

**D-Link VPN Application**  
**Руководство по быстрой установке**

## **Содержание**

<b>1. Удаленный доступ</b>	<b>3</b>
1-1 Цель:	3
1-2 Окружение:	3
1-3 Настройка	3
1-3-1 Сервер PPTP	3
DFL-1500	4
DFL-1100/700/200	4
DFL-600	5
Настройка клиента PPTP (VPN-адаптер ОС Microsoft XP PRO)	6
1-3-2 L2TP без IPSec	10
1-3-3 IPSec	10
DFL-1500/900	11
DFL-1100/700/200	15
DFL-600	18
Настройка подключения IPSec (D-Link DS-601)	20
<b>2. Туннель между двумя сетями (LAN to LAN).</b>	<b>28</b>
2-1 Цель:	28
2-2 Окружение:	28
2-3 Параметры настройки:	28
2-3-1 Сервер PPTP и клиент PPTP	28
DFL-1500	29
DFL-1100/700/200	30
2-3-2 Сервер L2TP и клиент L2TP	31
2-3-3 IPSec	31
DFL-1500	32
DFL-1100/700/200	39
DFL-600	45

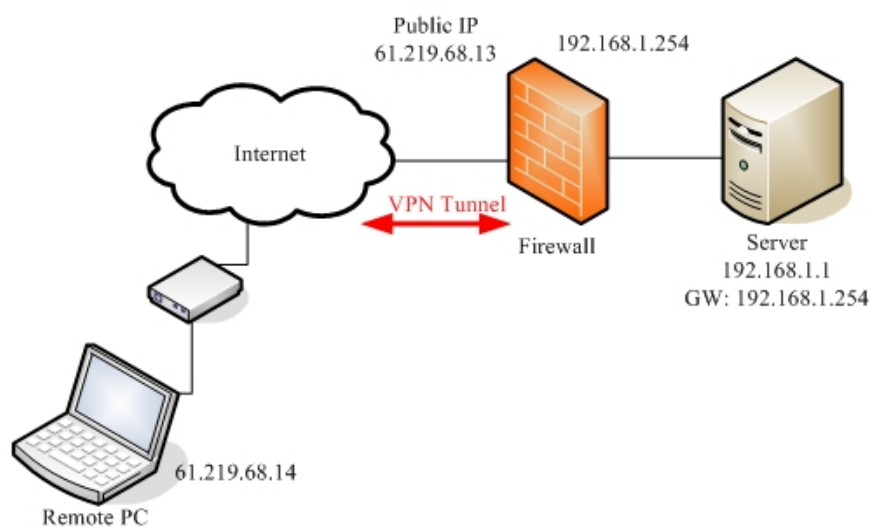
## 1. Удаленный доступ

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

## D-Link corporation

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>	<b>PPTP</b>	<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**)

## D-Link corporation

### 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="192.168.1.100 - 192.168.1.105"/>
	<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)

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"/>

## D-Link corporation

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

Шаг1

Выберите “Новое подключение” для того, чтобы создать исходящее подключение VPN-PPTP.



Шаг2

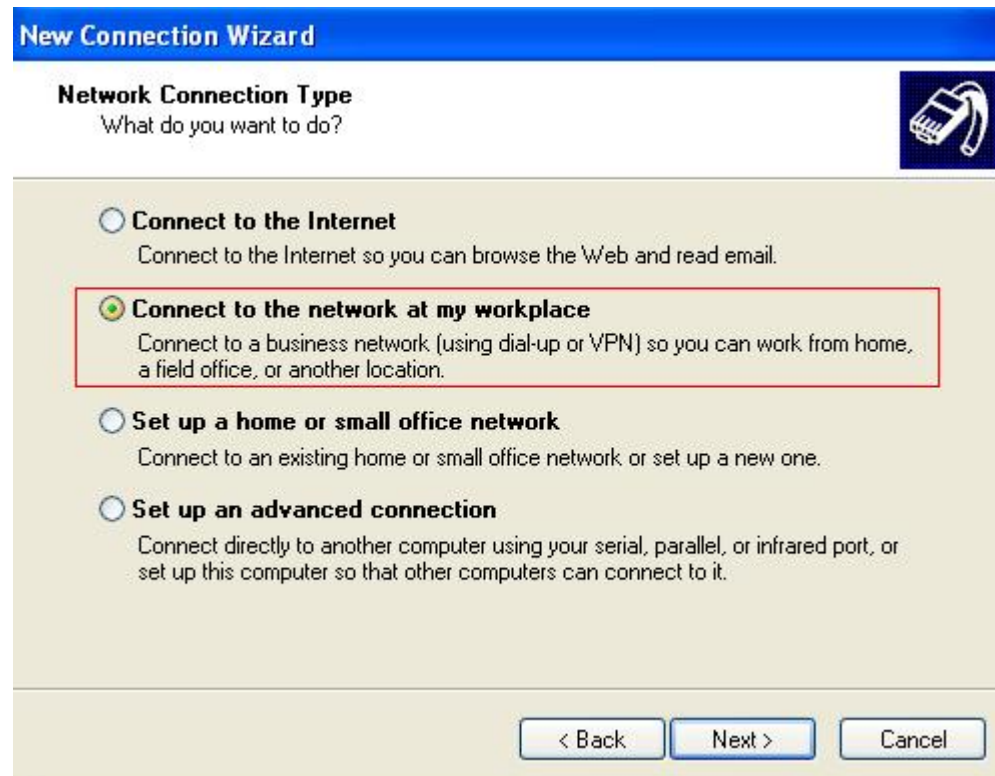
Нажмите **Next** для перехода на следующий шаг.



