

**D-Link VPN Application
Quick Installation Guide**

Contents

1. Remote Access	3
1-1 Objective:	3
1-2 Environment:	3
1-3 Setup	3
1-3-1 PPTP Server	3
DFL-1500	4
DFL-1100/700/200	4
DFL-600	5
Configuring PPTP Client (Microsoft XP PRO's VPN adapter)	6
1-3-2 L2TP without IPSec	10
1-3-3 IPSec	10
DFL-1500/900	11
DFL-1100/700/200	15
DFL-600	18
Configuring IPSec connection (D-Link DS-601)	20
2. LAN to LAN	27
2-1 Objective:	27
2-2 Environment:	27
2-3 Setups:	27
2-3-1 PPTP Server & PPTP Client	27
DFL-1500	28
DFL-1100/700/200	29
2-3-2 L2TP Server & L2TP Client	30
2-3-3 IPSec	30
DFL-1500	31
DFL-1100/700/200	38
DFL-600	44

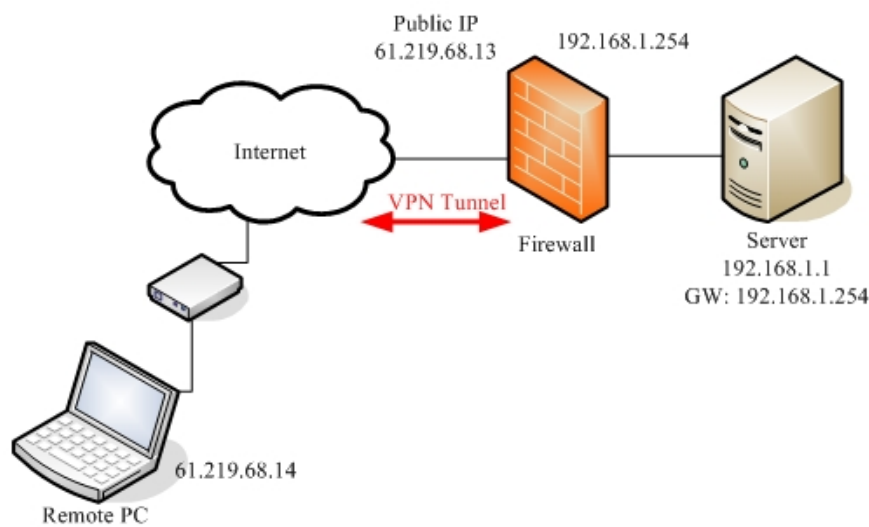
1. Remote Access

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

D-Link corporation

Device setting page

DFL-1500

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

<u>IPSec</u>	<u>VPN Hub</u>	<u>VPN Spoke</u>	PPTP	<u>L2TP</u>	<u>Pass Through</u>
--------------	----------------	------------------	-------------	-------------	---------------------

☒ Enable PPTP Server

[Server] [Client]

Local IP: 192.168.1.254

Assigned IP Range

Start: 192.168.1.100 End: 192.168.1.105

Username: firewall Password: *****

Apply

DFL-1100/700/200

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

User Management

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:

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:

☒ Proxy ARP dynamically added routes

Primary DNS: (Optional)

Secondary DNS: (Optional)

☒ Use unit's own DNS relay 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:

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:

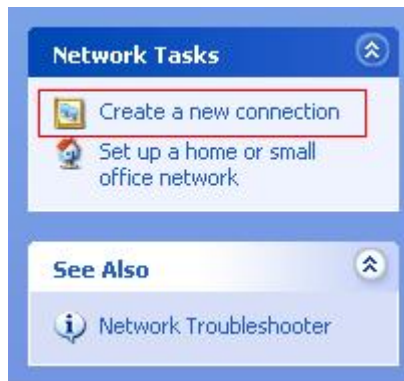
Ending IP address:

D-Link corporation

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

Setup1

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



Setup2

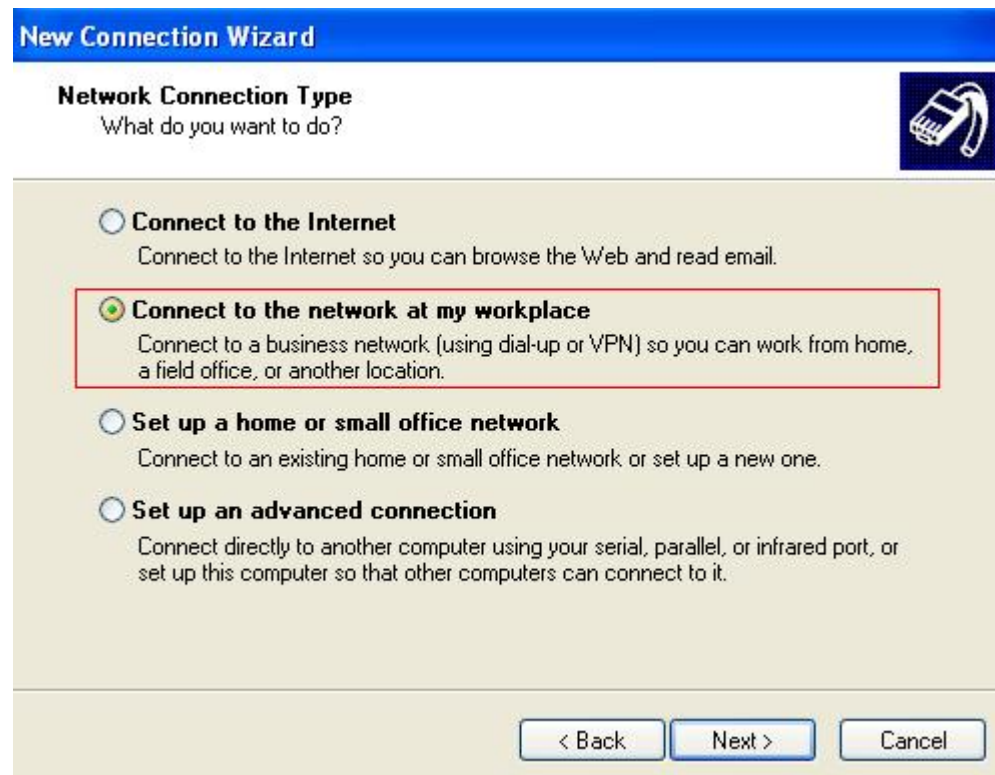
Click **Next** to the next step.



