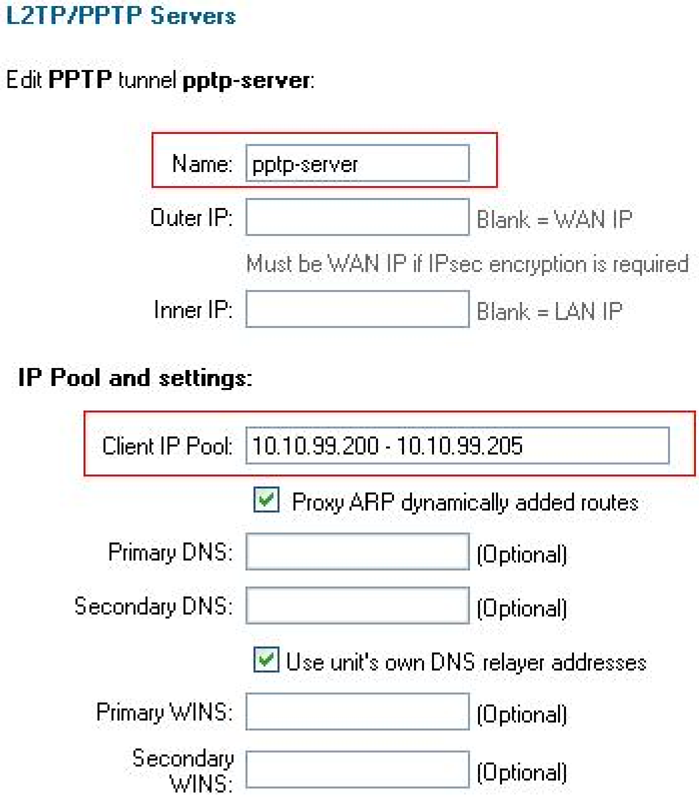
L2TP/PPTP settings:

Static client IP:

If empty, the IP address will be taken from the server's IP pool

Networks behind user: 192.168.1.0/24

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



L2TP/PPTP Servers

Edit **PPTP** tunnel **pptp-server**:

Name: pptp-server

Outer IP: Blank = WAN IP

Must be WAN IP if IPsec encryption is required

Inner IP: Blank = LAN IP

IP Pool and settings:

Client IP Pool: 10.10.99.200 - 10.10.99.205

☑ Proxy ARP dynamically added routes

Primary DNS: (Optional)

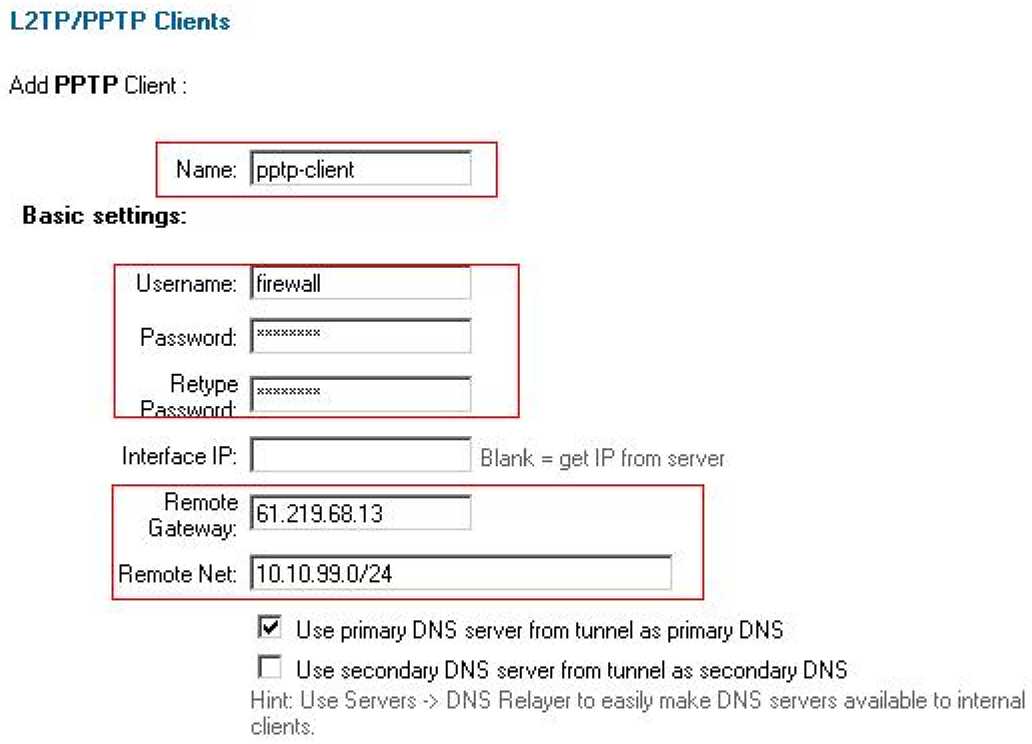
Secondary DNS: (Optional)

☑ Use unit's own DNS relayer addresses

Primary WINS: (Optional)

Secondary WINS: (Optional)

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



L2TP/PPTP Clients

Add PPTP Client :

Name: pptp-client

Basic settings:

Username: firewall

Password: ********

Retype Password: ********

Interface IP: Blank = get IP from server

Remote Gateway: 61.219.68.13

Remote Net: 10.10.99.0/24

☑ Use primary DNS server from tunnel as primary DNS

☐ Use secondary DNS server from tunnel as secondary DNS

Hint: Use Servers -> DNS Relayer to easily make DNS servers available to internal clients.

2-3-2 L2TP Server & L2TP Client

Remote_Firewall settings	Local_Firewall settings

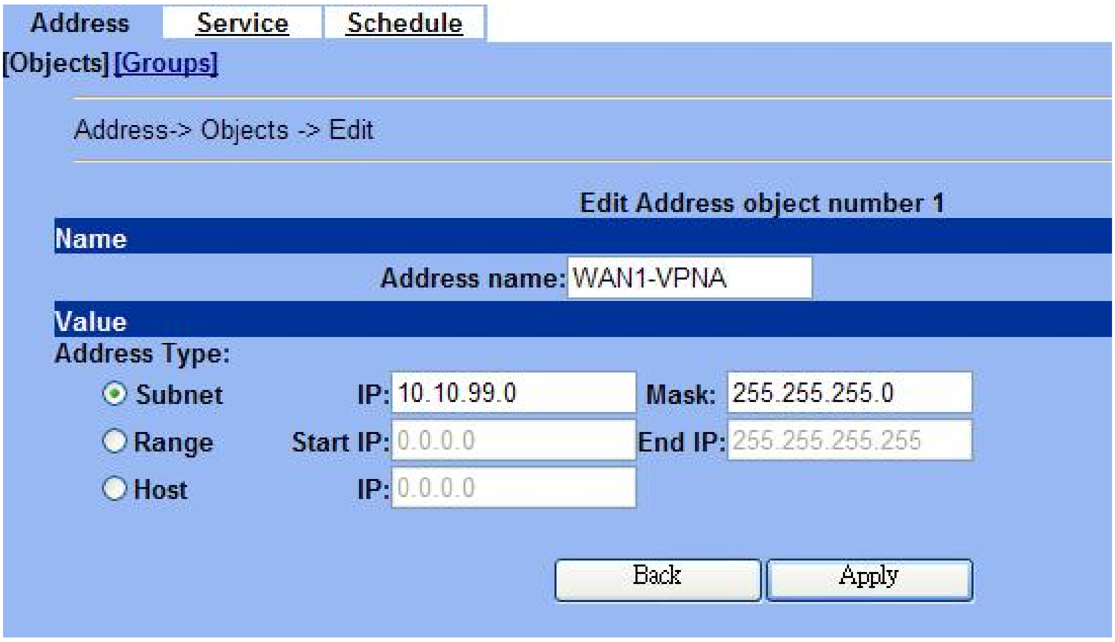
2-3-3 IPSec

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

DFL-1500

Remote_Firewall:

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



Address | Service | Schedule

[Objects] [Groups]

Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: WAN1-VPNA

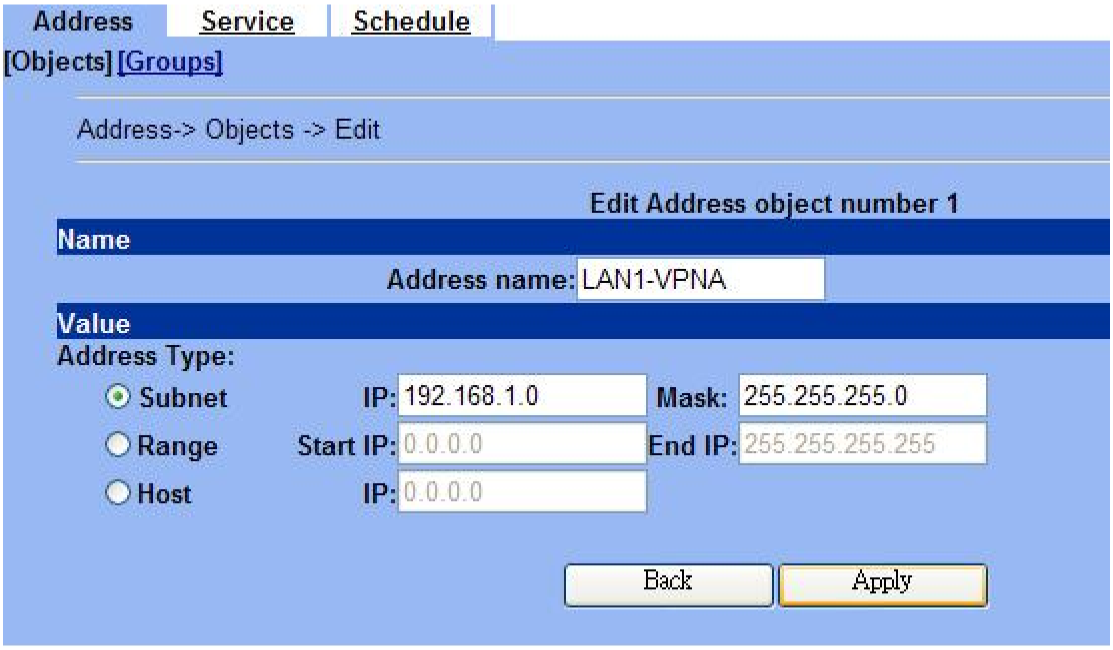
Value

Address Type:

● Subnet IP: 10.10.99.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0



Address | Service | Schedule

[Objects] [Groups]

Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: LAN1-VPNA

Value

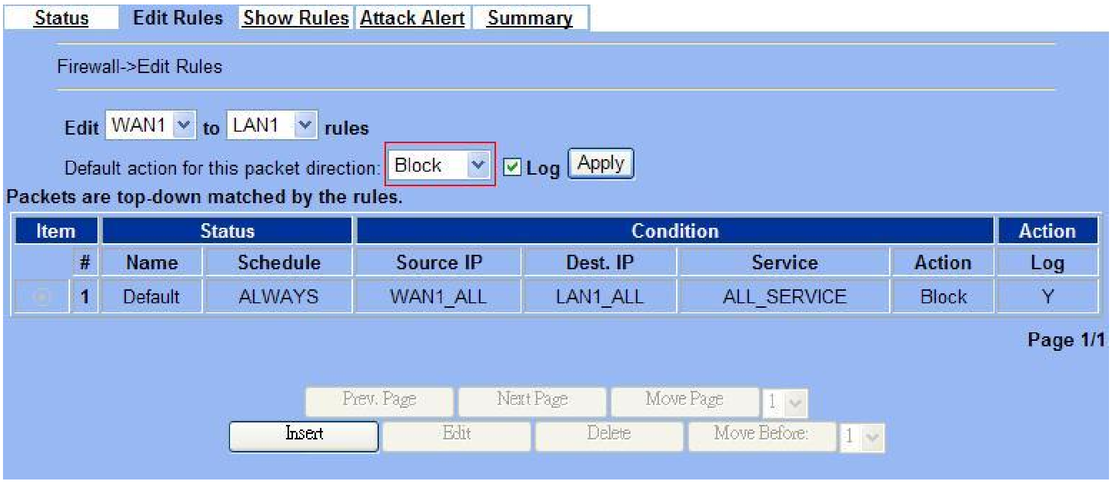
Address Type:

● Subnet IP: 192.168.1.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0

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



Firewall->Edit Rules

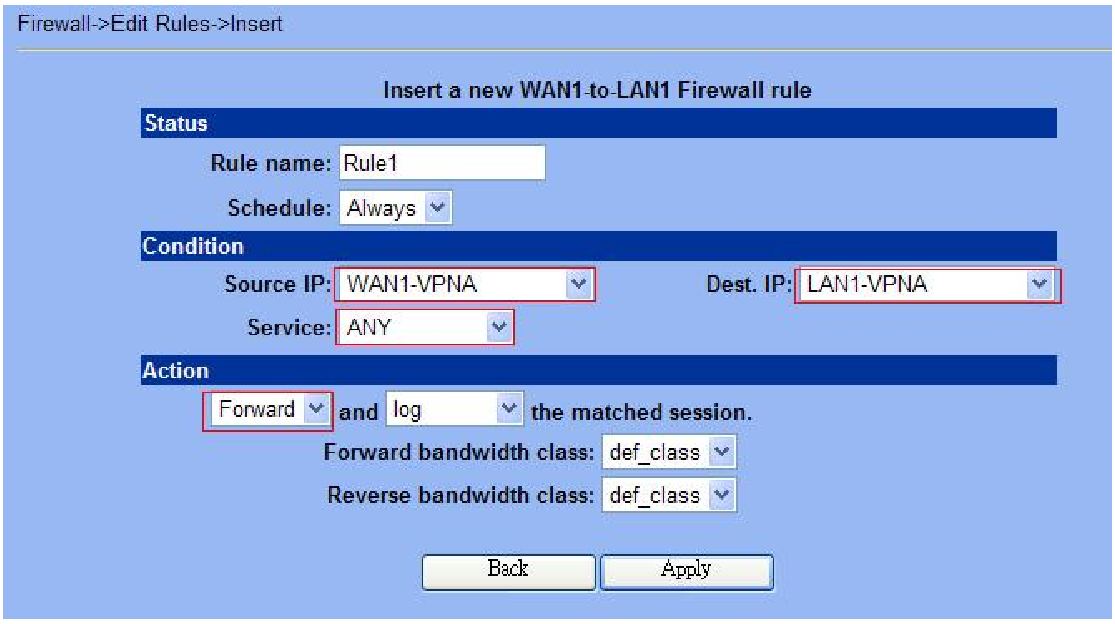
Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item	Status			Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
○	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1


Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: Rule1

Schedule: Always

Condition

Source IP: WAN1-VPNA Dest. IP: LAN1-VPNA

Service: ANY

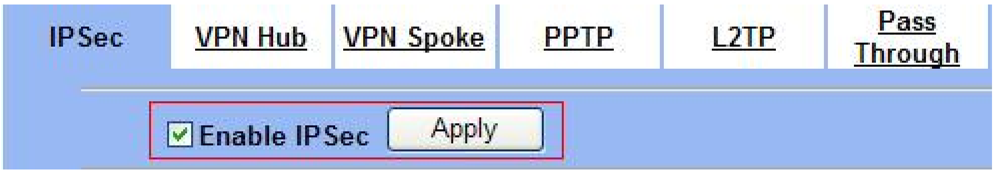
Action

Forward and log the matched session.

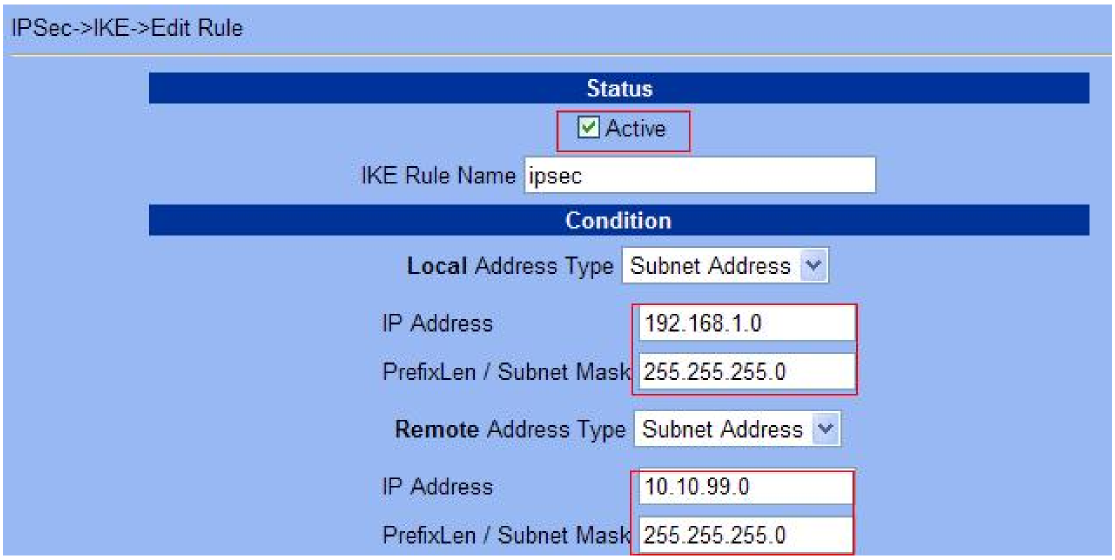
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

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



☑ Enable IPSec Apply



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: ipsec

Condition

Local Address Type: Subnet Address

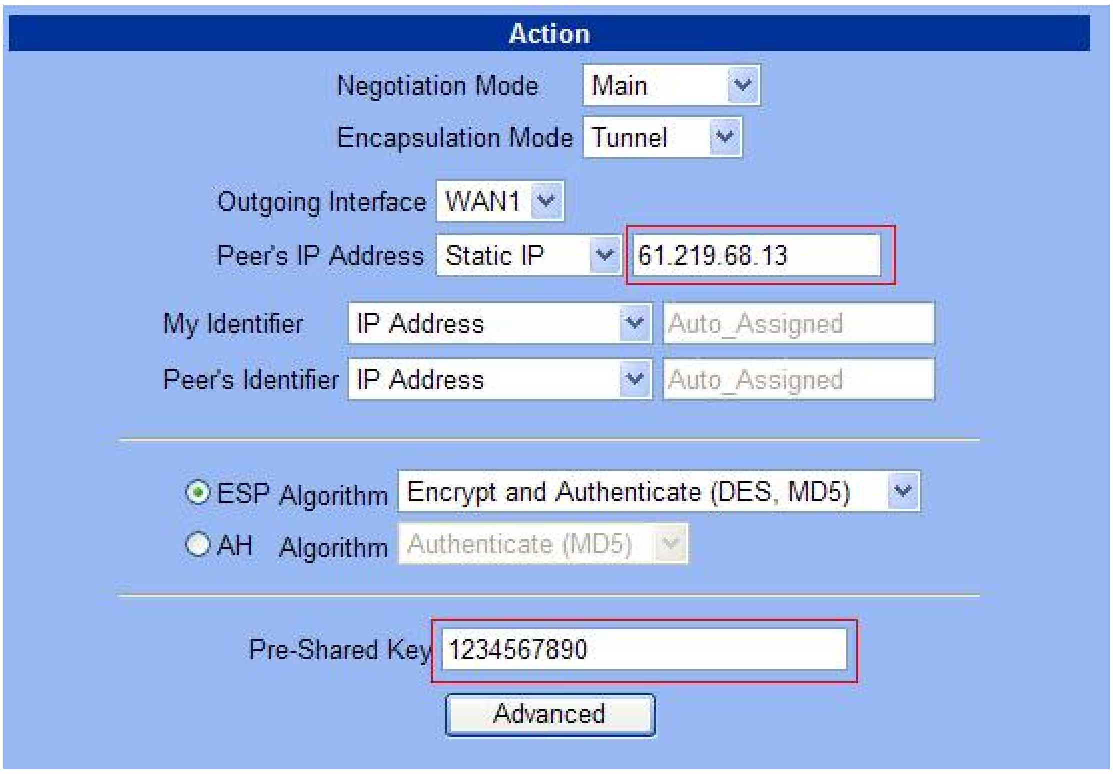
IP Address: 192.168.1.0

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

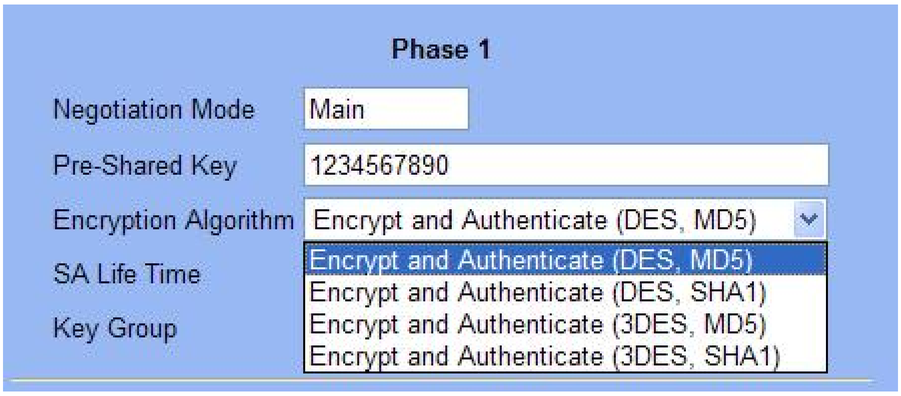
My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890