## D-Link corporation

Шаг3

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

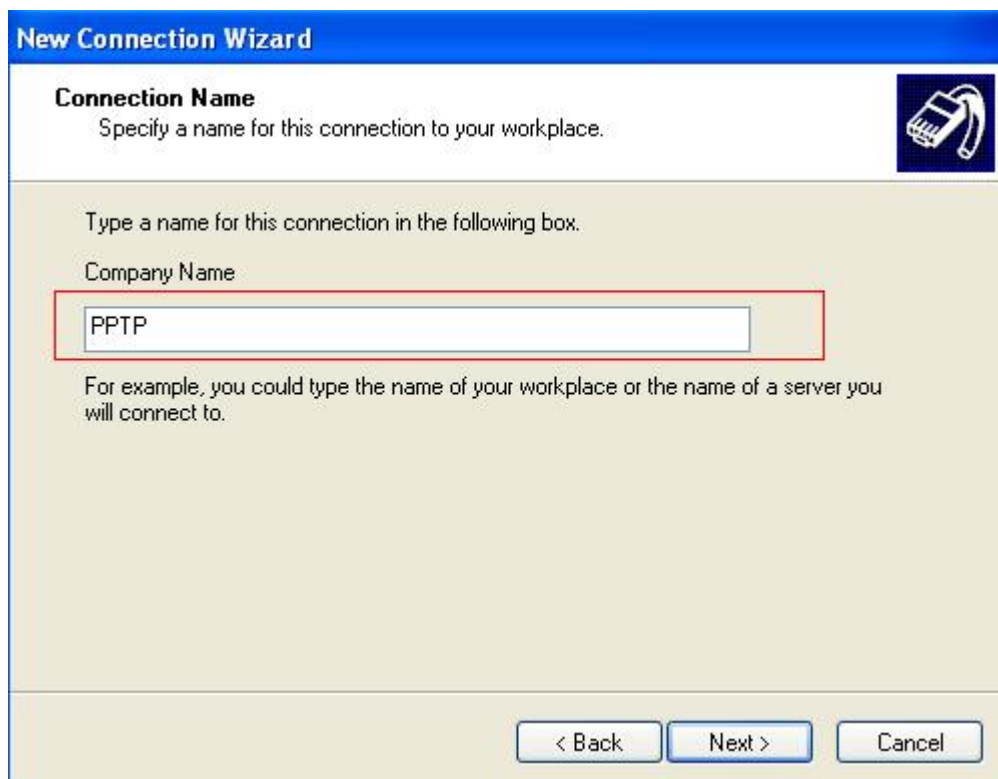
Шаг4

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



Ша5

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



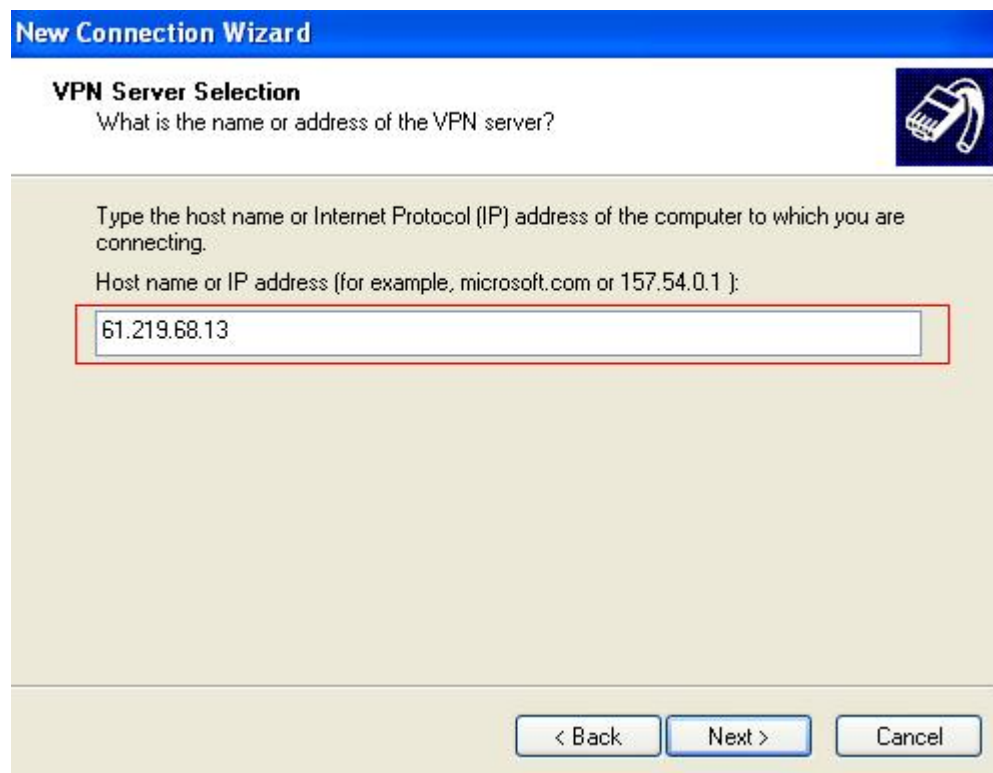
Ша6

Введите IP-адрес сервера VPN-PPTP: 61.219.68.13. Нажмите **Next** для перехода на