D-Link corporation

Setup3

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



The image shows a Windows XP-style dialog box titled "New Connection Wizard". The title bar is blue with white text. Below the title bar, the text "Network Connection Type" is followed by the question "What do you want to do?". To the right of this text is a small icon of a computer with a network cable. The main area of the dialog box is light beige and contains four radio button options. The second option, "Connect to the network at my workplace", is selected and highlighted with a red rectangular border. Below the options are three buttons: "< Back", "Next >", and "Cancel".

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.

< Back Next > Cancel

Steup4

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



The image shows a second Windows XP-style dialog box titled "New Connection Wizard". The title bar is blue with white text. Below the title bar, the text "Network Connection" is followed by the question "How do you want to connect to the network at your workplace?". To the right of this text is a small icon of a computer with a network cable. The main area of the dialog box is light beige and contains two radio button options. The second option, "Virtual Private Network connection", is selected and highlighted with a red rectangular border. Below the options are three buttons: "< Back", "Next >", and "Cancel".

New Connection Wizard

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

Create the following connection:

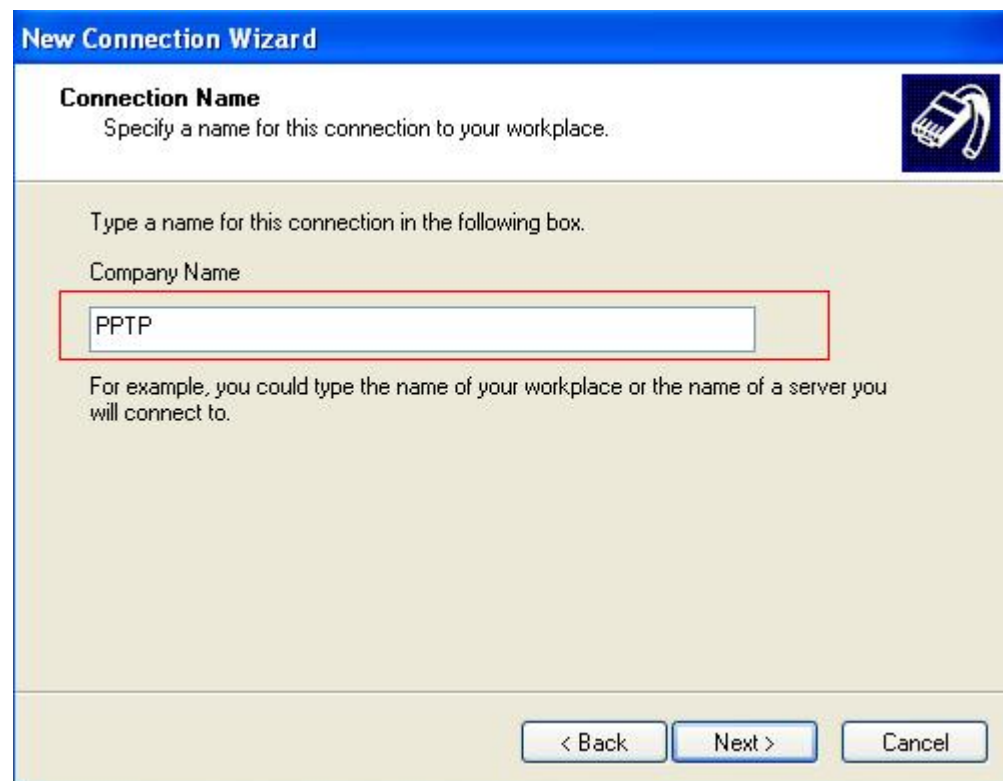
- ☐ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
- ☒ **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

< Back Next > Cancel

D-Link corporation

Step5

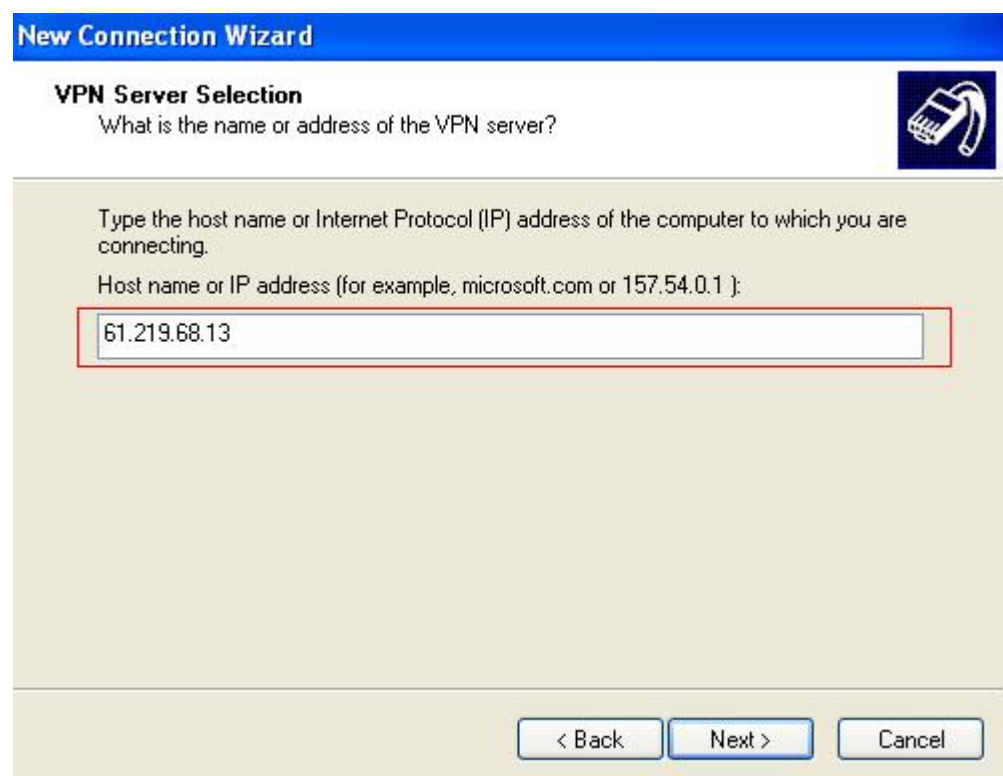
Give a name to the PPTP connection. Click **Next** to the next step.



