

D-Link VPN Application
Руководство по быстрой установке

Содержание

1-1 Цель:	2
1-2 Окружение:	3
1-3 Настройка	3
2-1 Цель:	30
2-2 Окружение:	30
2-3 Параметры настройки:	30
2-3-1 Сервер PPTP и клиент PPTP.....	30

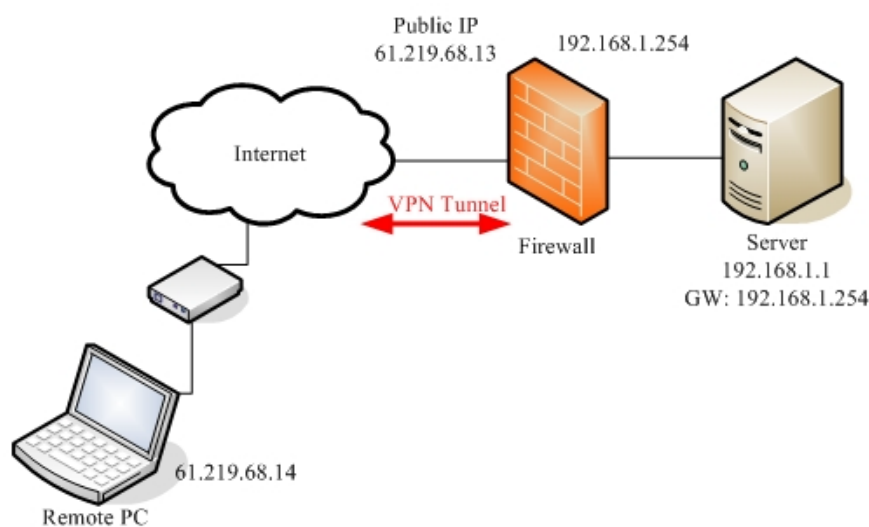
1. Удаленный доступ

1-1 Цель:

Кто-либо находится вне офиса и нуждается в подключении к сети компании, используя VPN (PPTP/L2TP/IPSec).

1-2 Окружение:

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



1-3 Настройка

1-3-1 Сервер PPTP

Настройки удаленного ПК	Настройки межсетевого экрана
01-IP-адрес ПК: 61.219.68.13	01-Включить сервер PPTP
02-Тип VPN: PPTP	02-Локальный IP-адрес: 192.168.1.254
03-Имя пользователя: firewall	03-Диапазон IP-адресов: 192.168.1.100~105
04-Пароль: firewall	04-Имя пользователя: firewall
	05-Пароль: firewall

Страница настройки параметров устройства

DFL-1500

01- Включить сервер PPTP (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:

Assigned IP Range

Start: End:

Username: Password:

DFL-1100/700/200

01- Добавить пользователя (Firewall -> Users)

User Management

Add new user:

User name:

Group membership:

Password:

Retype password:

02- Включить сервер PPTP (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- Добавить пользователя (**Advanced** -> **VPN-PPTP** -> **PPTP Account**)

[PPTP Settings](#) / [PPTP Account](#) / [PPTP Status](#)

Add/New User Account

User Name	<input type="text" value="firewall"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

02- Включить сервер PPTP (**Advanced** -> **VPN-PPTP** -> **PPTP settings**)

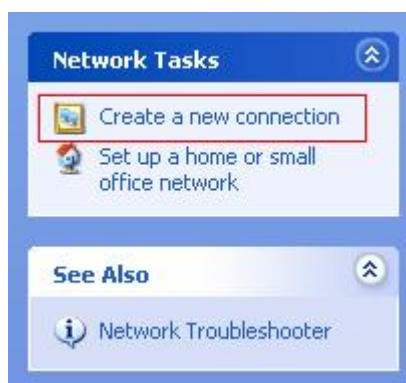
[PPTP Settings](#) / [PPTP Account](#) / [PPTP Status](#)

PPTP Pass Through	<input type="checkbox"/> Enable
PPTP Status	<input checked="" type="checkbox"/> Enable
Starting IP address	<input type="text" value="192.168.1.100"/>
Ending IP address	<input type="text" value="192.168.1.105"/>

Настройка клиента PPTP (VPN-адаптер ОС Microsoft XP PRO)

Шаг 1

В свойствах сетевого окружения выберите “Новое подключение” для того, чтобы создать исходящее подключение VPN-PPTP.



Шаг 2

Нажмите **Next** для перехода на следующий шаг.



D-Link corporation

Шаг 3

Выберите **Подключить к сети на рабочем месте**. Нажмите **Next** для перехода на следующий шаг.

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

D-Link corporation

Шаг 4

Выберите **Подключение к виртуальной частной сети**. Нажмите **Next** для перехода на следующий шаг.

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

Шаг 5

Введите имя подключения PPTP. Нажмите **Next** для перехода на следующий шаг.

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

PPTP

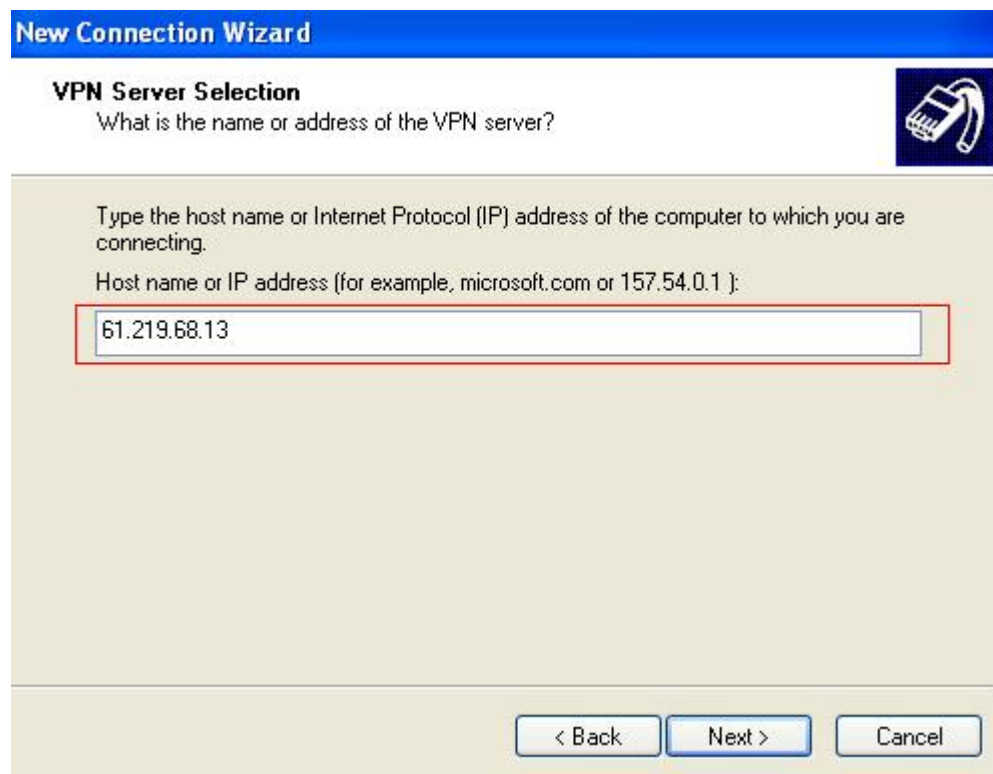
For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel

D-Link corporation

Шаг 6

Введите IP-адрес сервера VPN-PPTP (адрес внешнего интерфейса устройства): 61.219.68.13. Нажмите **Next** для перехода на следующий шаг.



New Connection Wizard

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

< Back Next > Cancel

Шаг 7

Нажмите **Готово** для завершения настройки параметров VPN-PPTP.



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.

< Back **Finish** Cancel

D-Link corporation

Шаг 8

Введите имя пользователя в поле User Name и пароль в поле Password. Нажмите **Подключиться** для установки соединения.



Connect PPTP

User name: firewall

Password: ●●●●●●●●●●

Save this user name and password for the following users:

Me only

Anyone who uses this computer

Connect Cancel Properties Help

1-3-2 L2TP без IPSec

Настройки удаленного ПК	Настройки межсетевого экрана

Например: DFL-1500 с VPN-адаптером Microsoft (Windows 2K)

1-3-3 IPSec

Настройки удаленного ПК	Настройки межсетевого экрана
01- Имя профиля: test	01- Имя политики: IPSec
02- Среда взаимодействия: LAN over IP	02- Локальный IP-адрес: 192.168.1.0/24
03- Шлюз: 61.219.68.13	03- Удаленный IP-адрес: 61.219.68.14
04- Политика IKE: DES+MD5	04- Режим согласования: Main
05- Группа ключей IKE: DH2	05- Режим инкапсуляции: Tunnel
06- Политика IPSec: DES+MD5 (ESP)	06- Конечный IP-адрес туннеля: 61.219.68.14
07- Группа ключей IPSec: DH1	07- PSK: 1234567890
08- Режим согласования: Main	08- Политика IKE: DES+MD5
09- Локальный идентификатор: IP address	09- Группа ключей IKE: DH2
10- Идентификатор ID: 61.219.68.14	10- Политика IPSec: DES+MD5 (ESP)
11- PSK: 1234567890	11- Группа ключей IPSec: DH1
12- Удаленные сети: 192.168.1.0/24	
13- Отключить межсетевой экран	

Настройка параметров устройства

DFL-1500/900

01- Добавить адреса (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

D-Link corporation

02- Отредактировать правила межсетевого экрана (**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:

Condition

Source IP: Dest. IP:

Service:

Action

and the matched session.

Forward bandwidth class:

Reverse bandwidth class:

Back **Apply**

03- Включить IPSec и отредактировать политику IPSec (**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

Condition

Local Address Type

IP Address

PrefixLen / Subnet Mask

Remote Address Type

IP Address

PrefixLen / Subnet Mask

Action

Negotiation Mode

Encapsulation Mode

Outgoing Interface

Peer's IP Address

My Identifier

Peer's Identifier

ESP Algorithm

AH Algorithm

Pre-Shared Key

Phase 1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

SA Life Time

Key Group

Phase 1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

SA Life Time sec min hour

Key Group

- DH1
- DH2**
- DH5

Phase 2

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

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)

to Save Running Configur

Phase 2

Encapsulation

Active Protocol

Encryption Algorithm

SA Life Time sec min hour

Perfect Forward Secrecy(PFS)

- None
- DH1**
- DH2
- DH5

DFL-1100/700/200

01- Разрешить весь трафик VPN (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.



02- Включить IPSec и отредактировать политику IPSec (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:

D-Link corporation

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	DES	MD5	0	28800
#2:	DES	MD5	0	28800
#3:	3DES	MD5	0	28800
#4:	CAST-128	SHA-1	0	28800
#5:	Blowfish-40 Allowed: 40-448	MD5	0	28800
#6:	Blowfish-128 Allowed: 40-448	MD5	0	28800
#7:	Blowfish-256 Allowed: 40-448	SHA-1	0	28800
#8:	Blowfish-128 Allowed: 128-448	MD5	0	28800
#9:	Blowfish-256 Allowed: 128-448	MD5	0	28800
#10:	Blowfish-256 Allowed: 256-448	MD5	0	28800
#11:	Blowfish-448 Allowed: 256-448	MD5	0	0
#12:	.	MD5	0	0

IPsec Proposal List

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

DFL-600

01- Разрешить весь трафик VPN (**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- Включить IPSec и отредактировать политику IPSec (**Firewall -> VPN -> IPSec Tunnels**)

[IPSec Settings](#) / [Manual Key](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

Add/New Tunnel

Tunnel Name	<input type="text" value="ipsec"/>
Peer Tunnel Type	<input type="text" value="Static IP address"/> ▼
Termination IP	<input type="text" value="61.219.68.14"/>
DomainName	<input type="text"/>
Peer ID Type	<input type="text" value="Address(IPV4_Addr)"/> ▼
Peer ID	<input type="text" value="61.219.68.14"/> (optional)
Shared Key	<input type="text" value="1234567890"/>
IKE Mode	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
Encapsulation	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport mode
NAT traversal	<input checked="" type="radio"/> Normal <input type="radio"/> ESP Over UDP (port 500)
IPSec Operation	<input type="text" value="ESP"/> ▼

Phase 1 Proposal

Name	<input type="text" value="P1Param"/>
DH Group	<input type="text" value="Group 2"/> ▼
IKE Life Duration	<input type="text" value="6000"/> seconds
IKE Encryption	<input type="text" value="DES"/> ▼
IKE Hash	<input type="text" value="MD5"/> ▼