## D-Link corporation

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

Шаг8

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



### 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:
07- Группа ключей IPSec: DH1	61.219.68.14

**D-Link corporation**

08- Режим согласования: Main	07- PSK: 1234567890
09- Локальный идентификатор: IP address	08- Политика IKE: DES+MD5
10- Идентификатор ID: 61.219.68.14	09- Группа ключей IKE: DH2
11- PSK: 1234567890	10- Политика IPsec: DES+MD5 (ESP)
12- Удаленные сети: 192.168.1.0/24	11- Группа ключей IPsec: DH1
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

Back Apply

LAN1:

**D-Link corporation**

Address | Service | Schedule |

[Objects] [Groups]

Address-> Objects -> Edit

**Edit Address object number 1**

**Name**

Address name:

**Value**

Address Type:

Subnet      IP:       Mask:

Range      Start IP:       End IP:

Host      IP:

02- Отредактировать правила межсетевого экрана (**Advanced Settings -> Firewall -> Edit Rules**)

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

Firewall->Edit Rules

Edit  to  rules

Default action for this packet direction:   Log

Packets are top-down matched by the rules.

Item	Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	
<input checked="" type="radio"/>	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block

           1

               1

**D-Link corporation**

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:

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

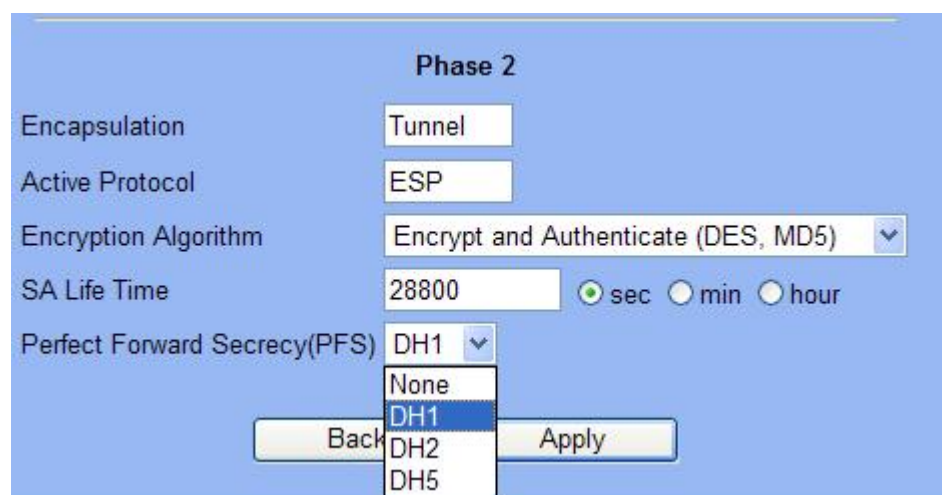
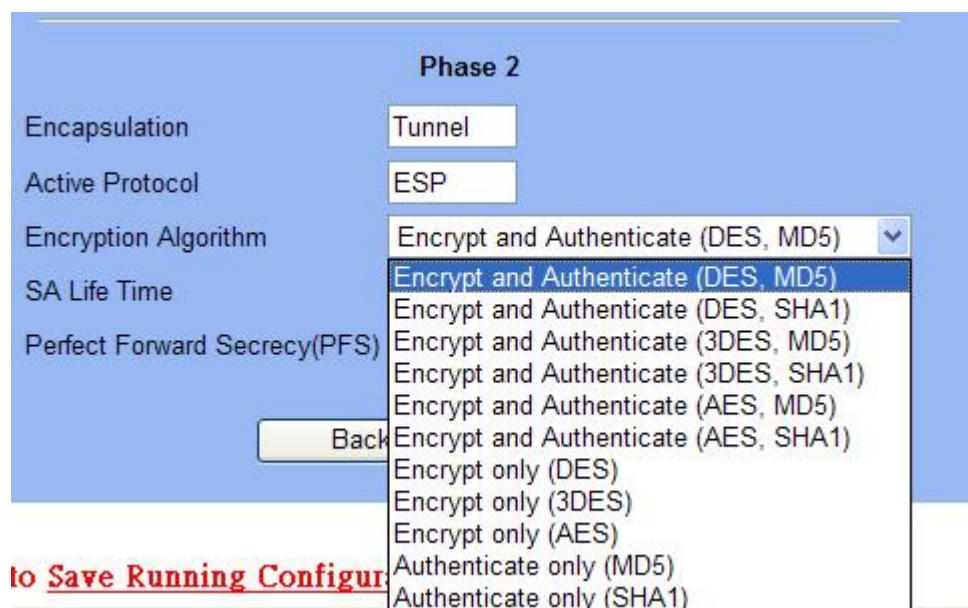
Pre-Shared Key

Encryption Algorithm

SA Life Time   sec  min  hour

Key Group

hase 2



DFL-1100/700/200

01- Разрешить весь трафик VPN (Firewall -> Policy)

## D-Link corporation

### 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- 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:

Tunnel type:

**Roaming Users** - single-host IPsec clients

IKE XAuth:  Require user authentication via IKE XAuth to open tunnel.