The screenshot shows the 'New Connection Wizard' window with the 'Connection Name' step. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section is titled 'Connection Name' with a subtitle 'Specify a name for this connection to your workplace.' and a small icon of a network card. The main area is light beige and contains the instruction 'Type a name for this connection in the following box.' followed by 'Company Name'. A text input field contains the text 'PPTP' and is highlighted with a red rectangular border. Below the input field, there is a note: 'For example, you could type the name of your workplace or the name of a server you will connect to.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Step6

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



The screenshot shows the 'New Connection Wizard' window with the 'VPN Server Selection' step. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section is titled 'VPN Server Selection' with a subtitle 'What is the name or address of the VPN server?' and a small icon of a network card. The main area is light beige and contains the instruction 'Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.' followed by 'Host name or IP address (for example, microsoft.com or 157.54.0.1)'. A text input field contains the text '61.219.68.13' and is highlighted with a red rectangular border. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

D-Link corporation

Step7

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



Step8

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



D-Link corporation

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

D-Link corporation

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

Back Apply

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

Back Apply

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

Status **Edit Rules** **Show Rules** **Attack Alert** **Summary**

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

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name:

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**

Back **Apply**

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

IPSec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

☒ **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 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

Pre-Shared Key

Encryption Algorithm

SA Life Time ☒ sec ☐ min ☐ hour

Key Group

Phase 2

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

SA Life Time

Perfect Forward Secrecy(PFS)

to Save Running Configuration

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)

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

SA Life Time ☒ sec ☐ min ☐ hour

Perfect Forward Secrecy(PFS)

D-Link corporation

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:

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



Apply



Cancel



Help

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

VPN Tunnels

Edit IPsec tunnel **ipsec**:

Name:

Local Net:

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:

Retype PSK:

1234567890

☐ **Certificate-based**

Local Identity:

Certificates:

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

Identity List:

D-Link corporation

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:

IKE Mode: ☒ Main mode IKE
☐ Aggressive mode IKE

IKE DH Group:

PFS: ☒ Enable Perfect Forward Secrecy

PFS DH Group:

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:	DES	MD5	0	28800
#3:	CAST-128	SHA-1	0	28800
#4:	Blowfish-40 Allowed: 40-448	MD5	0	28800
#5:	Blowfish-128 Allowed: 40-448	SHA-1	0	28800
#6:	Blowfish-256 Allowed: 128-448	MD5	0	28800
#7:	Blowfish-256 Allowed: 256-448	MD5	0	0
#8:	Blowfish-448 Allowed: 256-448	MD5	0	0

IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:	DES	MD5	0	3600
#3:	CAST-128	SHA-1	0	3600
#4:	Blowfish-40 Allowed: 40-448	MD5	0	3600
#5:	Blowfish-128 Allowed: 40-448	SHA-1	0	3600
#6:	Blowfish-256 Allowed: 128-448	MD5	0	3600
#7:	Blowfish-256 Allowed: 256-448	MD5	0	0
#8:	Blowfish-448 Allowed: 256-448	MD5	0	0

D-Link corporation

DFL-600

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

[Policy Rules](#) / [Global Policy Status](#) / [Policies](#)

Inbound Port Filter

☒ Enabled

☒ Allow all except policy settings

☐ Deny all except policy settings

Outbound Port Filter

☒ Enabled

☒ Allow 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	

D-Link corporation

[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

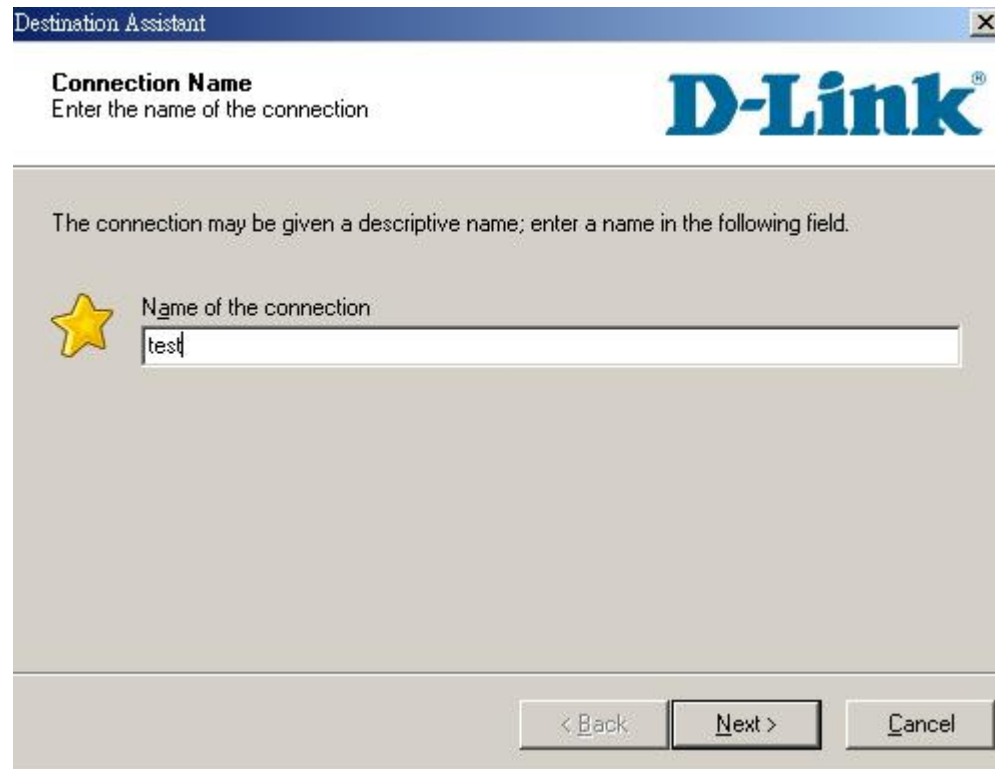
D-Link corporation

Configuring IPSec connection (D-Link DS-601)