D-Link corporation

Phase 2 Proposal

Name	<input type="text" value="P2Param"/>
PFS Mode	<input type="button" value="Group 1"/>
Encapsulation	<input type="button" value="ESP"/>
IPSec Life Duration	<input type="text" value="6000"/> seconds
ESP Transform	<input type="button" value="DES"/>
ESP Auth	<input type="button" value="HMAC-MD5"/>
AH Transform	<input type="button" value="MD5"/>

[Click here to add P1 proposal](#)

P1 Proposals	<input type="button" value="P1Param"/>	<input type="button" value="NOT_SET"/>
	<input type="button" value="NOT_SET"/>	<input type="button" value="NOT_SET"/>

[Click here to add P2 proposal](#)

P2 Proposals	<input type="button" value="P2Param"/>	<input type="button" value="NOT_SET"/>
	<input type="button" value="NOT_SET"/>	<input type="button" value="NOT_SET"/>

Target Host Range

Starting Target Host	<input type="text" value="61.219.68.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Настройка подключения IPSec (D-Link DS-601)

Шаг 1

Configuration->Profile settings->New Entry

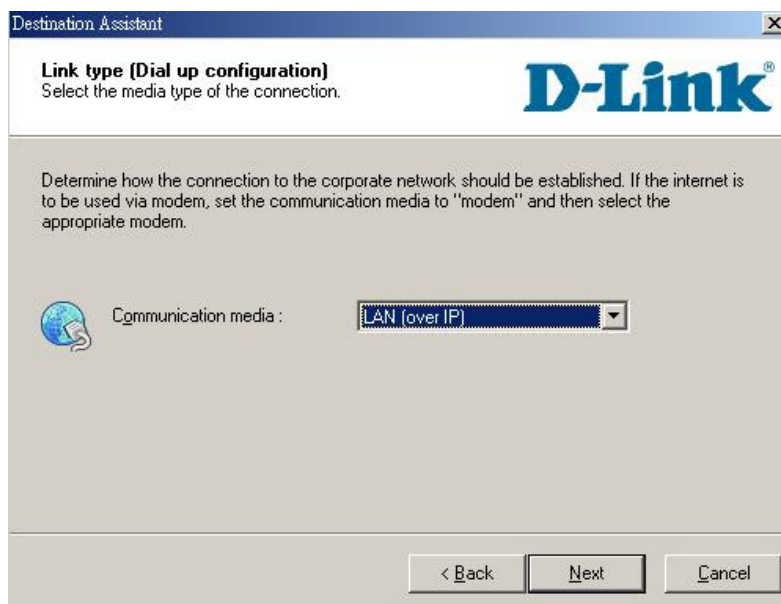
Введите **имя профиля** и нажмите кнопку **Next**



The screenshot shows a window titled "Destination Assistant" with a close button (X) in the top right corner. The main heading is "Connection Name" with the instruction "Enter the name of the connection". The D-Link logo is in the top right. Below the heading, it says "The connection may be given a descriptive name; enter a name in the following field." There is a yellow star icon to the left of a text input field labeled "Name of the connection" which contains the text "test". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Шаг 2

В качестве среды взаимодействия в поле Communication media выберите **LAN over IP** и нажмите кнопку **Next**.

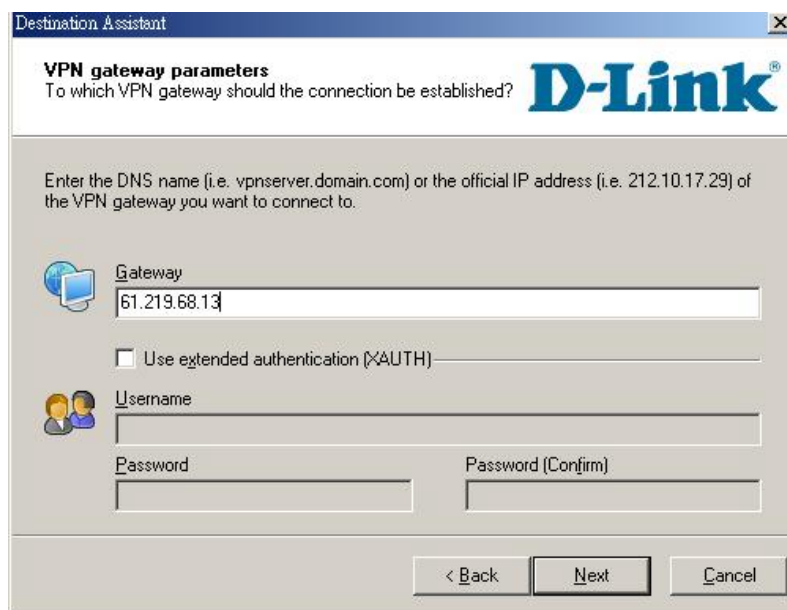


The screenshot shows a window titled "Destination Assistant" with a close button (X) in the top right corner. The main heading is "Link type (Dial up configuration)" with the instruction "Select the media type of the connection". The D-Link logo is in the top right. Below the heading, it says "Determine 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." There is a globe icon to the left of a dropdown menu labeled "Communication media:" which is set to "LAN (over IP)". At the bottom, there are three buttons: "< Back", "Next", and "Cancel".

Шаг 3

D-Link corporation

Введите адрес шлюза VPN (61.219.68.13) и нажмите кнопку **Next**

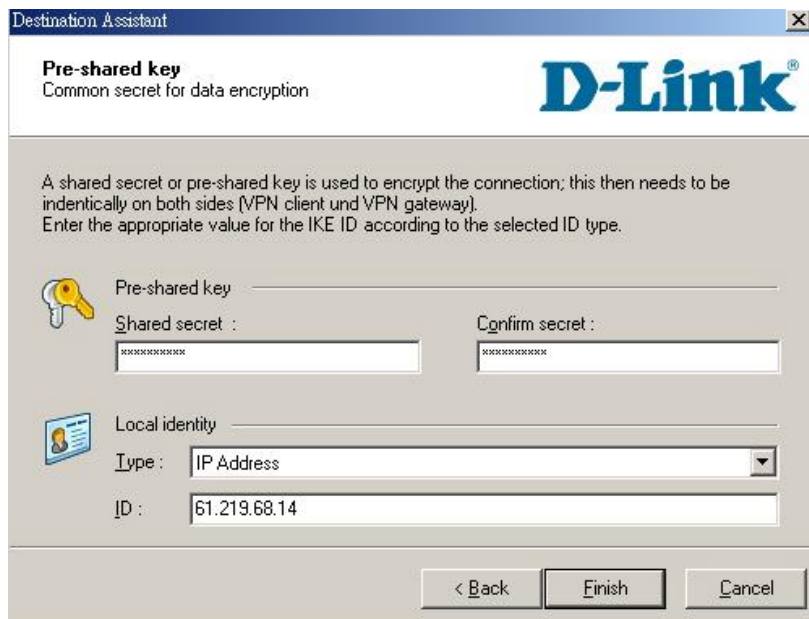


The screenshot shows a window titled "Destination Assistant" with the "VPN gateway parameters" section. The text asks, "To which VPN gateway should the connection be established?" and provides instructions: "Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to." The "Gateway" field contains "61.219.68.13". There is an unchecked checkbox for "Use extended authentication (XAUTH)". The "Username" and "Password" fields are empty. At the bottom, there are buttons for "< Back", "Next", and "Cancel".