## D-Link corporation

### 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:	<input type="text" value="DES"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#2:	<input type="text" value="DES"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#3:	<input type="text" value="CAST-128"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#4:	<input type="text" value="Blowfish-40 Allowed:40-448"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#5:	<input type="text" value="Blowfish-128 Allowed:128-448"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#6:	<input type="text" value="Blowfish-256 Allowed:256-448"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#7:	<input type="text" value="Blowfish-448 Allowed:256-448"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
#8:	<input type="text" value="."/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

## D-Link corporation

### 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:	-	MD5	0	3600
#6:	Blowfish-40 Allowed: 40-448	SHA-1	0	3600
#7:	Blowfish-128 Allowed: 40-448	MD5	0	3600
#8:	Blowfish-256 Allowed: 40-448	SHA-1	0	3600
#9:	Blowfish-128 Allowed: 128-448	MD5	0	3600
#10:	Blowfish-256 Allowed: 128-448	MD5	0	3600
#11:	Blowfish-256 Allowed: 256-448	MD5	0	0
#12:	Blowfish-448 Allowed: 256-448	MD5	0	0
#13:	-	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**)

**D-Link corporation**

[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"/> ▼

**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="61.219.68.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

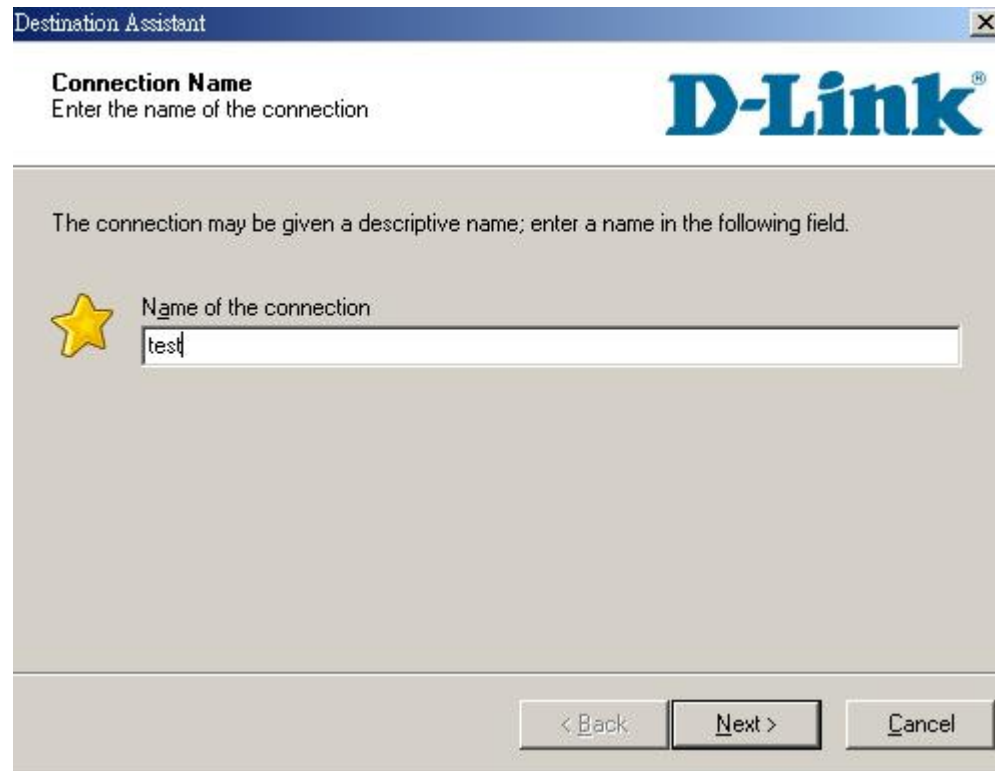
## **D-Link corporation**

Настройка подключения IPSec (D-Link DS-601)

Шаг1

Configuration->Profile settings->New Entry

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



The screenshot shows a window titled "Destination Assistant" with a close button in the top right corner. Below the title bar, the text "Connection Name" is displayed in bold, followed by the instruction "Enter the name of the connection". To the right of this text is the D-Link logo. Below the instruction, a message states: "The connection may be given a descriptive name; enter a name in the following field." To the left of the input field is a yellow star icon. The input field is labeled "Name of the connection" and contains the text "test". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Шаг2

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

## D-Link corporation

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)

< Back   Next   Cancel

Шаг3

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

Destination Assistant

**VPN gateway parameters**  
To which VPN gateway should the connection be established?

**D-Link®**

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)

< Back   Next   Cancel

Шаг4

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**.