Phase 1

Negotiation Mode: Main

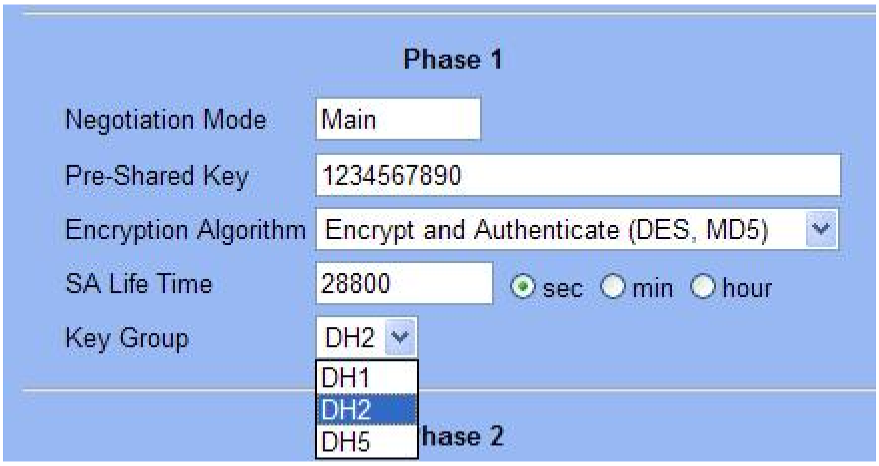
Pre-Shared Key: 1234567890

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

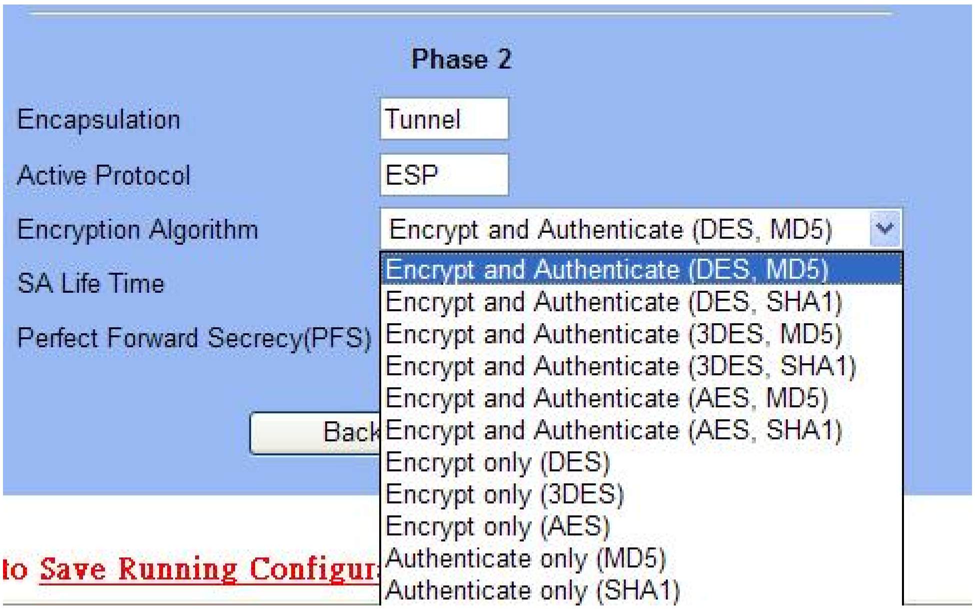
Negotiation Mode: Main

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Key Group: DH2



Phase 2

Encapsulation: Tunnel

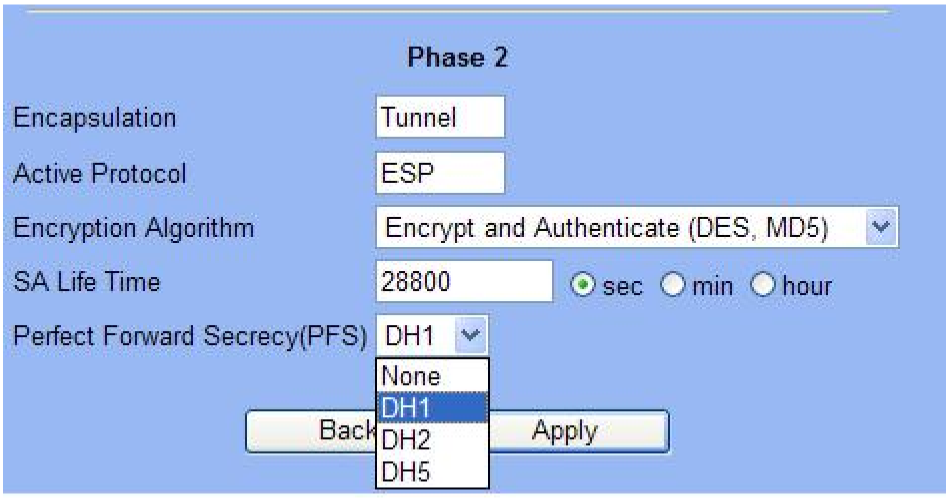
Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time

Perfect Forward Secrecy(PFS)

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)
Back
to Save Running Configur



Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

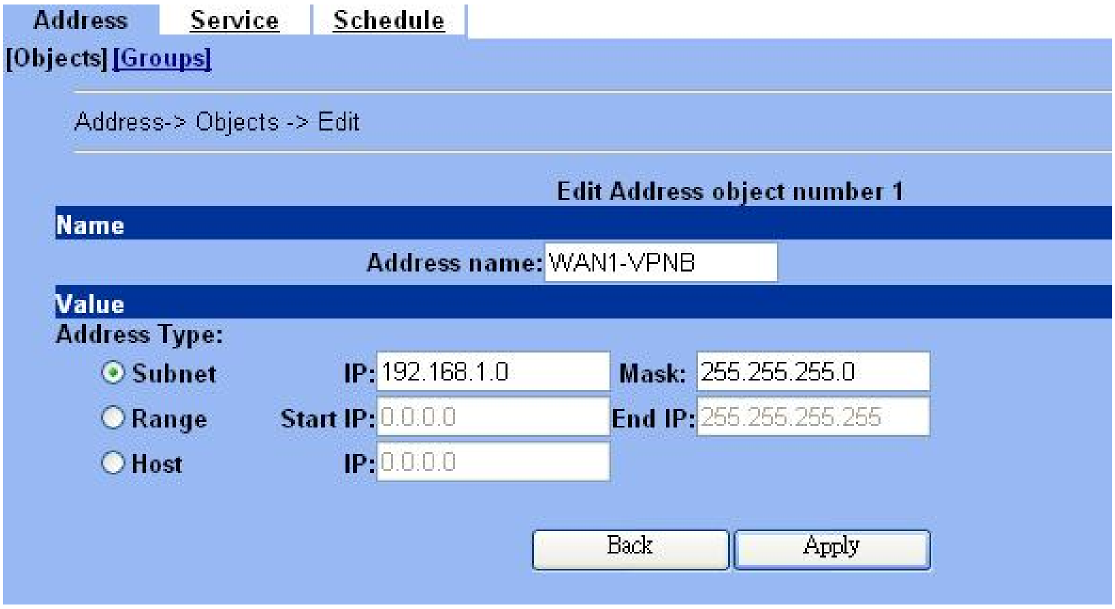
Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Perfect Forward Secrecy(PFS): DH1

Local_Firewall:

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



Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: WAN1-VPNB

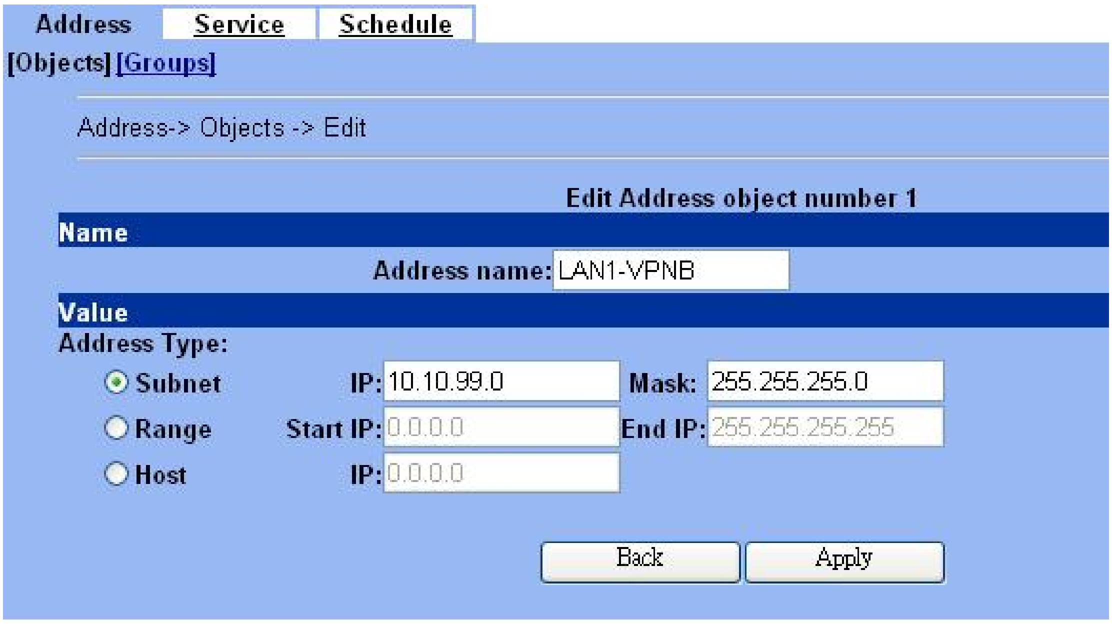
Value

Address Type:

● Subnet IP: 192.168.1.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0



Address-> Objects -> Edit

Edit Address object number 1

Name

Address name: LAN1-VPNB

Value

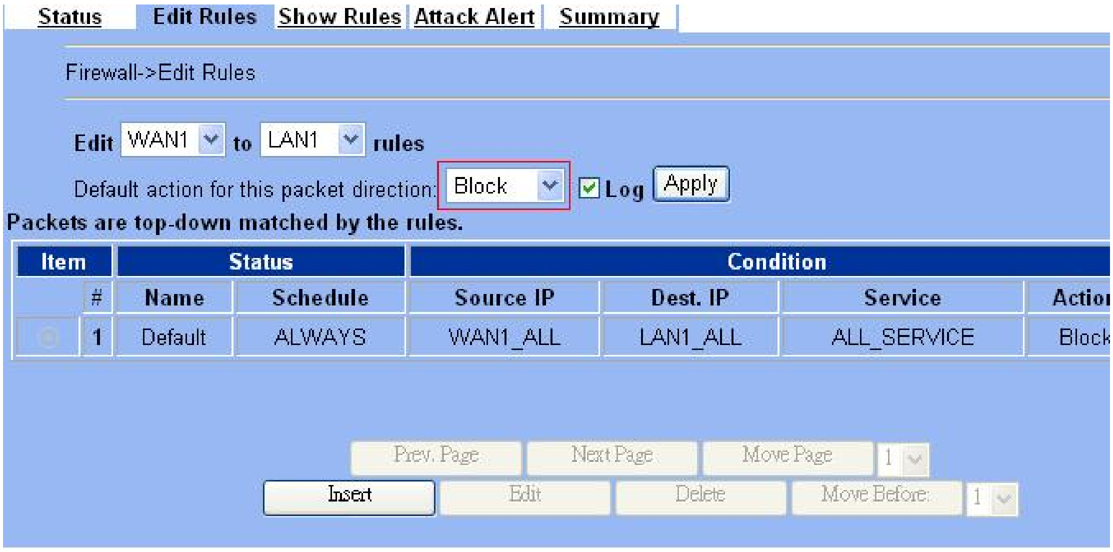
Address Type:

● Subnet IP: 10.10.99.0 Mask: 255.255.255.0

○ Range Start IP: 0.0.0.0 End IP: 255.255.255.255

○ Host IP: 0.0.0.0

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



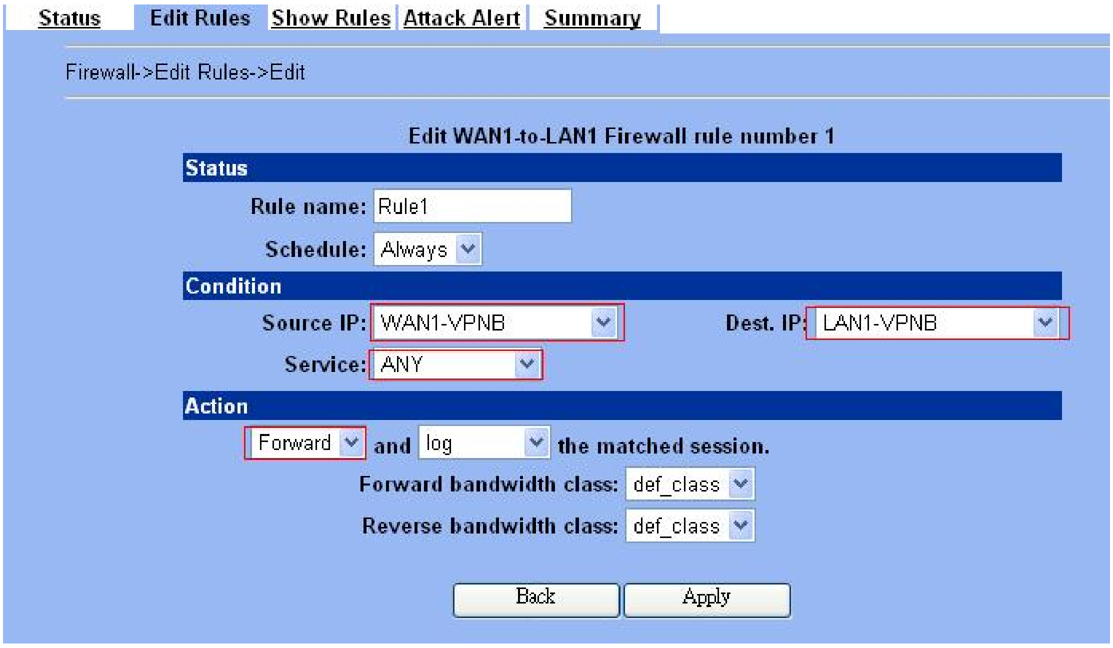
Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item	Status			Condition			
	#	Name	Schedule	Source IP	Dest. IP	Service	Actio
○	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block



Firewall->Edit Rules->Edit

Edit WAN1-to-LAN1 Firewall rule number 1

Status

Rule name: Rule1

Schedule: Always

Condition

Source IP: WAN1-VPNB Dest. IP: LAN1-VPNB

Service: ANY

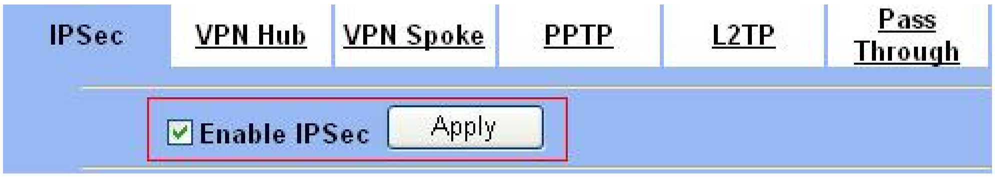
Action

Forward and log the matched session.

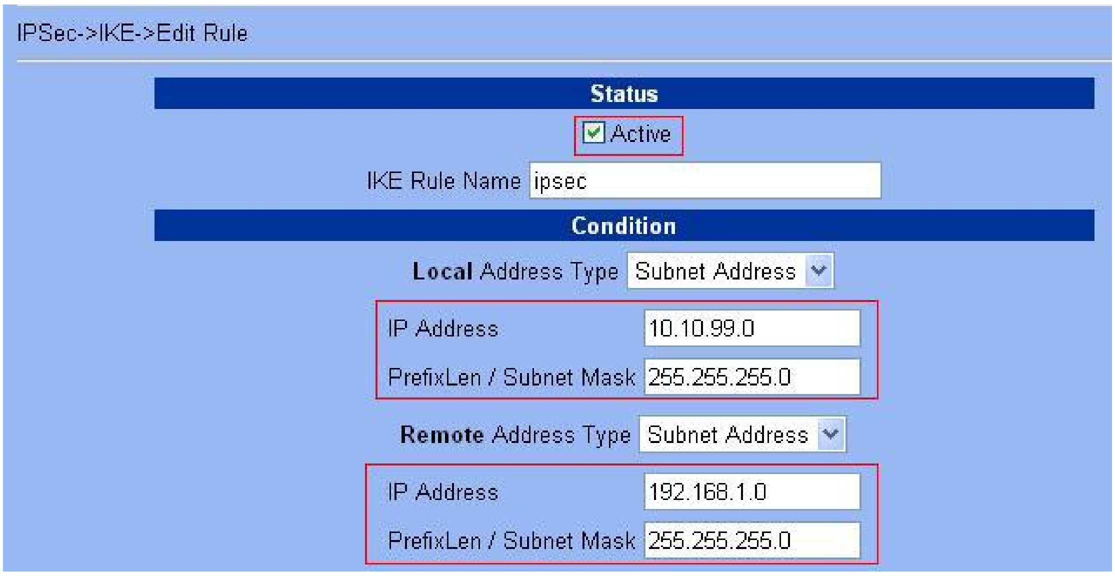
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

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



☑ Enable IPSec



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: ipsec

Condition

Local Address Type: Subnet Address

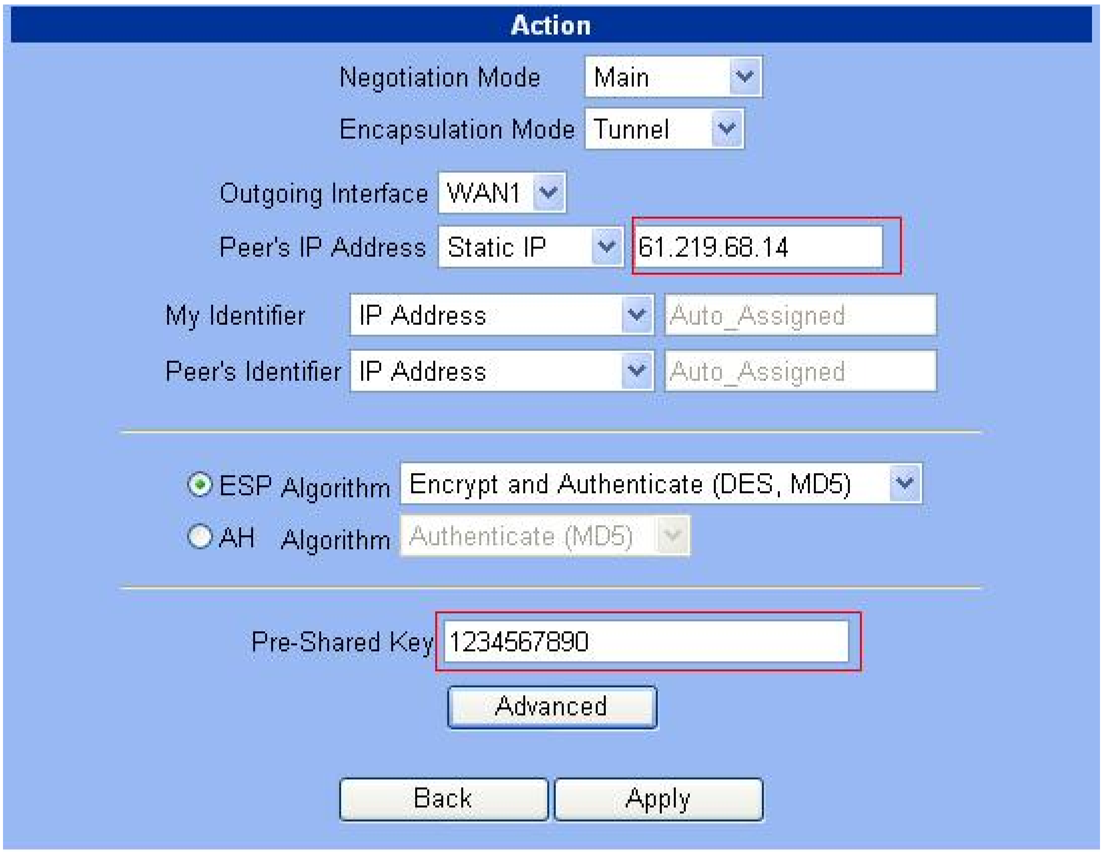
IP Address: 10.10.99.0

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

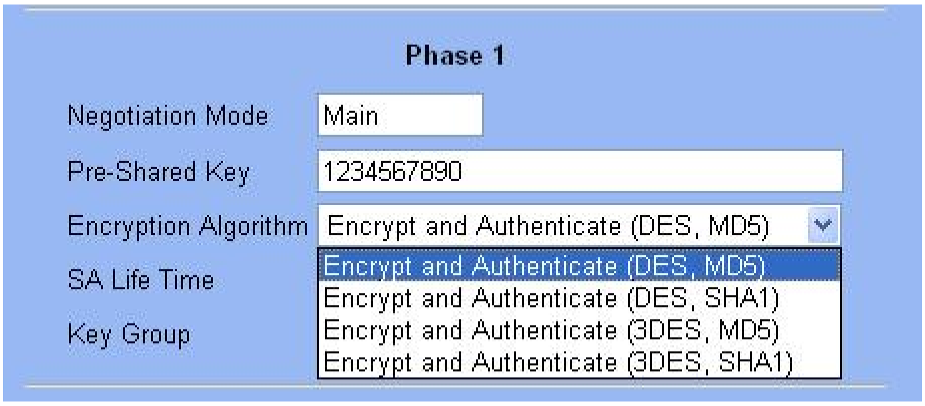
My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890