Шаг 4

Введите ключ 1234567890 в поле **Shared secret** и затем повторно введите его в поле **Confirm secret**.

Введите Ваш локальный IP-адрес в поле **Local identity** и нажмите кнопку **Finish**.

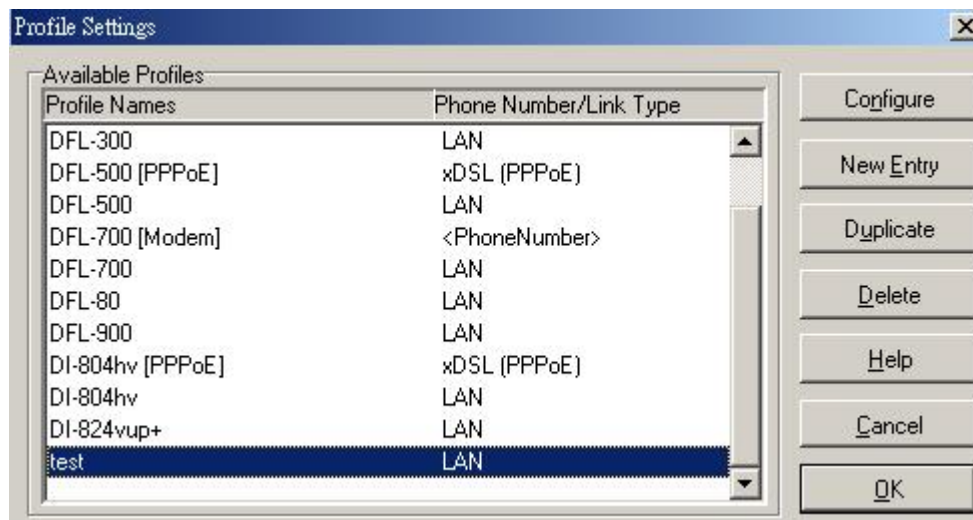


The screenshot shows a window titled "Destination Assistant" with the "Pre-shared key" section. The text explains: "A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically on both sides (VPN client und VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type." The "Pre-shared key" field is empty. The "Shared secret" and "Confirm secret" fields both contain "XXXXXXXXXX". The "Local identity" section has a "Type" dropdown menu set to "IP Address" and an "ID" field containing "61.219.68.14". At the bottom, there are buttons for "< Back", "Finish", and "Cancel".

D-Link corporation

Шаг 5

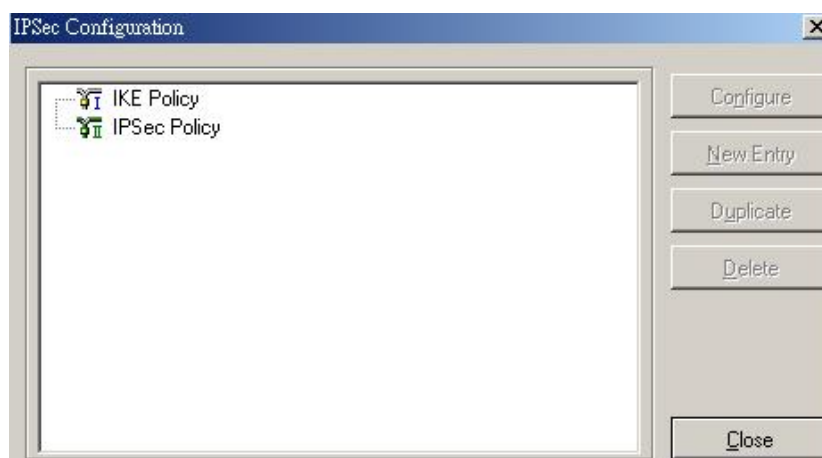
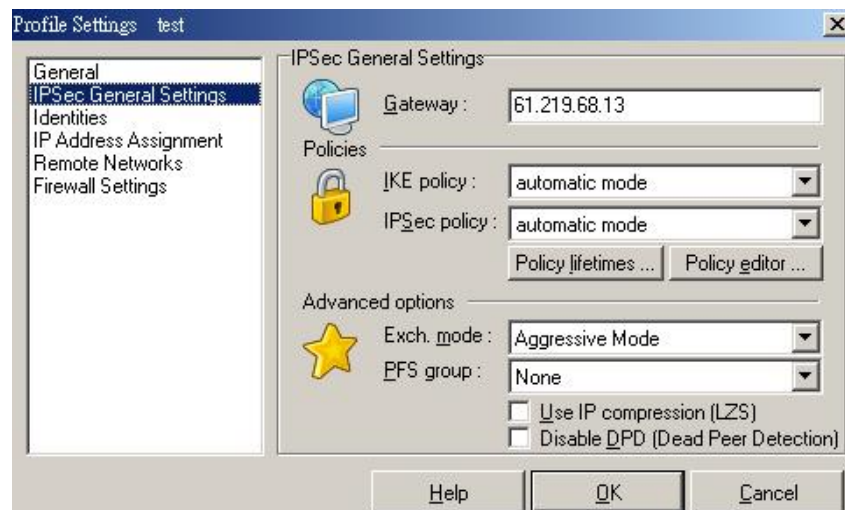
По завершении настройки параметров Вы увидите, что был добавлен новый профиль.



Шаг 6

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

Нажмите кнопку **Policy editor**, чтобы отредактировать политики IPSec и IKE.