## D-Link corporation

The screenshot shows the 'Destination Assistant' dialog box with the 'Pre-shared key' tab selected. The D-Link logo is in the top right. Below the title, there is explanatory text: 'A shared secret or pre-shared key is used to encrypt the connection; this then needs to be indentially 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' section has a key icon and two input fields: 'Shared secret' and 'Confirm secret', both containing masked characters. The 'Local identity' section has a person icon, a 'Type' dropdown menu set to 'IP Address', and an 'ID' input field containing '61.219.68.14'. At the bottom are buttons for '< Back', 'Finish', and 'Cancel'.

### Ша5

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

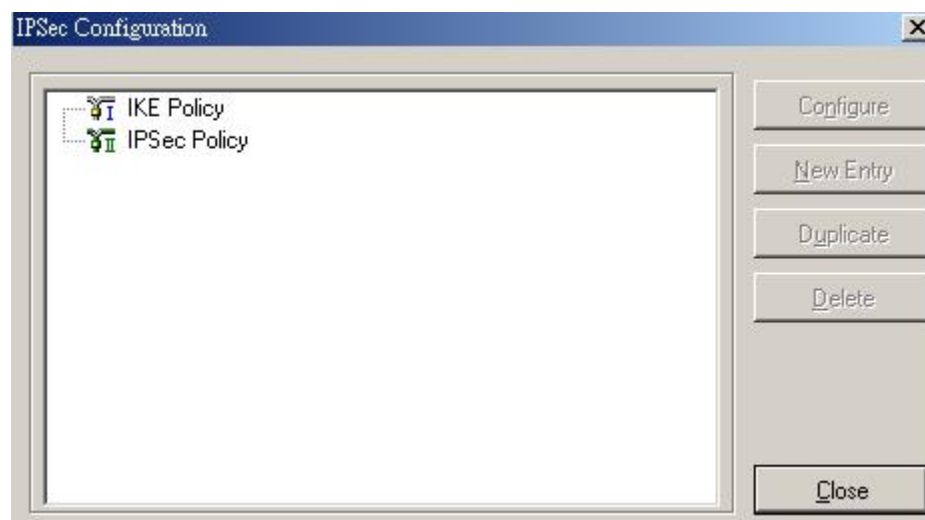
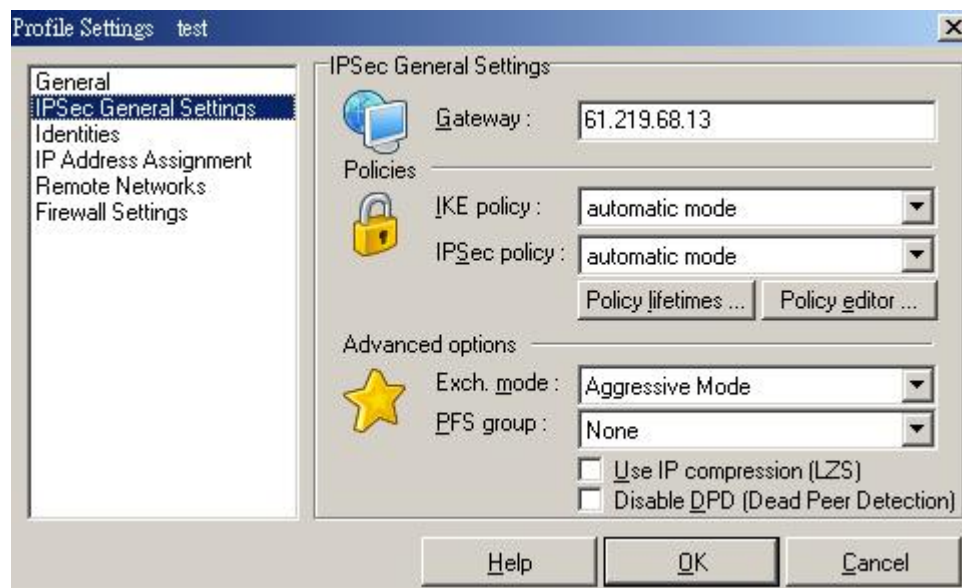
The screenshot shows the 'Profile Settings' dialog box. It features a table of 'Available Profiles' with two columns: 'Profile Names' and 'Phone Number/Link Type'. The 'test' profile is selected. To the right of the table are buttons for 'Configure', 'New Entry', 'Duplicate', 'Delete', 'Help', 'Cancel', and 'OK'.