Setup1

Configuration->Profile settings->New Entry

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



Destination Assistant

Connection Name
Enter the name of the connection

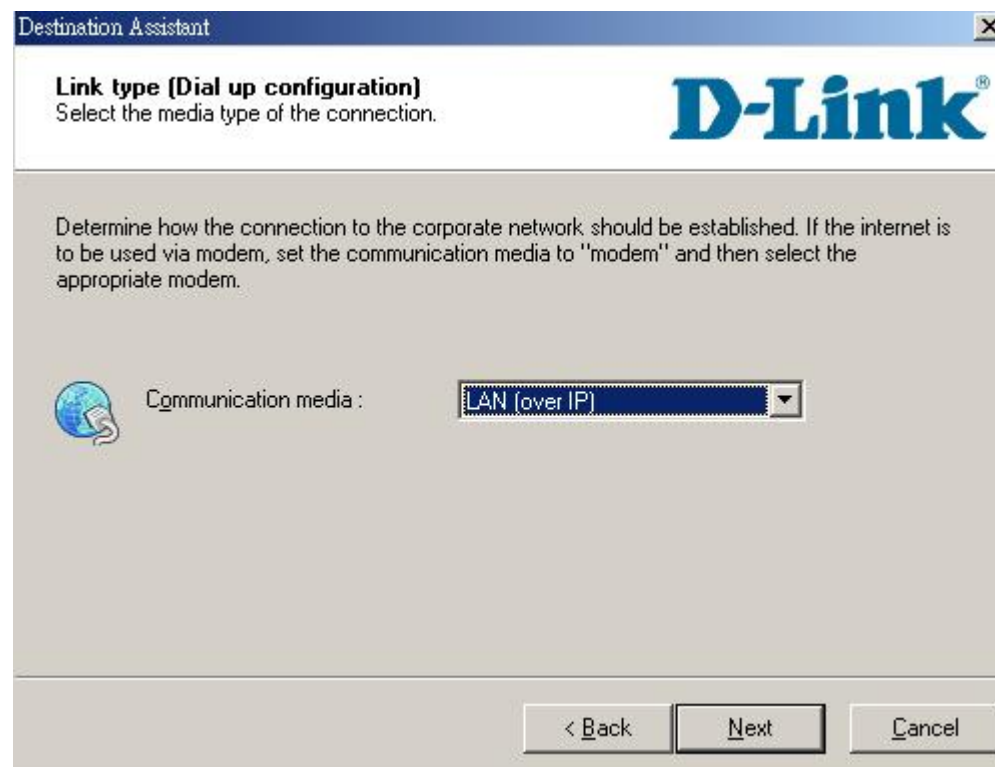
The connection may be given a descriptive name; enter a name in the following field.

 Name of the connection

< Back Next > Cancel

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.

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.

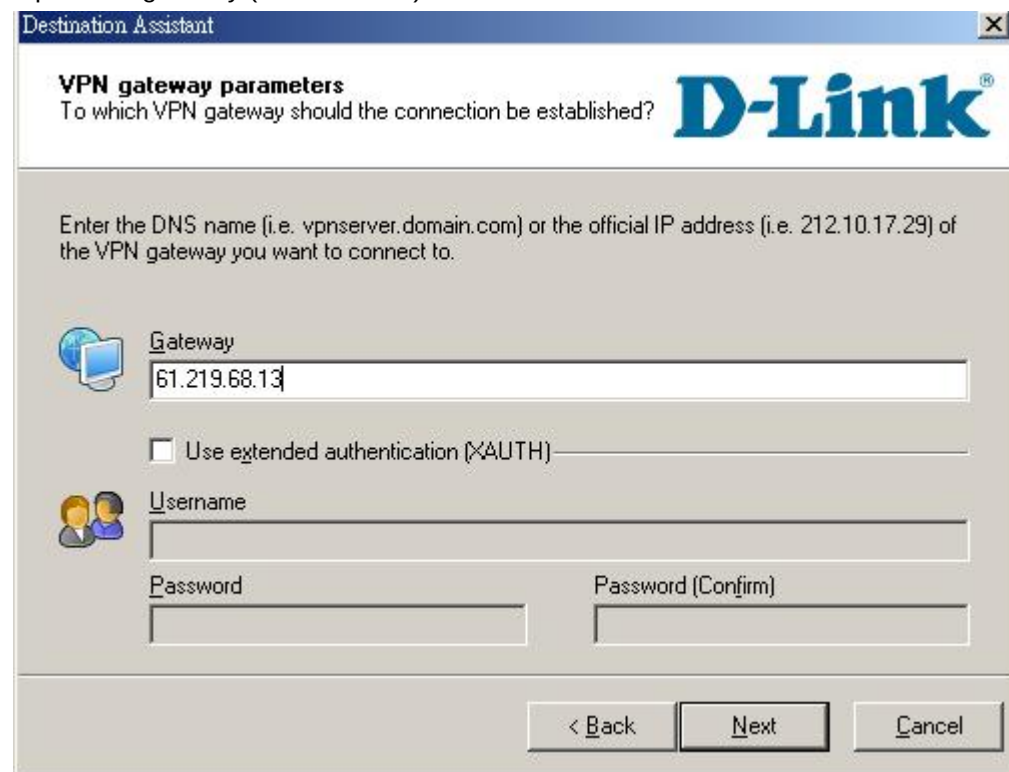
 Communication media :

< Back Next Cancel

D-Link corporation

Setup3

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



The screenshot shows the 'Destination Assistant' window with the title bar 'Destination Assistant' and a close button. The main heading is 'VPN gateway parameters' with the subtext 'To which VPN gateway should the connection be established?'. The D-Link logo is in the top right. Below the heading, it says '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.' There are three input fields: 'Gateway' with the value '61.219.68.13', 'Username' (empty), and 'Password' (empty). There is a checkbox for 'Use extended authentication (XAUTH)' which is unchecked. To the right of the 'Password' field is a 'Password (Confirm)' field, also empty. At the bottom are three buttons: '< Back', 'Next', and 'Cancel'.