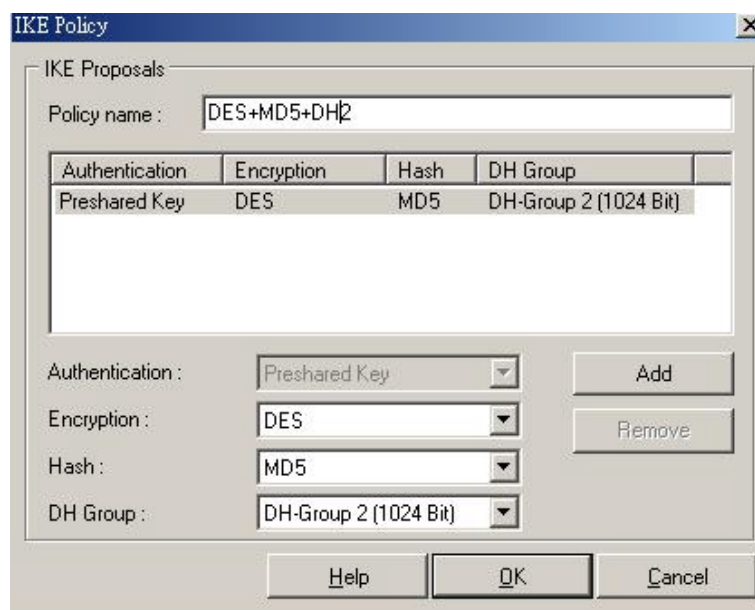


D-Link corporation

Шаг 7

Нажмите **IKE Policy->New Entry**, введите DES+MD5+DH2 в качестве имени политики IKE в поле Policy name.

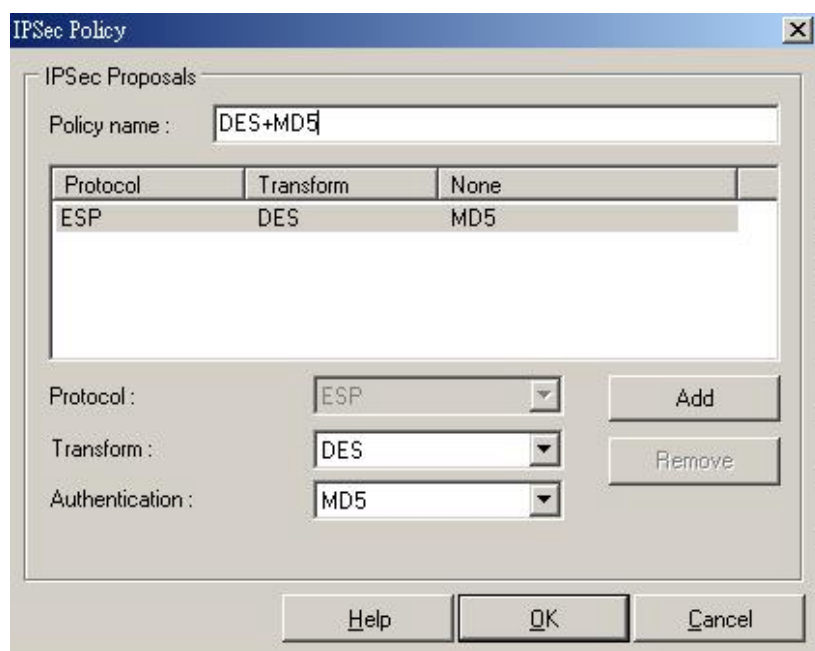
Выберите DES в качестве алгоритма шифрования в поле **Encryption**, MD5 в качестве алгоритма хеширования в поле **Hash**, DH2 в качестве группы ключей в поле **DH group** и нажмите кнопку **OK**.



Шаг 8

Нажмите **IPSec Policy->New Entry**, введите DES+MD5 в качестве имени политики IPSec в поле Policy name.

Выберите DES в качестве алгоритма шифрования в поле **Transform**, MD5 в качестве алгоритма аутентификации в поле **Authentication** и нажмите кнопку **OK**.

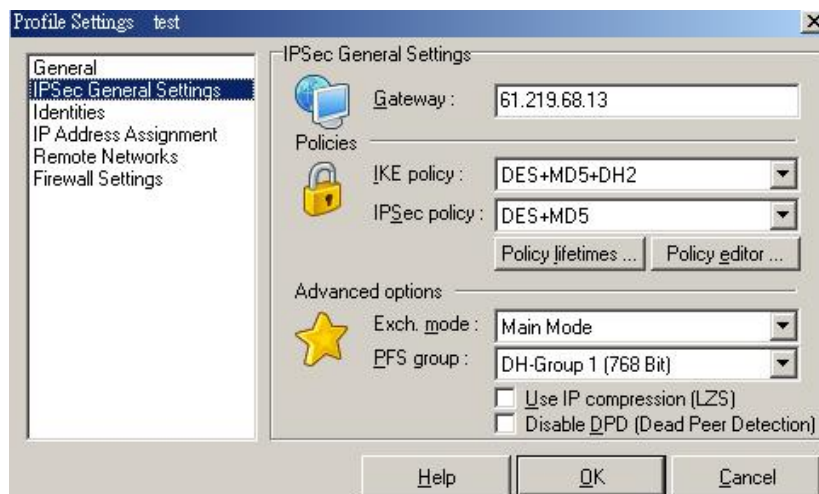


D-Link corporation

Шаг 9

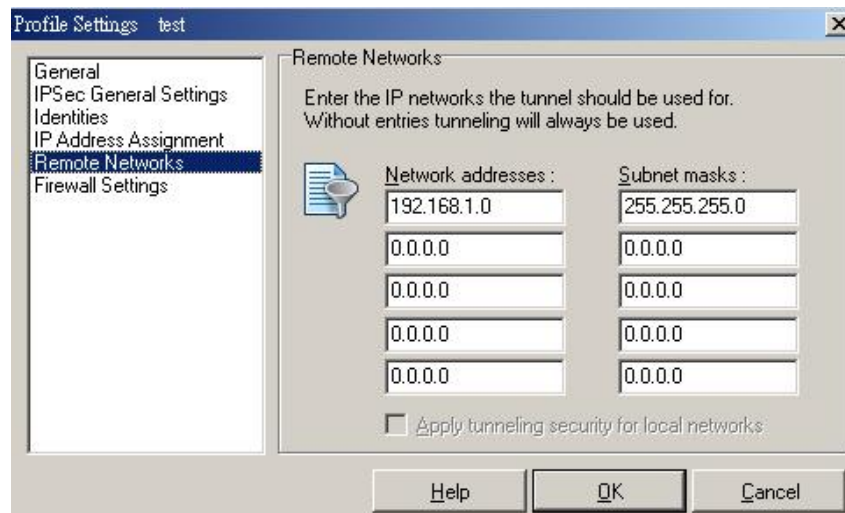
Configuration->Profile settings->test->IPSec General Settings