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

### Ша6

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

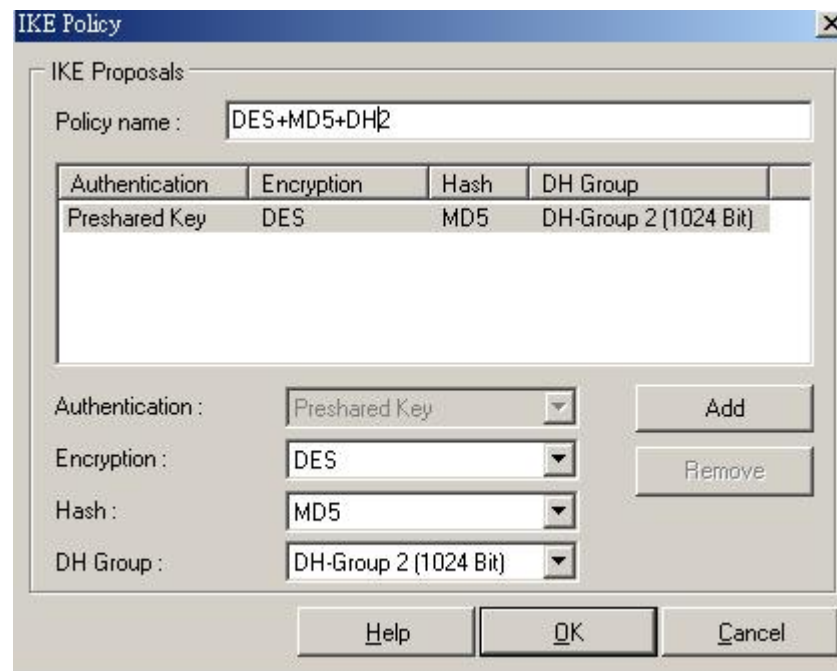
Нажмите кнопку **Policy editor**, чтобы отредактировать политики IPSec и IKE.



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**.



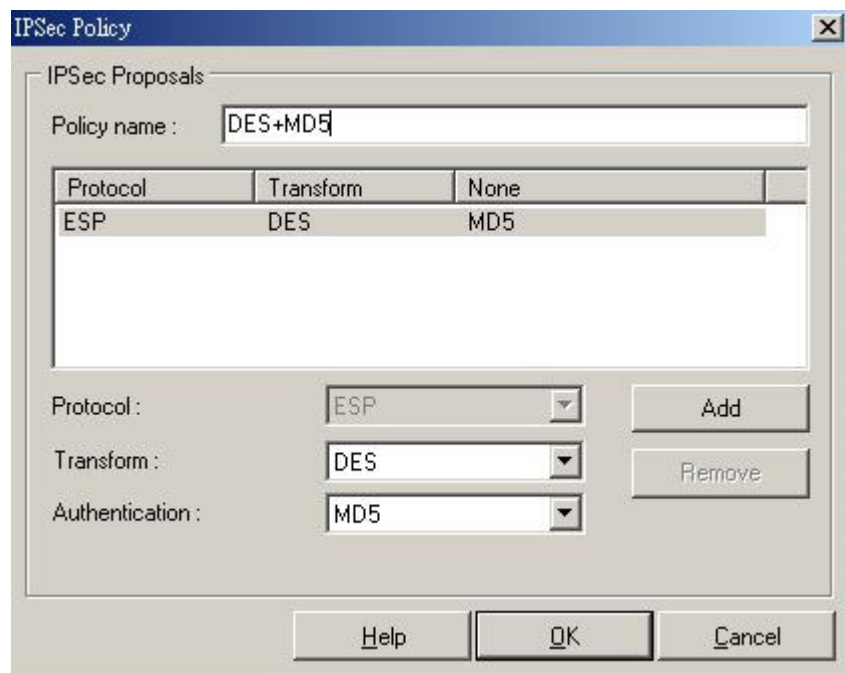
Ша8

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.