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
[Empty field]

Password
[Empty field]

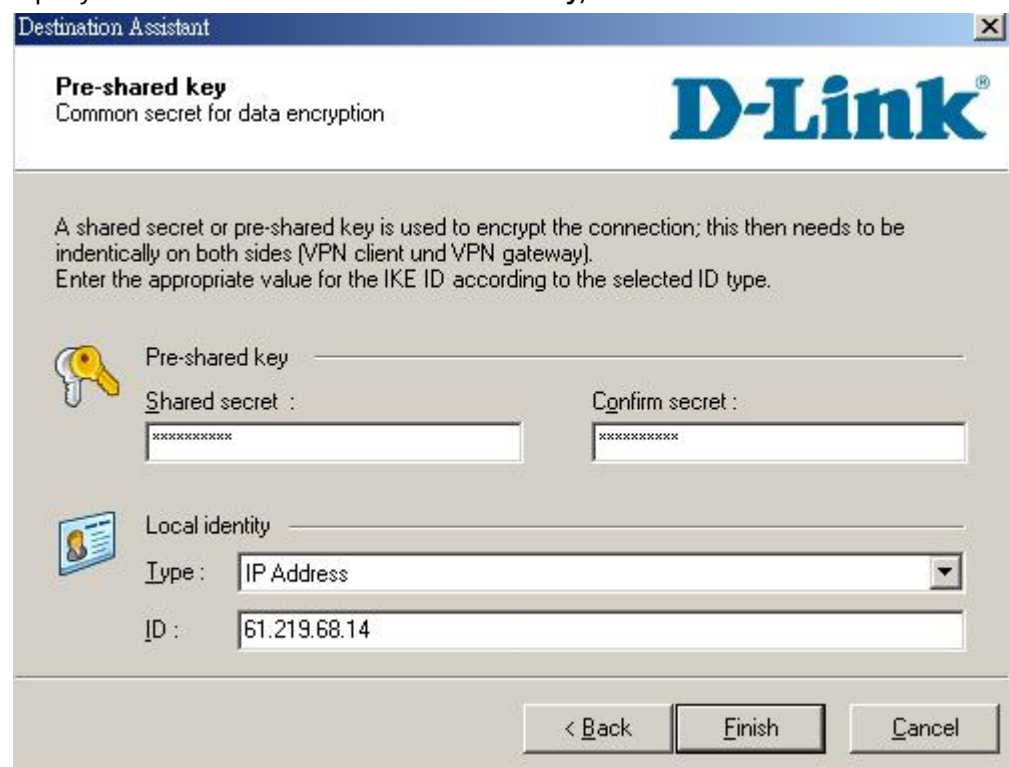
Password (Confirm)
[Empty field]

< Back Next Cancel

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.



The screenshot shows the 'Destination Assistant' window with the title bar 'Destination Assistant' and a close button. The main heading is 'Pre-shared key' with the subtext 'Common secret for data encryption'. The D-Link logo is in the top right. Below the heading, it says 'A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically on both sides (VPN client und VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type.' There are two input fields for the 'Pre-shared key': 'Shared secret' and 'Confirm secret', both containing 'xxxxxxxx'. Below these is the 'Local identity' section with a dropdown menu for 'Type' set to 'IP Address' and an input field for 'ID' containing '61.219.68.14'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.

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 identically 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 : xxxxxxxx Confirm secret : xxxxxxxx

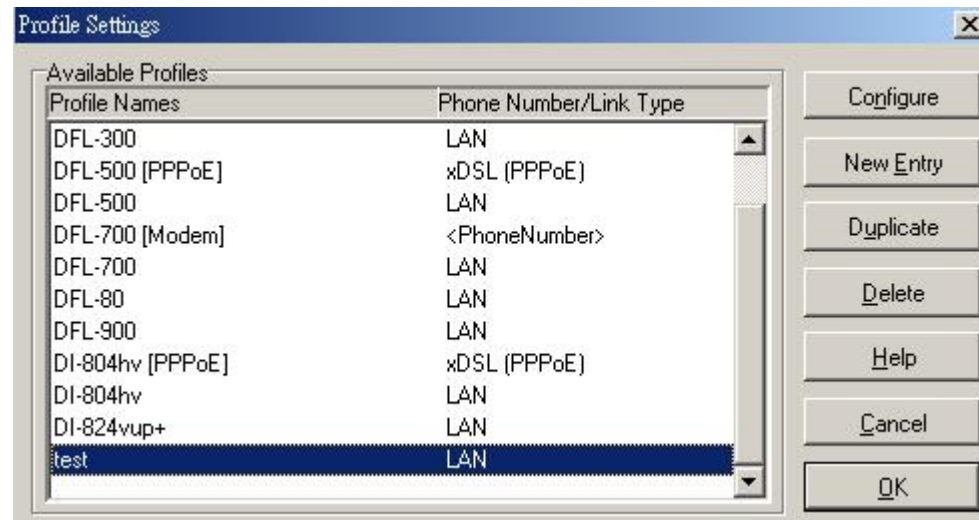
Local identity
Type : IP Address
ID : 61.219.68.14