Выберите DES+MD5+DH2 в качестве политики IKE в поле **IKE policy**, DES+MD5 в качестве политики IPSec в поле **IPSec policy**, Main Mode в качестве режима согласования в поле **Exch. mode** и DH-1 в поле **PFS group**



Шаг 10

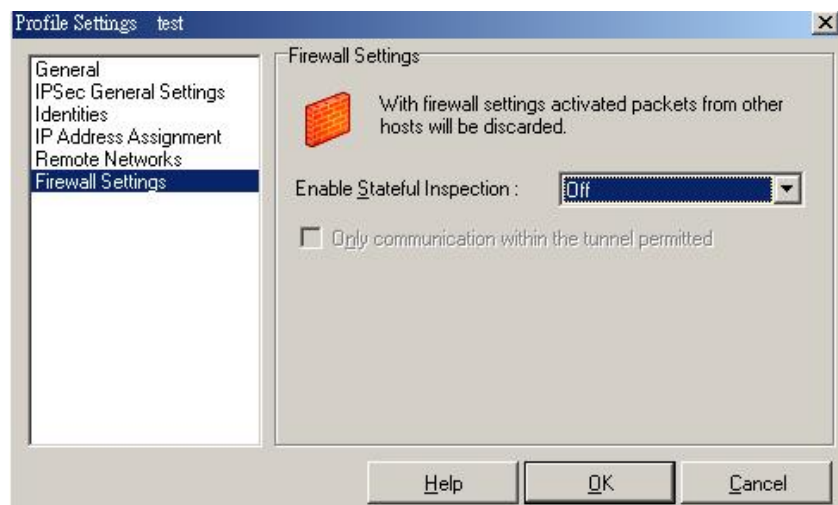
Настройте параметры удаленных сетей в меню **Remote Networks**, введите адрес сети 192.168.10.1 в поле **Network address** и маску подсети 255.255.255.0 в поле **Subnet masks**.



D-Link corporation

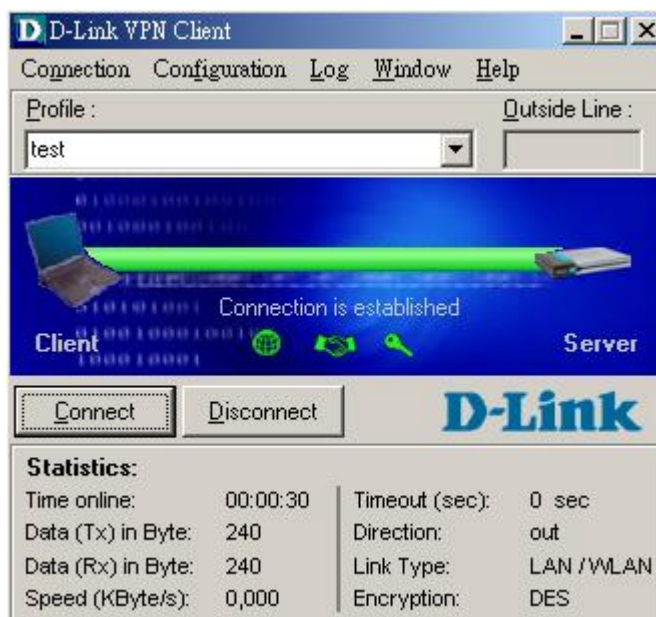
Шаг 11

Настройте параметры межсетевых экранов в меню Firewall settings, выберите Off в поле **Enable Stateful Inspection** и нажмите кнопку **OK**.



Шаг 12

Нажмите кнопку **Connect** для установления туннеля IPSec



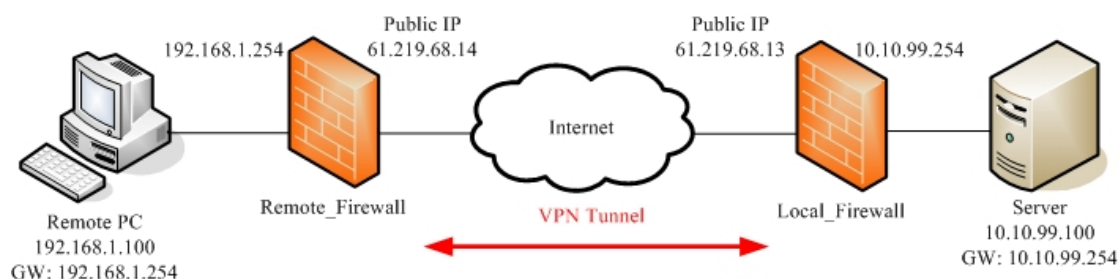
2. Туннель между двумя сетями (LAN to LAN).

2-1 Цель:

Удаленный офис хочет соединиться с другим офисом через Интернет.

2-2 Окружение:

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



2-3 Параметры настройки:

2-3-1 Сервер PPTP и клиент PPTP

Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана
1- Включить клиент PPTP	1- Включить сервер PPTP
2- IP-адрес сервера: 61.219.68.13	2- Локальный IP-адрес: 10.10.99.254
3- Имя пользователя: firewall	3- Диапазон IP-адресов: 10.10.99.200-205
4- Пароль: firewall	4- Имя пользователя: firewall
	5- Пароль: firewall

DFL-1500

1- Включить сервер PPTP (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

2- Включить клиент PPTP (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

3- Добавить статический маршрут (Advanced settings -> Routing -> Static Route)

Static Route Policy Route

#	Type	Destination/Netmask	Gateway	Activated	
<input checked="" type="radio"/>	1	Net	10.10.99.0/255.255.255.0	10.10.99.201	Yes
<input type="radio"/>	2	-	-	-	-
<input type="radio"/>	3	-	-	-	-
<input type="radio"/>	4	-	-	-	-
<input type="radio"/>	5	-	-	-	-
<input type="radio"/>	6	-	-	-	-

DFL-1100/700/200

1- Добавить пользователя (Firewall -> Users)

User Management

Add new user:

User name:	<input type="text" value="firewall"/>
Group membership:	<input type="text"/>
Password:	<input type="password" value="*****"/>
Retype password:	<input type="password" value="*****"/>