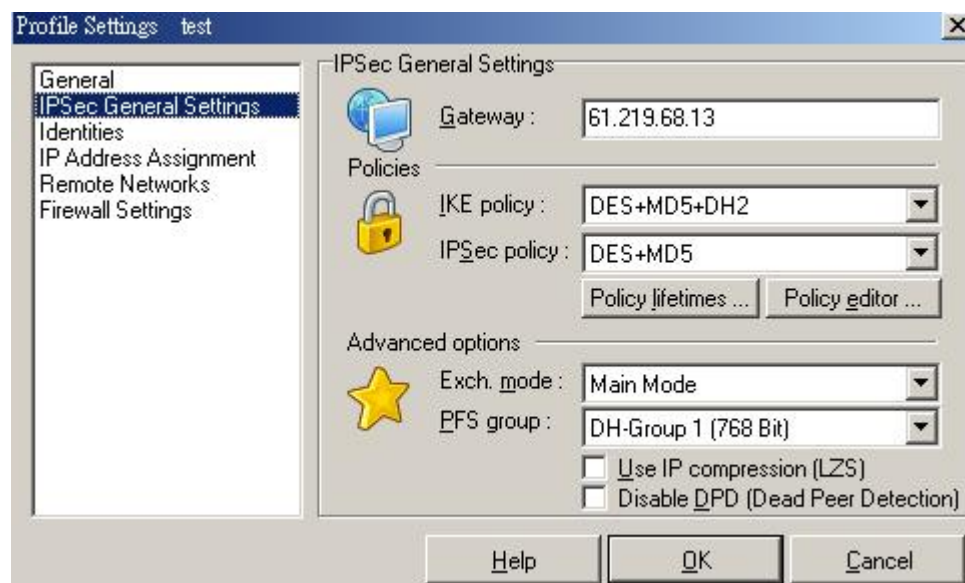
## D-Link corporation



Ша9

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**

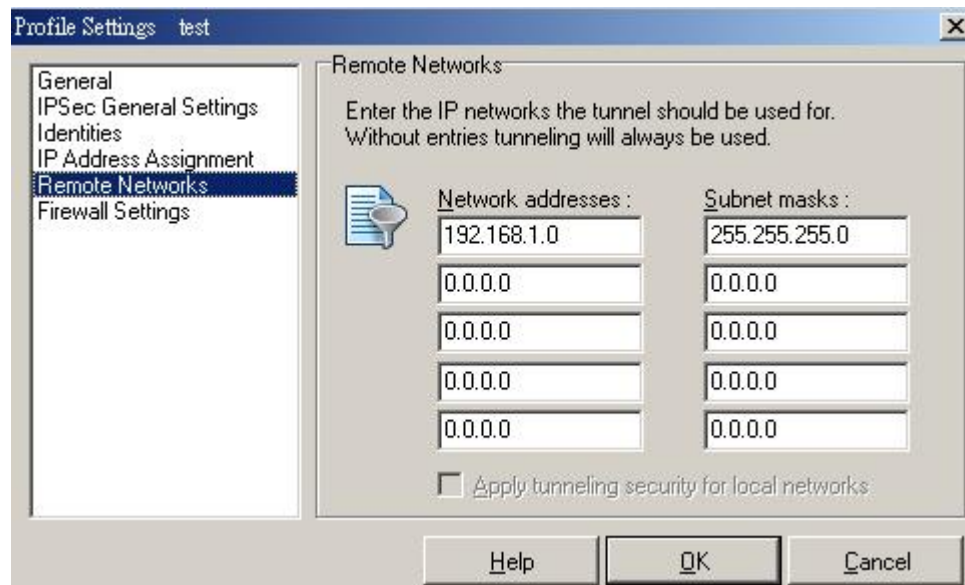


Ша10

Настройте параметры удаленных сетей в меню **Remote Networks**, введите адрес сети

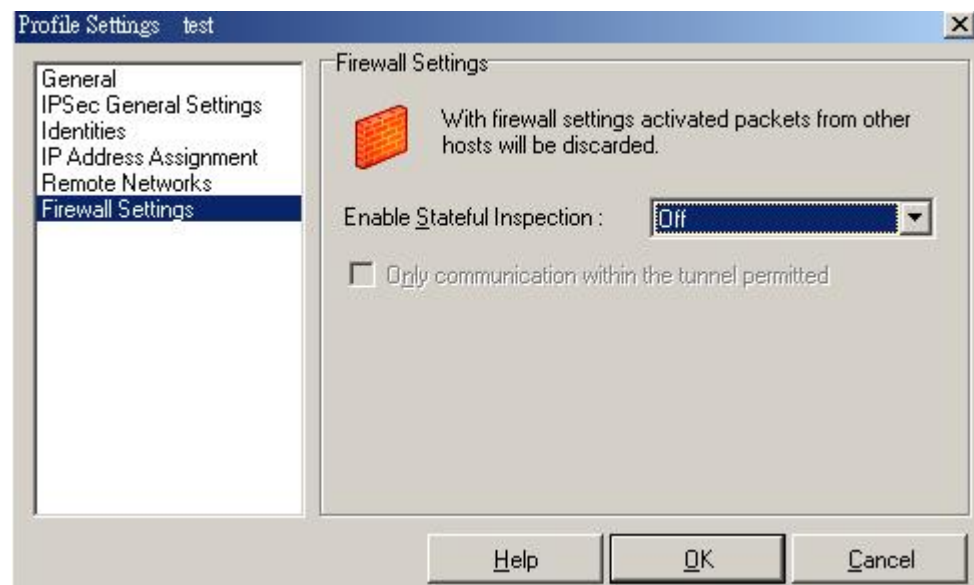
## D-Link corporation

192.168.10.1 в поле **Network address** и маску подсети 255.255.255.0 в поле **Subnet masks**.



Щар11

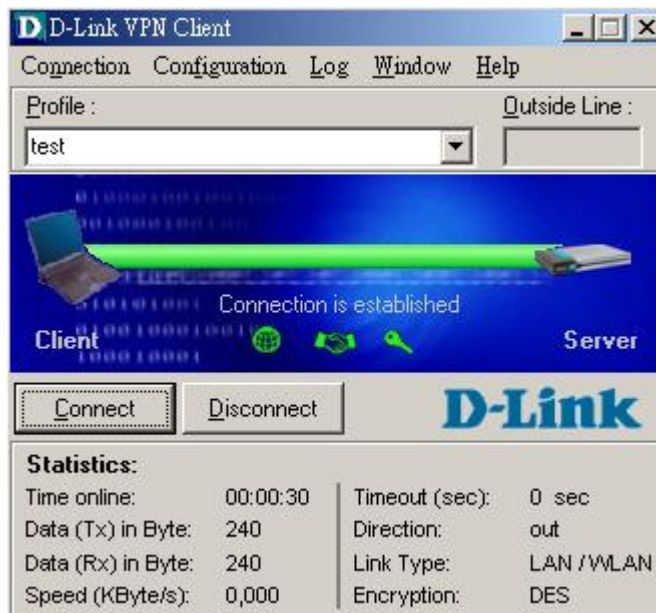
Настройте параметры межсетевых экранов в меню Firewall settings, выберите Off в поле **Enable Stateful Inspection** и нажмите кнопку **OK**.