< Back Finish Cancel

D-Link corporation

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

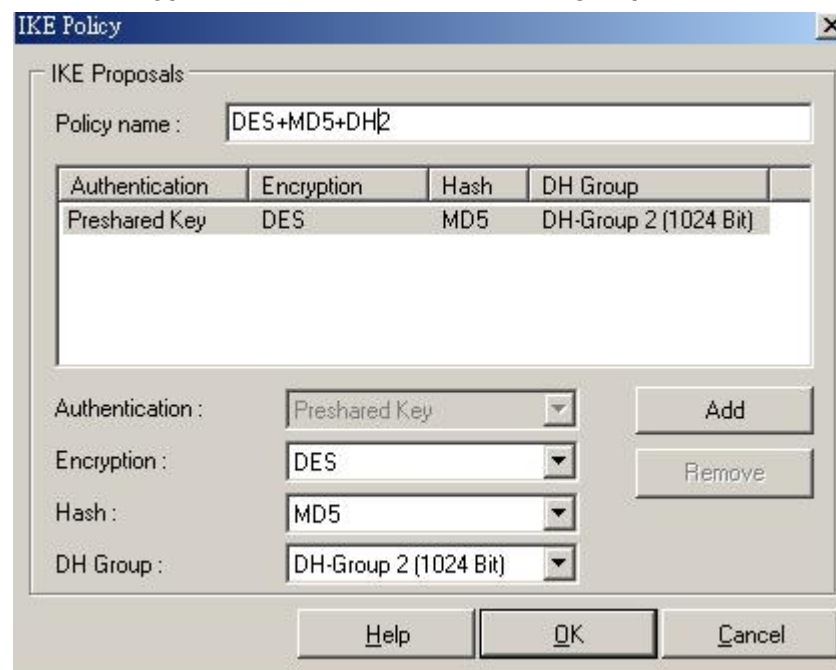




Setup7

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.

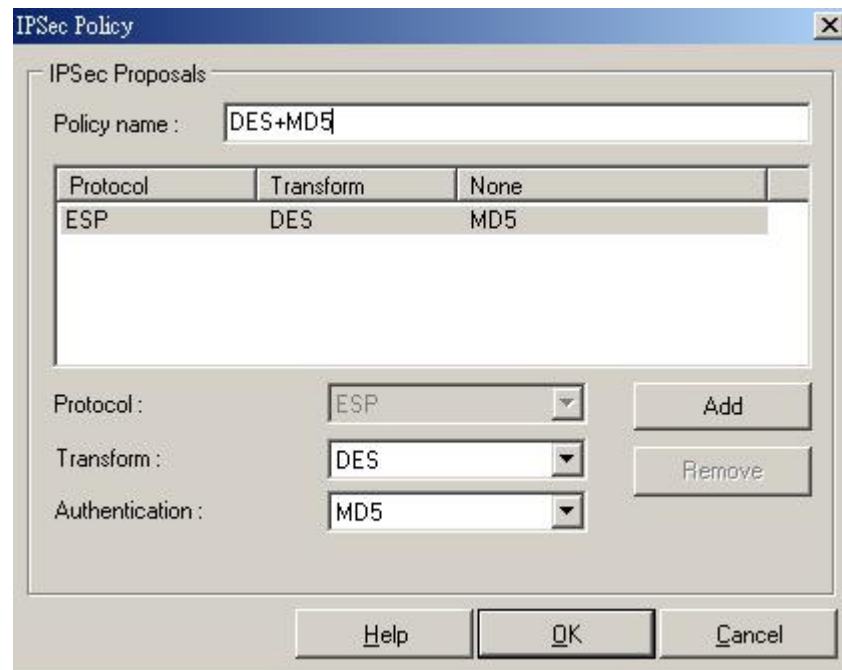


D-Link corporation

Setup8

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

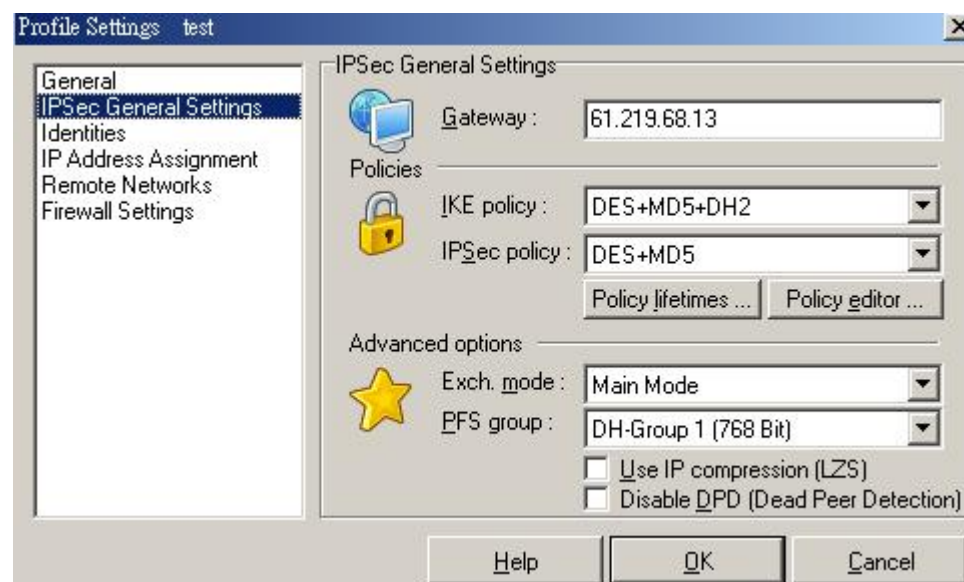
Select **Transform** as DES, **Authentication** as MD5 and click OK button.