L2TP/PPTP settings:

Static client IP:	<input type="text"/>	If empty, the IP address will be taken from the server's IP pool
Networks behind user:	<input type="text" value="192.168.1.0/24"/>	

2- Включить сервер PPTP (Firewall -> VPN)

L2TP/PPTP Servers

Edit PPTP tunnel **pptp-server**:

Name:	<input type="text" value="pptp-server"/>	
Outer IP:	<input type="text"/>	Blank = WAN IP
		Must be WAN IP if IPsec encryption is required
Inner IP:	<input type="text"/>	Blank = LAN IP

IP Pool and settings:

Client IP Pool:	<input type="text" value="10.10.99.200 - 10.10.99.205"/>
	<input checked="" type="checkbox"/> Proxy ARP dynamically added routes
Primary DNS:	<input type="text"/> (Optional)
Secondary DNS:	<input type="text"/> (Optional)
	<input checked="" type="checkbox"/> Use unit's own DNS relay addresses
Primary WINS:	<input type="text"/> (Optional)
Secondary WINS:	<input type="text"/> (Optional)

3- Включить сервер PPTP (Firewall -> VPN)

D-Link corporation

L2TP/PPTP Clients

Add PPTP Client :

Name:

Basic settings:

Username:
Password:
Retype Password:

Interface IP: Blank = get IP from server

Remote Gateway:
Remote Net:

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 Сервер L2TP и клиент L2TP

Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана

2-3-3 IPSec

Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана
1- Включить IPSec	1- Включить IPSec
2- Локальный IP-адрес: 192.168.1.0/24	2- Локальный IP-адрес: 10.10.99.0/24
3- Удаленный IP-адрес: 10.10.99.0/24	3- Удаленный IP-адрес: 192.168.1.0/24
4- Режим согласования: Main mode	4- Режим согласования: Main mode
5- Режим инкапсуляции: Tunnel mode	5- Режим инкапсуляции: Tunnel mode
6- Конечный IP-адрес туннеля: 61.219.68.13	6- Конечный IP-адрес туннеля: 61.219.68.14
7- Ключ PSK: 1234567890	7- Ключ PSK: 1234567890
8- Политика IKE: DES+MD5	8- Политика IKE: DES+MD5
9- Группа ключей IKE: DH2	9- Группа ключей IKE: DH2
10- Политика IPSec: DES+MD5 (ESP)	10- Политика IPSec: DES+MD5 (ESP)
11- Группа ключей IPSec: DH1	11- Группа ключей IPSec: DH1

DFL-1500

Удаленный межсетевой экран:

01- Добавить адреса (**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- Отредактировать правила межсетевого экран (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				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

Insert Edit Delete Move Before: 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

Back Apply

D-Link corporation

03- Включить IPSec и отредактировать политику IPSec (**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 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)
Key Group	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 <input checked="" type="radio"/> sec <input type="radio"/> min <input type="radio"/> hour
Key Group	DH2 ▾
	DH1
	DH2
	DH5

Phase 2

Phase 2

Encapsulation	Tunnel
Active Protocol	ESP
Encryption Algorithm	Encrypt and Authenticate (DES, MD5) ▾
SA Life Time	Encrypt and Authenticate (DES, MD5)
Perfect Forward Secrecy(PFS)	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

D-Link corporation

Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 sec min hour

Perfect Forward Secrecy(PFS): DH1

None
DH1
DH2
DH5

Back Apply

Локальный межсетевой экран:

01- Добавить адреса (**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

Back Apply

D-Link corporation

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- Отредактировать правила межсетевого экрана (**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

Packets are top-down matched by the rules.

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

Prev. Page Next Page Move Page 1

 Move Before: 1

D-Link corporation

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

Firewall->Edit Rules->Edit

Edit WAN1-to-LAN1 Firewall rule number 1

Status

Rule name:

Schedule:

Condition

Source IP: Dest. IP:

Service:

Action

and the matched session.

Forward bandwidth class:

Reverse bandwidth class:

03- Включить IPSec и отредактировать политику IPSec (**Advanced Settings -> VPN Settings**)

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

Enable IPSec

IPSec->IKE->Edit Rule

Status

Active

IKE Rule Name

Condition

Local Address Type

IP Address

PrefixLen / Subnet Mask

Remote Address Type

IP Address

PrefixLen / Subnet Mask

Action

Negotiation Mode

Encapsulation Mode

Outgoing Interface

Peer's IP Address

My Identifier

Peer's Identifier

ESP Algorithm

AH Algorithm

Pre-Shared Key

Phase 1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

SA Life Time

Key Group

Phase 1

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

SA Life Time sec min hour

Key Group

hase 2

Phase 2

Encapsulation Tunnel

Active Protocol ESP

Encryption Algorithm Encrypt and Authenticate (DES, MD5) ▾

SA Life Time

Perfect Forward Secrecy(PFS)

Back

Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)
Encrypt and Authenticate (AES, MD5)
Encrypt and Authenticate (AES, SHA1)
Encrypt only (DES)
Encrypt only (3DES)
Encrypt only (AES)
Authenticate only (MD5)
Authenticate only (SHA1)

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 ▾

None
DH1
DH2
DH5

Back Apply

DFL-1100/700/200

Удаленный межсетевой экран:

1- Разрешить весь трафик VPN (**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.



2- Включить IPSec и отредактировать политику IPSec (**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:

D-Link corporation

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	DES	MD5	0	28800
#2:	DES	MD5	0	28800
#3:	3DES	MD5	0	28800
#4:	CAST-128	SHA-1	0	28800
#5:	Blowfish-40 Allowed: 40-448	MD5	0	28800
#6:	Blowfish-128 Allowed: 40-448	MD5	0	28800
#7:	Blowfish-256 Allowed: 40-448	SHA-1	0	28800
#8:	Blowfish-128 Allowed: 128-448	MD5	0	28800
#9:	Blowfish-256 Allowed: 128-448	MD5	0	28800
#10:	Blowfish-256 Allowed: 256-448	MD5	0	28800
#11:	Blowfish-448 Allowed: 256-448	MD5	0	0
#12:	.	MD5	0	0

IPsec Proposal List

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

D-Link corporation

Локальный межсетевой экран:

01-Разрешить весь трафик VPN (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

2- Включить IPSec и отредактировать политику IPSec (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:

D-Link corporation

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	DES	MD5	0	28800
#2:	DES	MD5	0	28800
	3DES			
#3:	CAST-128	SHA-1	0	28800
	.			
#4:	Blowfish-40 Allowed:40-448	MD5	0	28800
	Blowfish-128 Allowed:40-448			
#5:	Blowfish-256 Allowed:40-448	SHA-1	0	28800
	Blowfish-128 Allowed:128-448			
#6:	Blowfish-256 Allowed:128-448	MD5	0	28800
	Blowfish-256 Allowed:256-448			
#7:	Blowfish-448 Allowed:256-448	MD5	0	0
	Blowfish-448 Allowed:448-448			
#8:	.	MD5	0	0
	Twofish-128 Allowed:128-256			
	Twofish-256 Allowed:128-256			
	Twofish-256 Allowed:256-256			
IPsec				
	AES-128 Allowed:128-256	HMAC	Life KB	Life Sec
	AES-256 Allowed:128-256	MD5	0	3600
#1:	AES-256 Allowed:256-256			

IPsec Proposal List

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

This unit will propose 128 bit encryption to the remote peer. This unit will accept any cipher key sizes between 128 and 256 bits.



DFL-600

Удаленный межсетевой экран:

- 1- Разрешить весь трафик VPN (**Advanced -> Policy -> Global Policy Status**)

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

Inbound Port Filter

Outbound Port Filter

<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
<input checked="" type="radio"/> Allow all except policy settings	<input checked="" type="radio"/> Allow all except policy settings
<input type="radio"/> Deny all except policy settings	<input type="radio"/> Deny all except policy settings

- 2- Включить IPSec и отредактировать политику IPSec (**Advanced -> VPN-IPSec -> Tunnel Settings**)

[IPSec Settings](#) / [Manual Key](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

Add/New Tunnel

Tunnel Name	<input type="text" value="ipsec"/>
Peer Tunnel Type	<input type="text" value="Static IP address"/> ▾
Termination IP	<input type="text" value="61.219.68.13"/>
DomainName	<input type="text"/>
Peer ID Type	<input type="text" value="Address(IPV4_Addr)"/> ▾
Peer ID	<input type="text" value="61.219.68.13"/> (optional)
Shared Key	<input type="text" value="1234567890"/>
IKE Mode	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
Encapsulation	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport mode
NAT traversal	<input checked="" type="radio"/> Normal <input type="radio"/> ESP Over UDP (port 500)
IPSec Operation	<input type="text" value="ESP"/> ▾

Phase 1 Proposal

Name	<input type="text" value="P1Param"/>
DH Group	<input type="text" value="Group 2"/> ▾
IKE Life Duration	<input type="text" value="6000"/> seconds
IKE Encryption	<input type="text" value="DES"/> ▾
IKE Hash	<input type="text" value="MD5"/> ▾

D-Link corporation

Phase 2 Proposal

Name	<input type="text" value="P2Param"/>
PFS Mode	<input type="text" value="Group 1"/>
Encapsulation	<input type="text" value="ESP"/>
IPSec Life Duration	<input type="text" value="6000"/> seconds
ESP Transform	<input type="text" value="DES"/>
ESP Auth	<input type="text" value="HMAC-MD5"/>
AH Transform	<input type="text" value="MD5"/>

[Click here to add P1 proposal](#)

P1 Proposals	<input type="text" value="P1Param"/>	<input type="text" value="NOT_SET"/>
	<input type="text" value="NOT_SET"/>	<input type="text" value="NOT_SET"/>

[Click here to add P2 proposal](#)

P2 Proposals	<input type="text" value="P2Param"/>	<input type="text" value="NOT_SET"/>
	<input type="text" value="NOT_SET"/>	<input type="text" value="NOT_SET"/>

Target Host Range

Starting Target Host	<input type="text" value="10.10.99.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

D-Link corporation

Локальный межсетевой экран:

- 1- Разрешить весь трафик VPN (**Advanced -> Policy -> Global Policy Status**)

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

Inbound Port Filter

Outbound Port Filter

<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
<input checked="" type="radio"/> Allow all except policy settings	<input checked="" type="radio"/> Allow all except policy settings
<input type="radio"/> Deny all except policy settings	<input type="radio"/> Deny all except policy settings

- 2- Включить IPSec и отредактировать политику IPSec (**Advanced -> VPN-IPSec -> Tunnel Settings**)

[IPSec Settings](#) / [Manual Key](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

Add/New Tunnel

Tunnel Name	<input type="text" value="Remote Gateway"/>
Peer Tunnel Type	<input type="text" value="Static IP address"/> ▼
Termination IP	<input type="text" value="61.219.68.14"/>
DomainName	<input type="text"/>
Peer ID Type	<input type="text" value="Address(IPV4_Addr)"/> ▼
Peer ID	<input type="text" value="61.219.68.14"/> (optional)
Shared Key	<input type="text" value="1234567890"/>
IKE Mode	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
Encapsulation	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport mode
NAT traversal	<input checked="" type="radio"/> Normal <input type="radio"/> ESP Over UDP (port 500)
IPSec Operation	<input type="text" value="ESP"/> ▼

Phase 1 Proposal

Name	<input type="text" value="P1Param"/>
DH Group	<input type="text" value="Group 2"/> ▼
IKE Life Duration	<input type="text" value="6000"/> seconds
IKE Encryption	<input type="text" value="DES"/> ▼
IKE Hash	<input type="text" value="MD5"/> ▼

D-Link corporation

Phase 2 Proposal

Name	<input type="text" value="P2Param"/>
PFS Mode	<input type="text" value="Group 1"/>
Encapsulation	<input type="text" value="ESP"/>
IPSec Life Duration	<input type="text" value="6000"/> seconds
ESP Transform	<input type="text" value="DES"/>
ESP Auth	<input type="text" value="HMAC-MD5"/>
AH Transform	<input type="text" value="MD5"/>

Click here to add P1 proposal

P1 Proposals	<input type="text" value="P1Param"/>	<input type="text" value="NOT_SET"/>
	<input type="text" value="NOT_SET"/>	<input type="text" value="NOT_SET"/>

Click here to add P2 proposal

P2 Proposals	<input type="text" value="P2Param"/>	<input type="text" value="NOT_SET"/>
	<input type="text" value="NOT_SET"/>	<input type="text" value="NOT_SET"/>

Target Host Range

Starting Target Host	<input type="text" value="192.168.1.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>