## D-Link corporation

Шар12

Нажмите кнопку **Connect** для установления туннеля IPSec



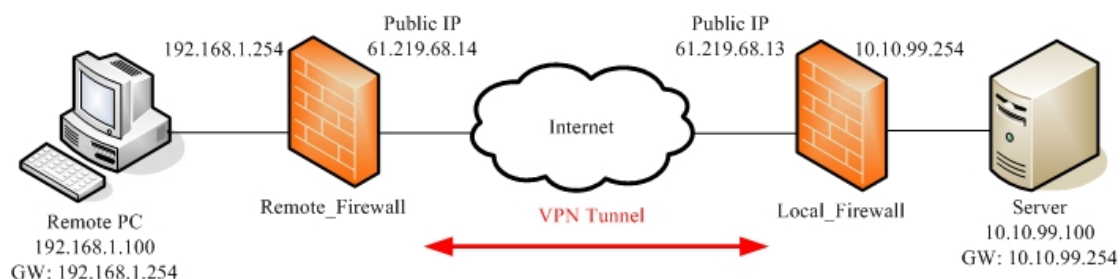
## 2. Туннель между двумя сетями (LAN to LAN).

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
01- Включить клиент PPTP	01- Включить сервер PPTP
02- IP-адрес сервера: 61.219.68.13	02- Локальный IP-адрес: 10.10.99.254
03- Имя пользователя: firewall	03- Диапазон IP-адресов: 10.10.99.200-205
04- Пароль: firewall	04- Имя пользователя: firewall
	05- Пароль: firewall

**D-Link corporation**

DFL-1500

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

The screenshot shows the PPTP configuration page. At the top, there are tabs for IPsec, VPN Hub, VPN Spoke, PPTP (selected), L2TP, and Pass Through. A checkbox labeled 'Enable PPTP Server' is checked. Below this, there are two radio buttons: '[Server]' (selected) and '[Client]'. The configuration fields include: Local IP: 10.10.99.254; Assigned IP Range: Start: 10.10.99.200, End: 10.10.99.205; Username: firewall; Password: [masked]. An 'Apply' button is at the bottom.

02- Включить клиент PPTP (**Advanced settings -> VPN settings -> PPTP -> Client**)

The screenshot shows the PPTP Client configuration page. At the top, there are tabs for IPsec, VPN Hub, VPN Spoke, PPTP (selected), L2TP, and Pass Through. A checkbox labeled 'Enable PPTP Client' is checked. Below this, there are two radio buttons: '[Server]' and '[Client]' (selected). The configuration fields include: Server IP: 61.219.68.13; Username: firewall; Password: [masked]; Assigned IP: 10.10.99.201. An 'Apply' button is at the bottom.

03- 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	-	-	-	-

## D-Link corporation

DFL-1100/700/200

01- 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"/>	

02- 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)

03- 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 Relayer 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
01- Включить IPSec	01- Включить IPSec
02- Локальный IP-адрес: 192.168.1.0/24	02- Локальный IP-адрес: 10.10.99.0/24
03- Удаленный IP-адрес: 10.10.99.0/24	03- Удаленный IP-адрес: 192.168.1.0/24
04- Режим согласования: Main mode	04- Режим согласования: Main mode
05- Режим инкапсуляции: Tunnel mode	05- Режим инкапсуляции: Tunnel mode
06- Конечный IP-адрес туннеля: 61.219.68.13	06- Конечный IP-адрес туннеля: 61.219.68.14
07- Ключ PSK: 1234567890	07- Ключ PSK: 1234567890
08- Политика IKE: DES+MD5	08- Политика IKE: DES+MD5
09- Группа ключей IKE: DH2	09- 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

**D-Link corporation**

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**)



## 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				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:

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](#)

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: Main

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800  sec  min  hour

Key Group: DH2

DH1  
DH2  
DH5

**Phase 2**

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800

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

Локальный межсетевой экран:

01- Добавить адреса (**Basic -> Books**)

**D-Link corporation**

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- Отредактировать правила межсетевого экрана (**Advanced Settings -> Firewall -> Edit Rules**)

## D-Link corporation

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		
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->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

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 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 Encrypt and Authenticate (DES, MD5)  
Encrypt and Authenticate (DES, SHA1)

Key Group 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

DH1

DH2

DH5

**Phase 2**

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800

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:

01- Разрешить весь трафик VPN (**Firewall -> Policy**)

## D-Link corporation

### 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- 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

Локальный межсетевой экран:

01-Разрешить весь трафик VPN (Firewall -> Policy)

## D-Link corporation

### 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- 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			
<b>IPsec</b>				
	AES-128 Allowed:128-256	<b>HMAC</b>	<b>Life KB</b>	<b>Life Sec</b>
	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-	.			
establi	AES-128 Allowed:128-256			
receiv	AES-256 Allowed:128-256			
	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:

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

## D-Link corporation

[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

02- 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"/> ▼

**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"/> ▼

**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

Локальный межсетевой экран:

01- 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

02- 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	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	<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	ESP

## D-Link corporation

### 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"/>

### 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"/>