Phase 1

Negotiation Mode: Main

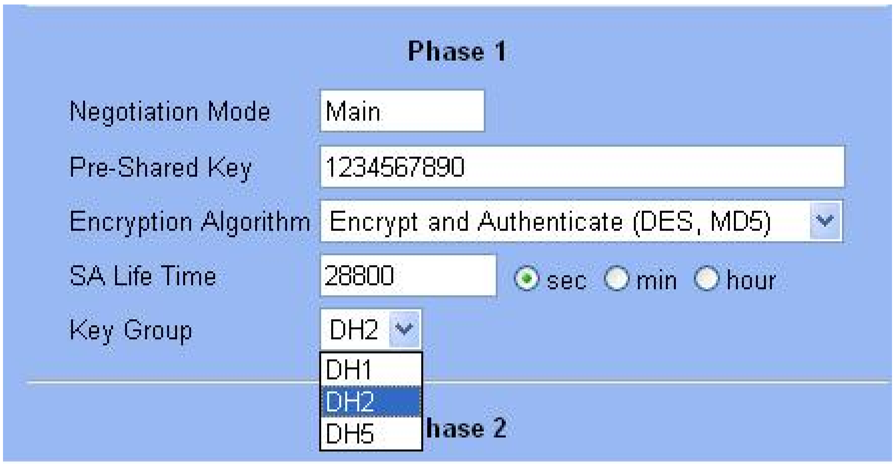
Pre-Shared Key: 1234567890

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

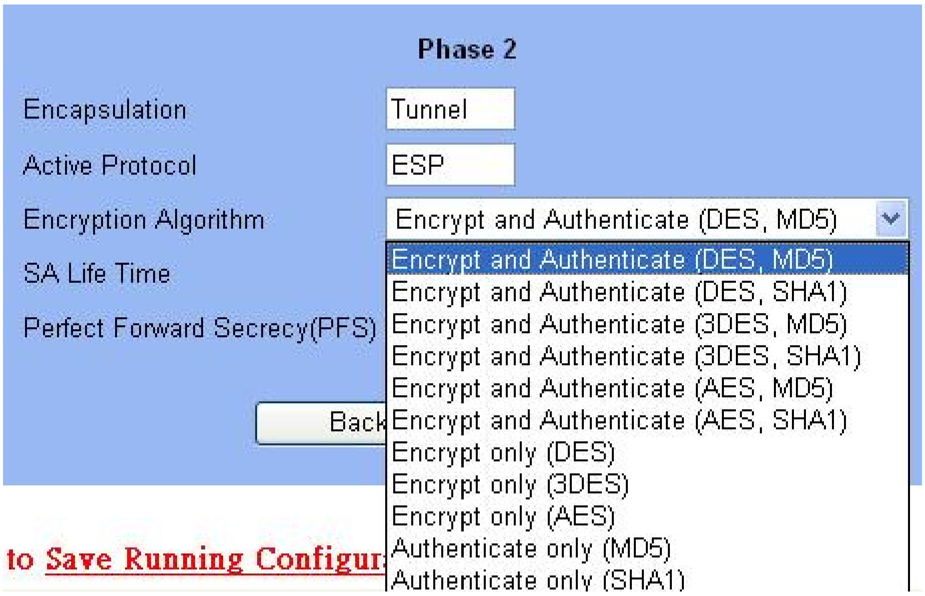
Negotiation Mode: Main

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Key Group: DH2



Phase 2

Encapsulation: Tunnel

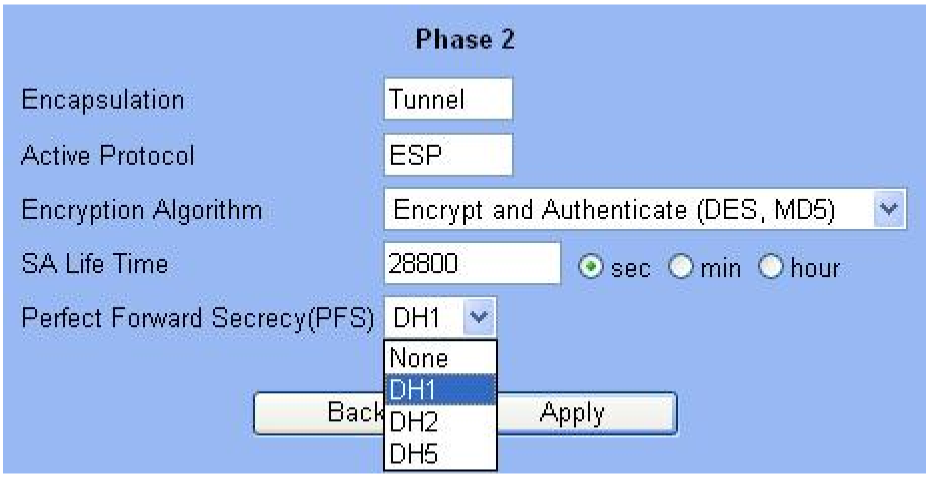
Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time

Perfect Forward Secrecy(PFS)

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)
Back
to Save Running Configur



Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

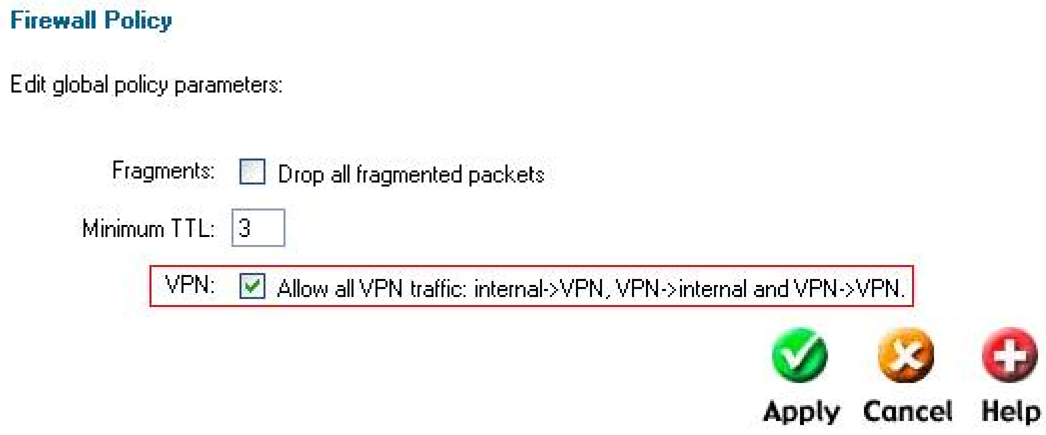
SA Life Time: 28800 ● sec ○ min ○ hour

Perfect Forward Secrecy(PFS): DH1

DFL-1100/700/200

Remote_Firewall:

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



Firewall Policy

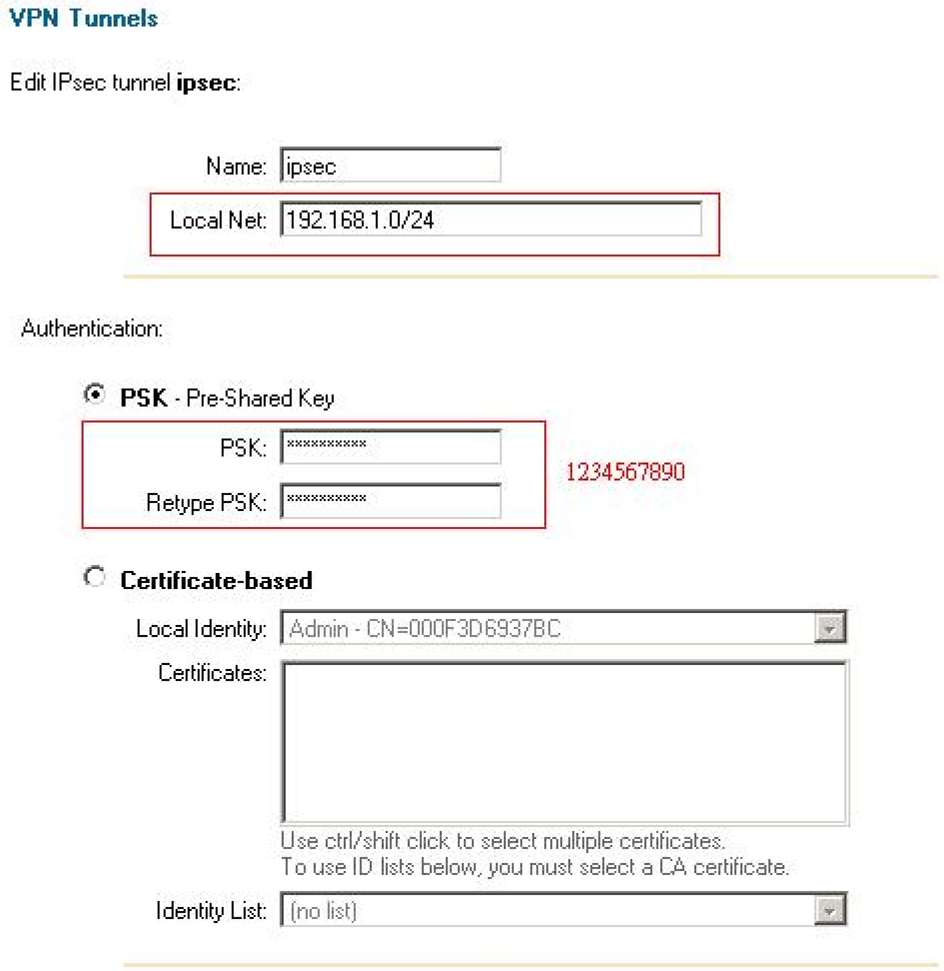
Edit global policy parameters:

Fragments: □ Drop all fragmented packets

Minimum TTL: 3

VPN: ☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

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



VPN Tunnels

Edit IPsec tunnel **ipsec**:

Name: ipsec

Local Net: 192.168.1.0/24

Authentication:

● **PSK** - Pre-Shared Key

PSK: **********

Retype PSK: **********

1234567890

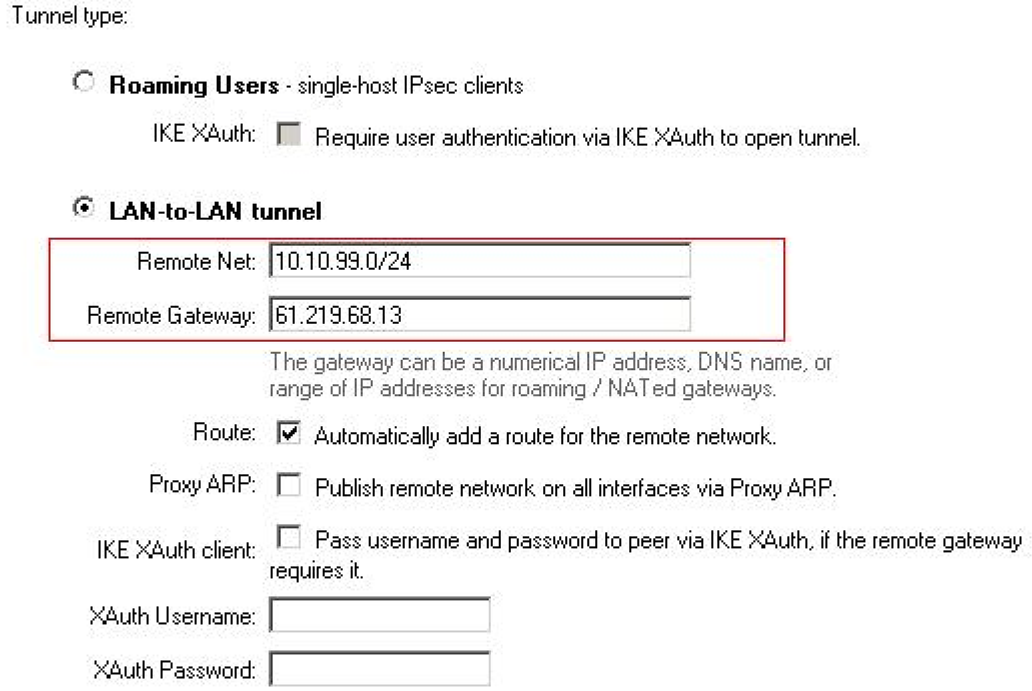
○ **Certificate-based**

Local Identity: Admin - CN=000F3D6937BC

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)



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.