Setup9

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

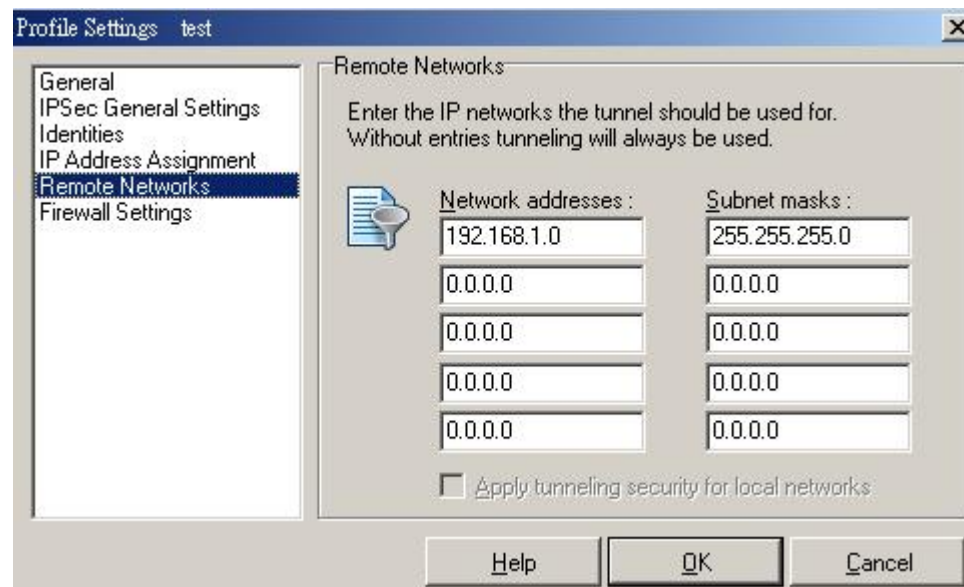
Select **IKE policy** as DES+MD5+DH2, **IPSec policy** as DES+MD5, **Exch. mode** as Main Mode, **PFS group** as DH-1



D-Link corporation

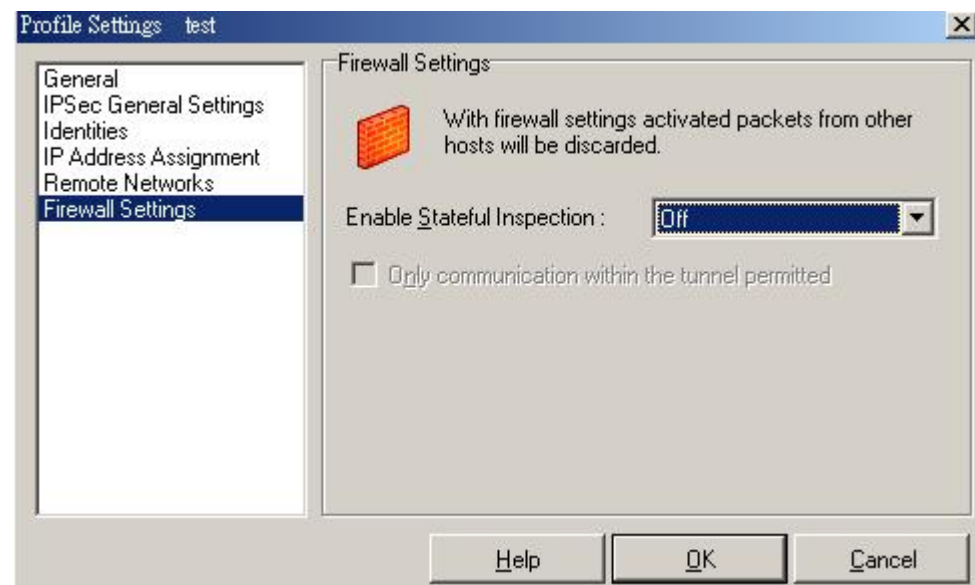
Setup10

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.



D-Link corporation

Setup12

Click **Connect** button to establish IPSec tunnel



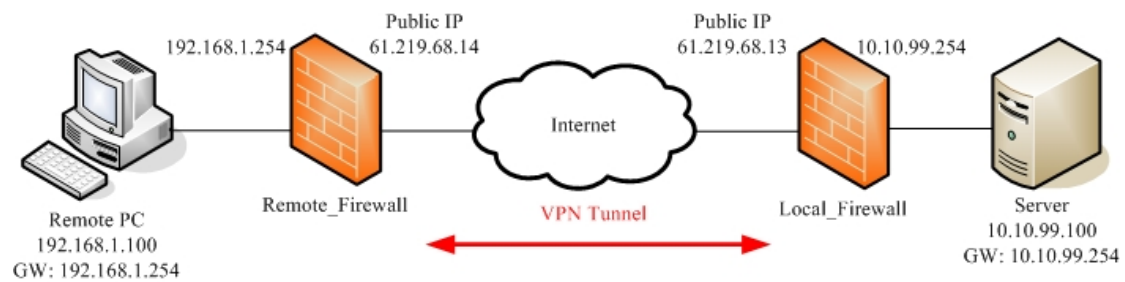
2. LAN to LAN

2-1 Objective:

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

2-2 Environment:

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	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**)

IPSec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

☒ **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: ●●●●●●●●

Apply

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

IPSec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

☒ **Enable PPTP Client**

[Server] **[Client]**

Server IP: 61.219.68.13

Username: firewall Password: ●●●●●●●●

Assigned IP: 10.10.99.201

Apply

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

Static Route **Policy 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	-	-	-	-

D-Link corporation

DFL-1100/700/200

01- Add User (Firewall -> Users)

User Management

Add new user:

User name:	firewall
Group membership:	
Password:	xxxxxxx
Retype password:	xxxxxxx

L2TP/PPTP settings:

Static client IP:

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

Networks behind user:

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 relay addresses
Primary WINS:	(Optional)
Secondary WINS:	(Optional)

03- Enable PPTP Client (Firewall -> VPN)

D-Link corporation

L2TP/PPTP Clients

Add PPTP Client :

Name: pptp-client

Basic settings:

Username: firewall

Password: xxxxxxxx

Retype Password: xxxxxxxx

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 Relay 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	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**)

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

Back Apply

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

Back Apply

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

D-Link corporation

[Status](#) [Edit Rules](#) [Show Rules](#) [Attack Alert](#) [Summary](#)

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☒ Log

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

Prev. Page Next Page Move Page 1

Move Before: 1

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name:

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**)

[IPSec](#) [VPN Hub](#) [VPN Spoke](#) [PPTP](#) [L2TP](#) [Pass Through](#)

☒ 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	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	Encrypt and Authenticate (DES, MD5) Encrypt and Authenticate (DES, SHA1) Encrypt and Authenticate (3DES, MD5) Encrypt and Authenticate (3DES, SHA1)
Key Group	Encrypt and Authenticate (3DES, SHA1)

Phase 1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

SA Life Time ☒ sec ☐ min ☐ hour

Key Group

Phase 2

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

SA Life Time

Perfect Forward Secrecy(PFS)

to Save Running Configur

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)

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

SA Life Time ☒ sec ☐ min ☐ hour

Perfect Forward Secrecy(PFS)

Local_Firewall:

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

Address | **Service** | **Schedule**

[Objects] [Groups]

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 | **Service** | **Schedule**

[Objects] [Groups]

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)

D-Link corporation

Status **Edit Rules** **Show Rules** **Attack Alert** **Summary**

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

Prev. Page Next Page Move Page 1

Insert **Edit** **Delete** Move Before: 1

Status **Edit Rules** **Show Rules** **Attack Alert** **Summary**

Firewall->Edit Rules->Edit

Edit WAN1-to-LAN1 Firewall rule number 1

Status

Rule name:

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**

Back **Apply**

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

IPSec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

☒ **Enable IPSec** **Apply**

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)

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

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): ☐

Back

to **Save Running Configuration**

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

Back

Apply

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:

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



Apply



Cancel



Help

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

VPN Tunnels

Edit IPsec tunnel **ipsec**:

Name:

Local Net:

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:

Retype PSK:

1234567890

☐ **Certificate-based**

Local Identity:

Certificates:

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

Identity List:

D-Link corporation

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:

Remote Gateway:

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:

IKE Mode: ☒ Main mode IKE

☐ Aggressive mode IKE

IKE DH Group:

PFS: ☒ Enable Perfect Forward Secrecy

PFS DH Group:

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:	DES	MD5	0	28800
#3:	CAST-128	SHA-1	0	28800
#4:	Blowfish-40 Allowed: 40-448	MD5	0	28800
#5:	Blowfish-128 Allowed: 40-448	SHA-1	0	28800
#6:	Blowfish-256 Allowed: 128-448	MD5	0	28800
#7:	Blowfish-256 Allowed: 256-448	MD5	0	0
#8:	Blowfish-448 Allowed: 256-448	MD5	0	0

IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:	DES	MD5	0	3600
#3:	CAST-128	SHA-1	0	3600
#4:	Blowfish-40 Allowed: 40-448	MD5	0	3600
#5:	Blowfish-128 Allowed: 40-448	SHA-1	0	3600
#6:	Blowfish-256 Allowed: 128-448	MD5	0	3600
#7:	Blowfish-256 Allowed: 256-448	MD5	0	0
#8:	Blowfish-448 Allowed: 256-448	MD5	0	0

Local_Firewall:

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

Firewall Policy

Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL:

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



Apply



Cancel



Help

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

VPN Tunnels

Edit IPSec tunnel **ipsec**:

Name:

Local Net:

Authentication:

☒ **PSK** - Pre-Shared Key

PSK:

Retype PSK:

1234567890

☐ **Certificate-based**

Local Identity:

Certificates:

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

Identity List:

D-Link corporation

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:

Remote Gateway:

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:

IKE Mode: ☒ Main mode IKE
☐ Aggressive mode IKE

IKE DH Group:

PFS: ☒ Enable Perfect Forward Secrecy

PFS DH Group:

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:	DES	MD5	0	28800
#3:	CAST-128	SHA-1	0	28800
#4:	Blowfish-40 Allowed:40-448	MD5	0	28800
#5:	Blowfish-128 Allowed:40-448	SHA-1	0	28800
#6:	Blowfish-256 Allowed:40-448	MD5	0	28800
#7:	Blowfish-128 Allowed:128-448	MD5	0	0
#8:	Blowfish-256 Allowed:128-448	MD5	0	0
#9:	Blowfish-256 Allowed:256-448			
#10:	Blowfish-448 Allowed:256-448			
#11:	Blowfish-448 Allowed:448-448			
#12:	Twofish-128 Allowed:128-256			
#13:	Twofish-256 Allowed:128-256			
#14:	Twofish-256 Allowed:256-256			
#15:	AES-128 Allowed:128-256			
#16:	AES-256 Allowed:128-256			
#17:	AES-256 Allowed:256-256			

IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	DES	MD5	0	3600
#2:	DES	MD5	0	3600
#3:	CAST-128	SHA-1	0	3600
#4:	Blowfish-40 Allowed:40-448	MD5	0	3600
#5:	Blowfish-128 Allowed:40-448	SHA-1	0	3600
#6:	Blowfish-256 Allowed:40-448	MD5	0	3600
#7:	Blowfish-128 Allowed:128-448	MD5	0	0
#8:	Blowfish-256 Allowed:128-448	MD5	0	0
#9:	Blowfish-256 Allowed:256-448			
#10:	Blowfish-448 Allowed:256-448			
#11:	Blowfish-448 Allowed:448-448			
#12:	Twofish-128 Allowed:128-256			
#13:	Twofish-256 Allowed:128-256			
#14:	Twofish-256 Allowed:256-256			
#15:	AES-128 Allowed:128-256			
#16:	AES-256 Allowed:128-256			
#17:	AES-256 Allowed:256-256			

This unit will propose 128 bit encryption to the remote peer. It will not accept any cipher key sizes between 128 and 256 bits.



DFL-600

Remote_Firewall:

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

[Policy Rules](#) / [Global Policy Status](#) / [Policies](#)

Inbound Port Filter

- ☒ Enabled
- ☒ Allow all except policy settings
- ☐ Deny all except policy settings

Outbound Port Filter

- ☒ Enabled
- ☒ Allow 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	

D-Link corporation

[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

D-Link corporation

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