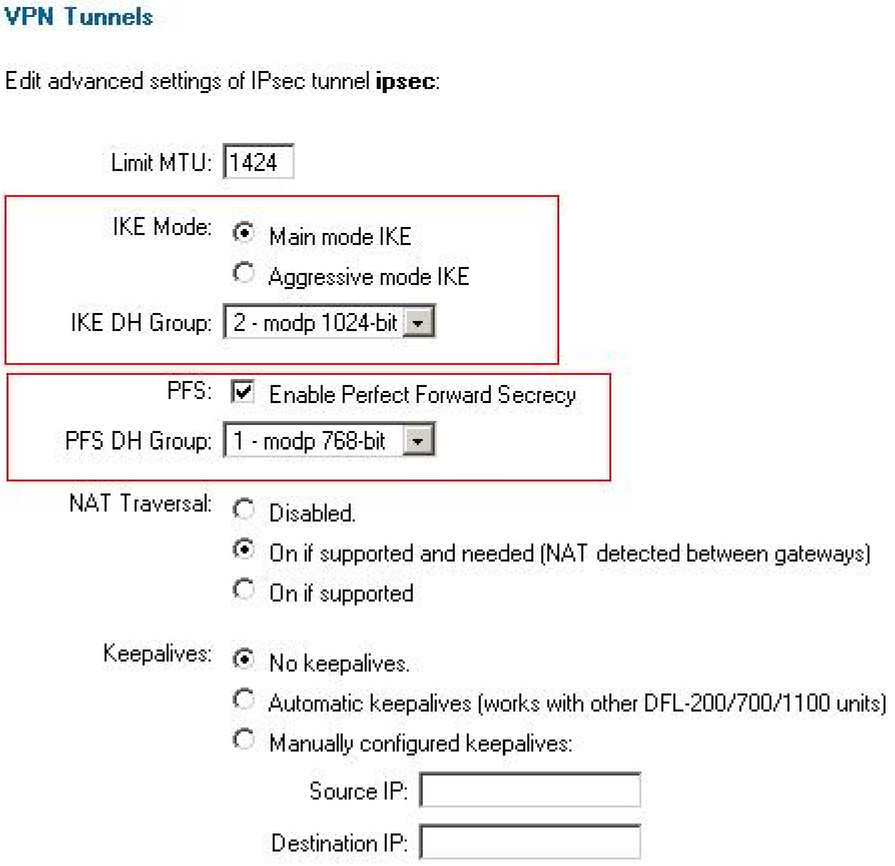
Route: ☑ Automatically add a route for the remote network.

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

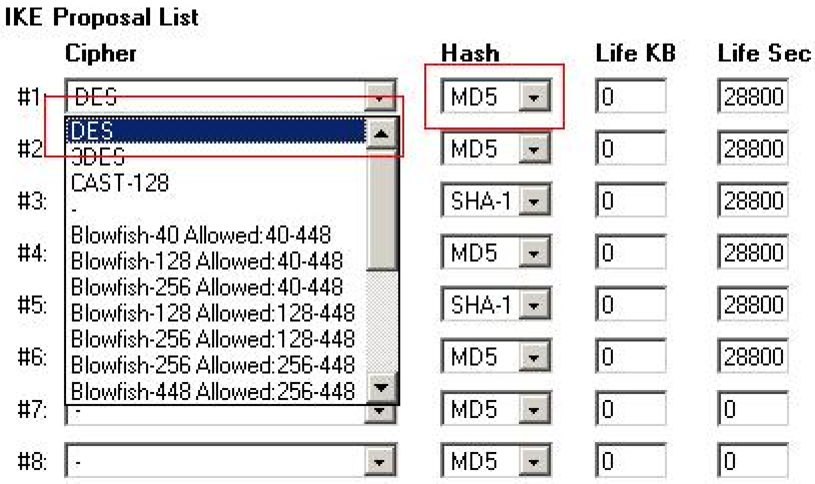
PFS DH Group: 1 - modp 768-bit

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:

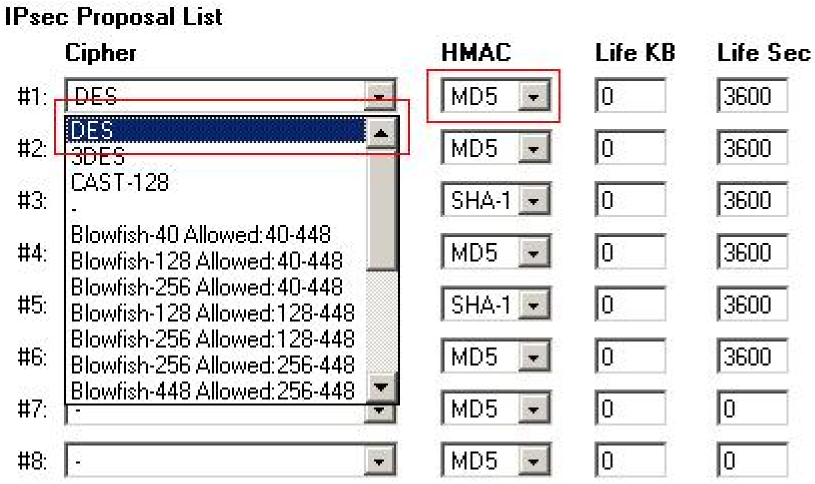
Destination IP:



IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1	DES	MD5	0	28800
#2		MD5	0	28800
#3:		SHA-1	0	28800
#4:		MD5	0	28800
#5:		SHA-1	0	28800
#6:		MD5	0	28800
#7:	-	MD5	0	0
#8:	-	MD5	0	0

DES
3DES
CAST-128
-
Blowfish-40 Allowed:40-448
Blowfish-128 Allowed:40-448
Blowfish-256 Allowed:40-448
Blowfish-128 Allowed:128-448
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448



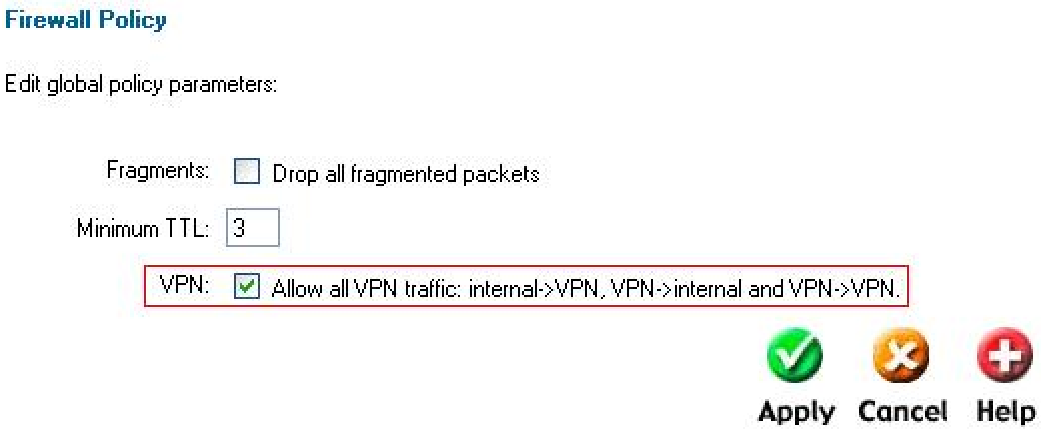
IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:		MD5	0	3600
#3:		SHA-1	0	3600
#4:		MD5	0	3600
#5:		SHA-1	0	3600
#6:		MD5	0	3600
#7:	-	MD5	0	0
#8:	-	MD5	0	0

DES
3DES
CAST-128
-
Blowfish-40 Allowed:40-448
Blowfish-128 Allowed:40-448
Blowfish-256 Allowed:40-448
Blowfish-128 Allowed:128-448
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

Local_Firewall:

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



Firewall Policy

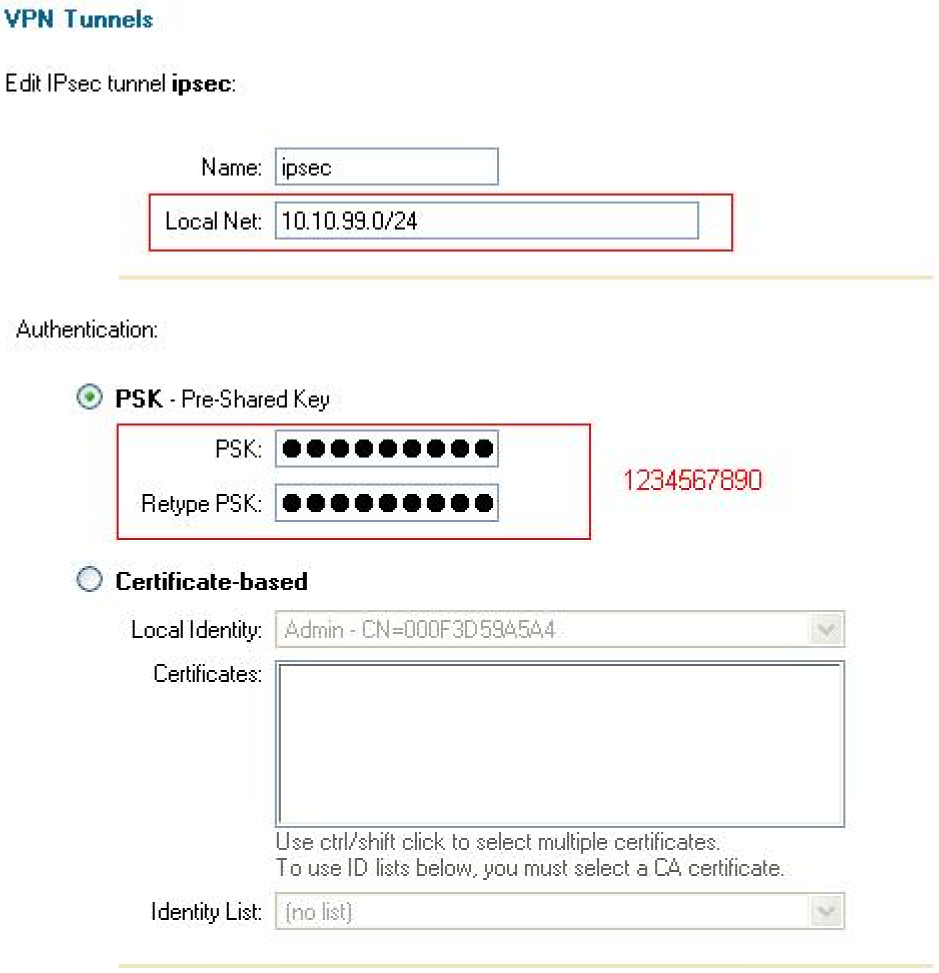
Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL: 3

VPN: ☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

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



VPN Tunnels

Edit IPsec tunnel **ipsec**:

Name: ipsec

Local Net: 10.10.99.0/24

Authentication:

● **PSK** - Pre-Shared Key

PSK: ●●●●●●●●●●

Retype PSK: ●●●●●●●●●●

1234567890

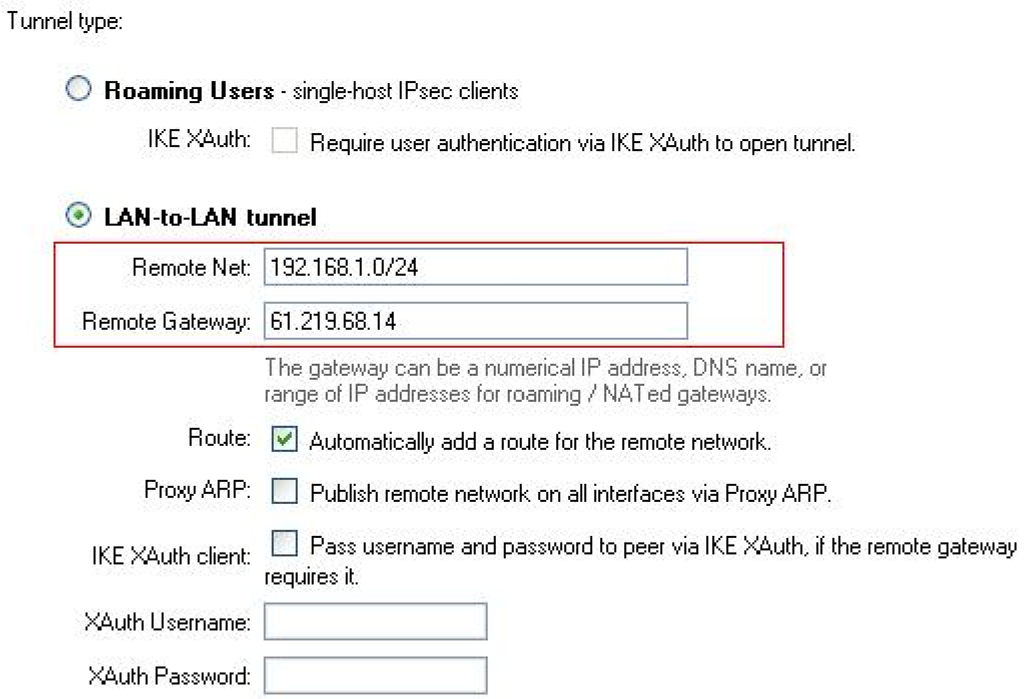
○ **Certificate-based**

Local Identity: Admin - CN=000F3D59A5A4

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)



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.

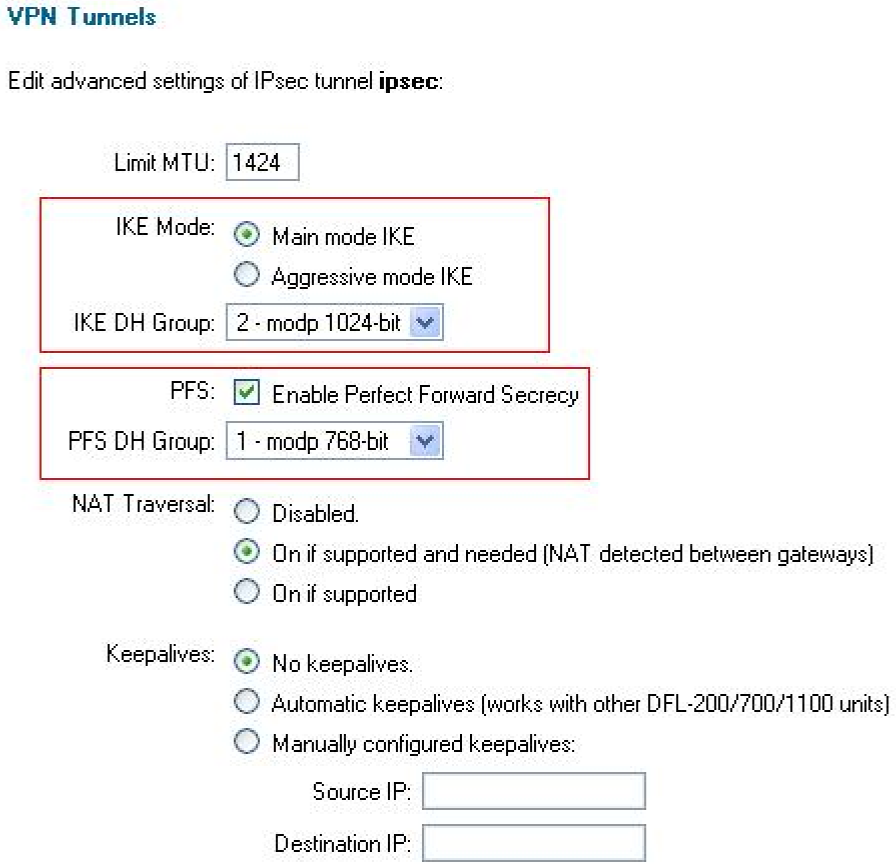
Route: ☑ Automatically add a route for the remote network.

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

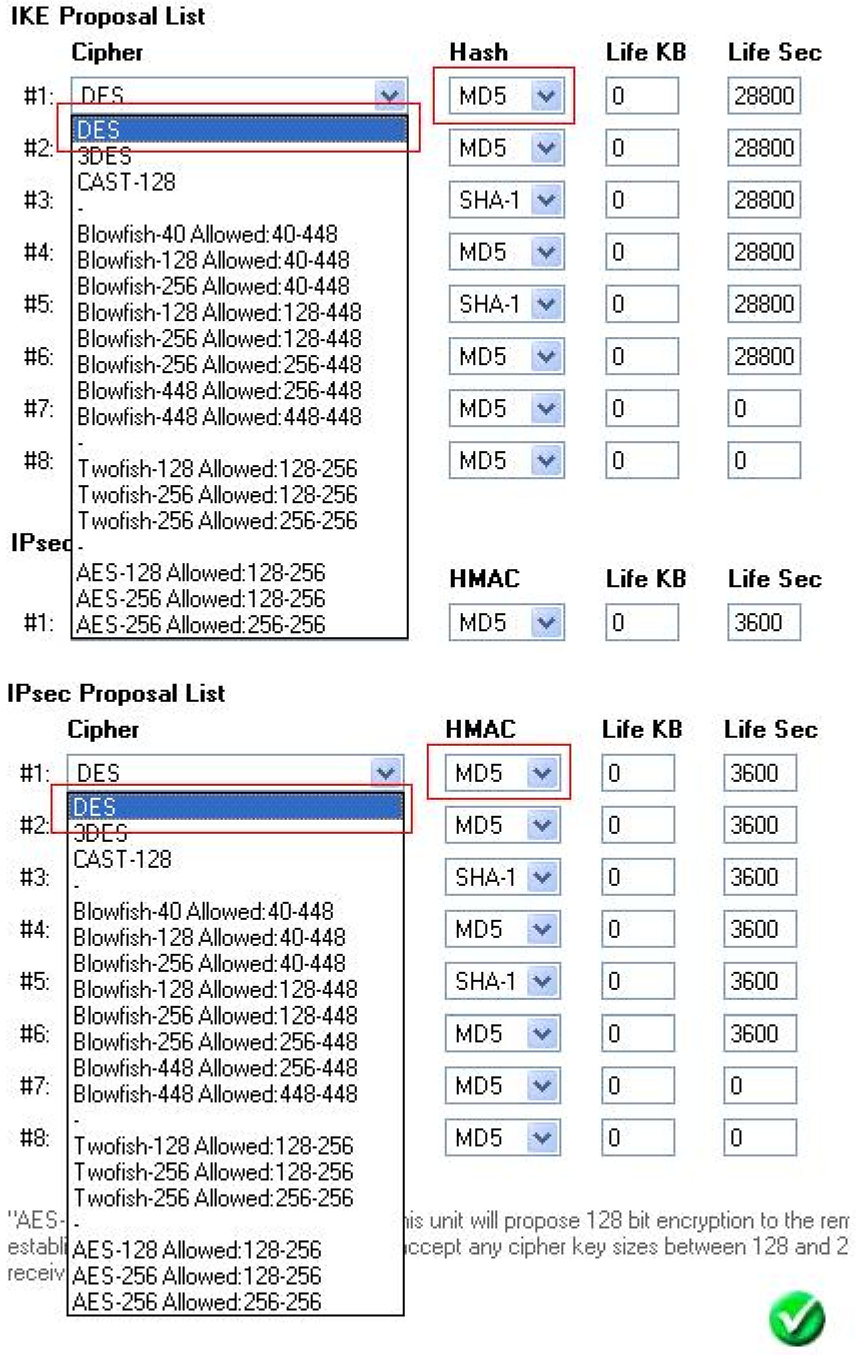
PFS DH Group: 1 - modp 768-bit

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:



IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	DES	MD5	0	28800
#2:		MD5	0	28800
#3:		SHA-1	0	28800
#4:		MD5	0	28800
#5:		SHA-1	0	28800
#6:		MD5	0	28800
#7:		MD5	0	0
#8:		MD5	0	0

IPsec

	HMAC	Life KB	Life Sec
#1:	MD5	0	3600

IPsec Proposal List

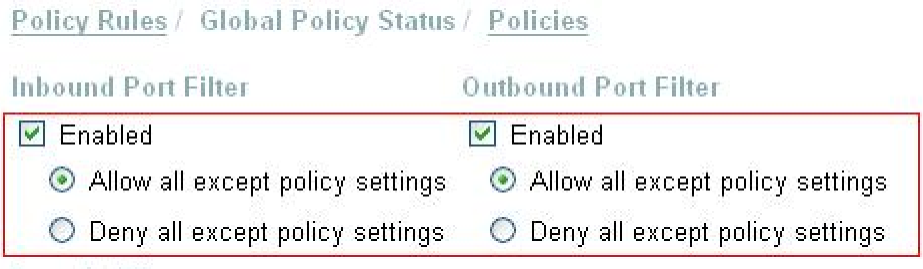
	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:		MD5	0	3600
#3:		SHA-1	0	3600
#4:		MD5	0	3600
#5:		SHA-1	0	3600
#6:		MD5	0	3600
#7:		MD5	0	0
#8:		MD5	0	0

DES
3DES
CAST-128
-
Blowfish-40 Allowed:40-448
Blowfish-128 Allowed:40-448
Blowfish-256 Allowed:40-448
Blowfish-128 Allowed:128-448
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448
Blowfish-448 Allowed:448-448
-
Twofish-128 Allowed:128-256
Twofish-256 Allowed:128-256
Twofish-256 Allowed:256-256
-
AES-128 Allowed:128-256
AES-256 Allowed:128-256
AES-256 Allowed:256-256
"AES-
establi
receiv
his unit will propose 128 bit encryption to the rem
ccept any cipher key sizes between 128 and 2

DFL-600

Remote_Firewall:

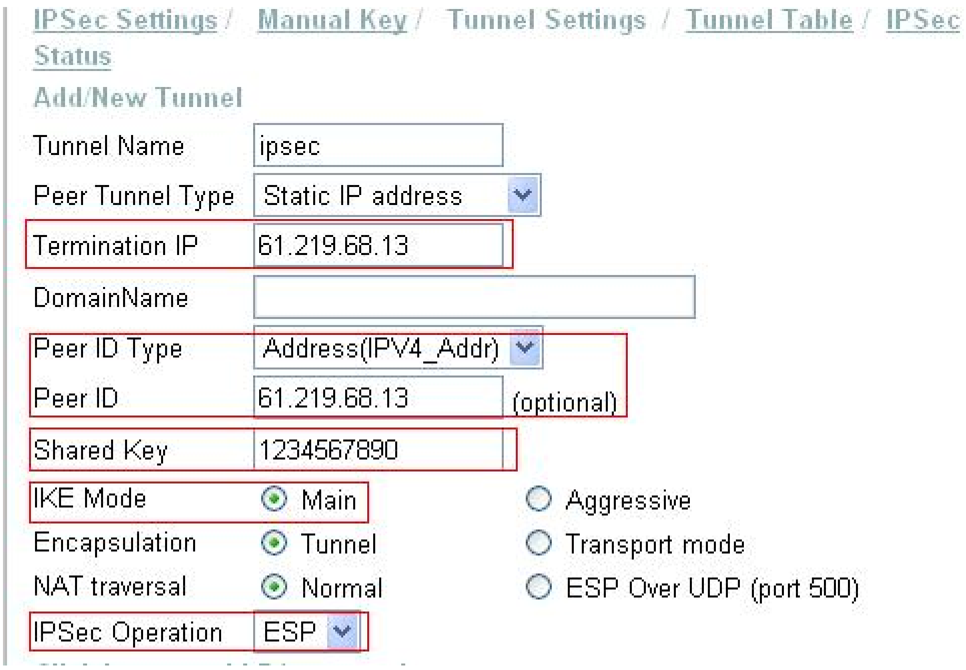
01- Enable allow all VPN traffic (**Advanced -> Policy -> Global Policy Status)**



Policy Rules / Global Policy Status / Policies

Inbound Port Filter	Outbound Port Filter
☑ Enabled	☑ Enabled
● Allow all except policy settings	● Allow all except policy settings
○ Deny all except policy settings	○ Deny all except policy settings

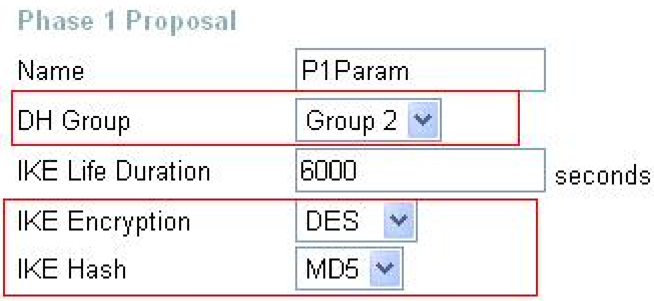
02- Enable IPSec and edit IPSec rule (**Advanced -> VPN-IPSec -> Tunnel Settings**)



IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status

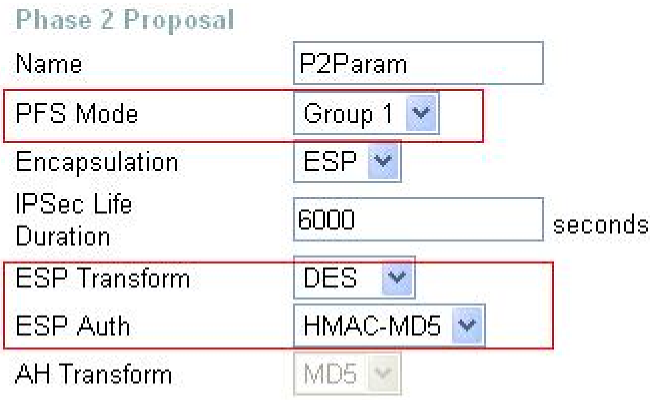
Add/New Tunnel

Tunnel Name	ipsec	
Peer Tunnel Type	Static IP address	
Termination IP	61.219.68.13	
DomainName		
Peer ID Type	Address(IPV4_Addr)	
Peer ID	61.219.68.13	(optional)
Shared Key	1234567890	
IKE Mode	● Main	○ Aggressive
Encapsulation	● Tunnel	○ Transport mode
NAT traversal	● Normal	○ ESP Over UDP (port 500)
IPSec Operation	ESP	



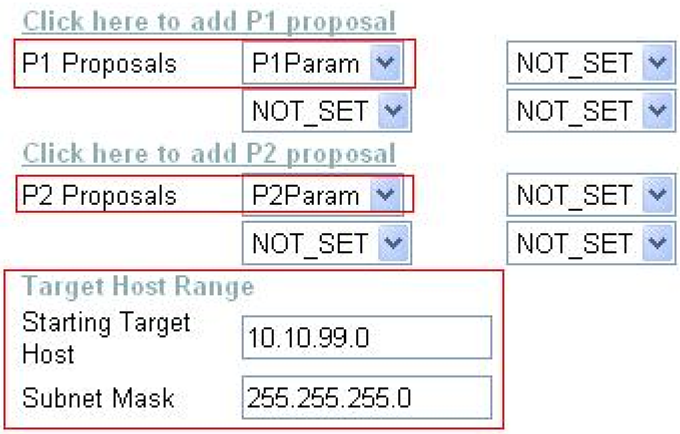
Phase 1 Proposal

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

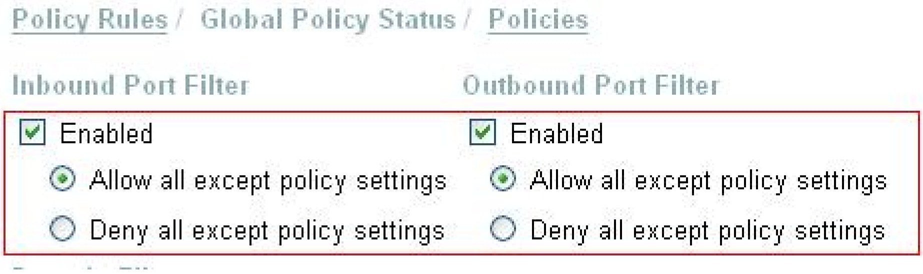
P2 Proposals	P2Param	NOT_SET
	NOT_SET	NOT_SET

Target Host Range

Starting Target Host	10.10.99.0
Subnet Mask	255.255.255.0

Local_Firewall:

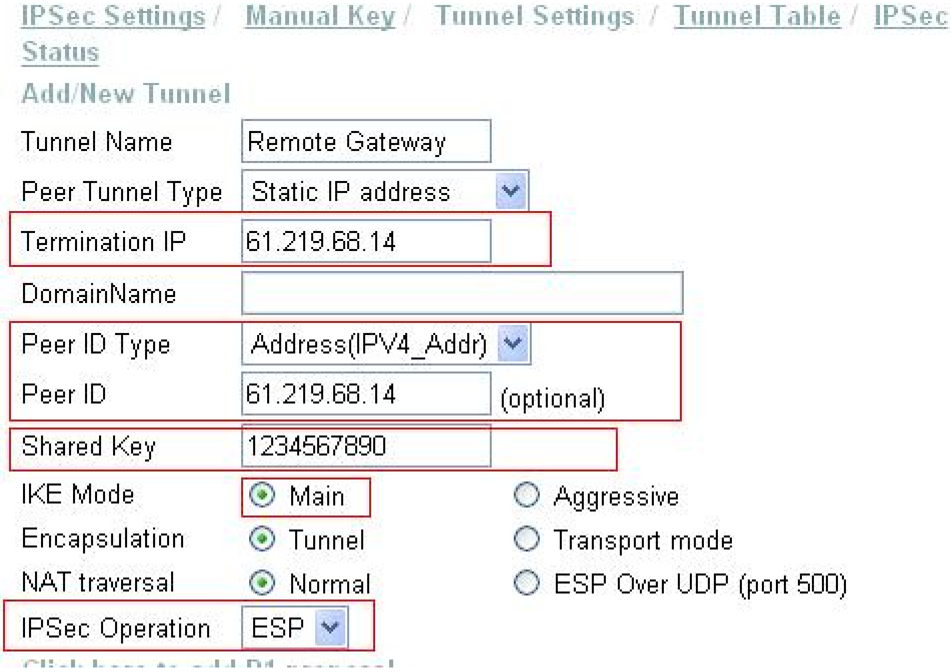
01- Enable allow all VPN traffic (**Advanced -> Policy -> Global Policy Status)**



Policy Rules / Global Policy Status / Policies

Inbound Port Filter	Outbound Port Filter
☑ Enabled	☑ Enabled
● Allow all except policy settings	● Allow all except policy settings
○ Deny all except policy settings	○ Deny all except policy settings

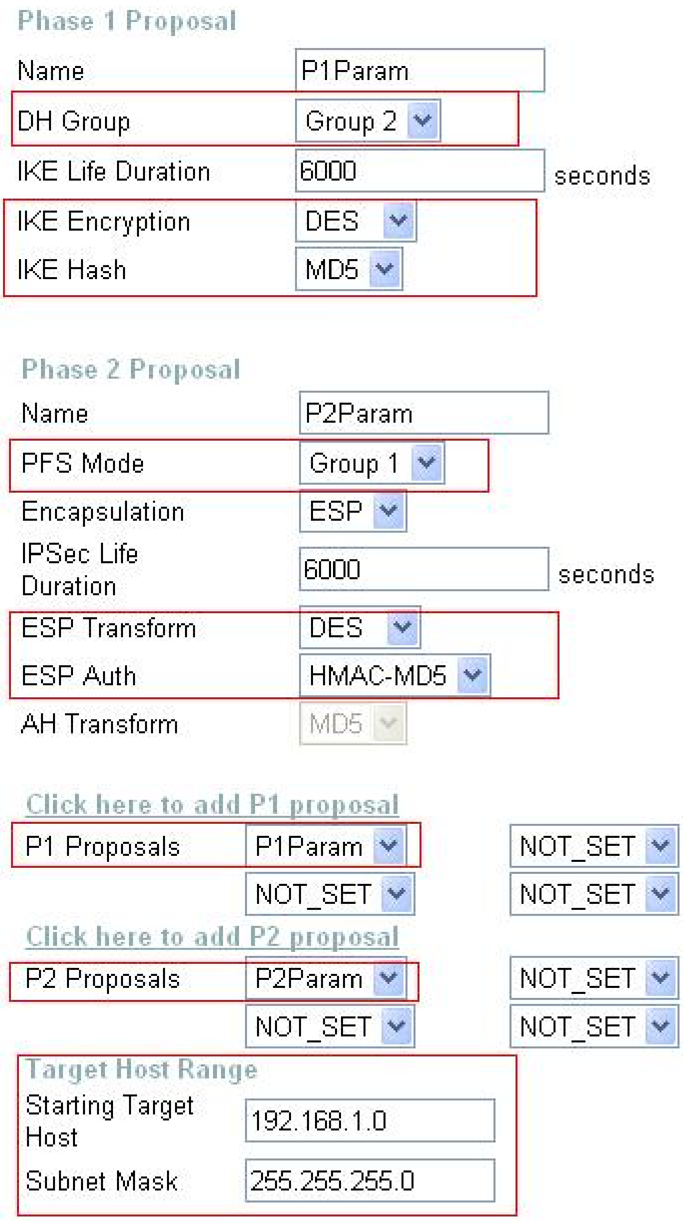
02- Enable IPSec and edit IPSec rule (**Advanced -> VPN-IPSec -> Tunnel Settings**)



IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status

Add/New Tunnel

Tunnel Name	Remote Gateway	
Peer Tunnel Type	Static IP address	
Termination IP	61.219.68.14	
DomainName		
Peer ID Type	Address(IPV4_Addr)	
Peer ID	61.219.68.14	(optional)
Shared Key	1234567890	
IKE Mode	● Main	○ Aggressive
Encapsulation	● Tunnel	○ Transport mode
NAT traversal	● Normal	○ ESP Over UDP (port 500)
IPSec Operation	ESP	



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