

# D-Link VPN Application Руководство по быстрой установке

#### Содержание

1-1 Цель:	2
1-2 Окружение:	3
1-3 Настройка	3
2-1 Цель:	
2-2 Окружение:	
2-3 Параметры настройки:	
2-3-1 Сервер РРТР и клиент РРТР	

## 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 РРТР

Настройки удаленного ПК	Настройки межсетевого экрана
01-IР-адрес ПК: 61.219.68.13	01-Включить сервер РРТР
02-Тип VPN: РРТР	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>	VPN Hub	<u>VPN Spoke</u>	РРТР	<u>L2TP</u>	<u>Pass</u> <u>Through</u>	
	🔽 Enable PF	TP Server				
[Server] [ <u>Clic</u>	ent]		Local	ID: 192.168	1 254	
			LUCA	Assigned IP	Range	
		Star	r  192.168.1.1	100 En	d: 192.168.1.105	
		Username	; firewall	Pa	ssword: ********	
				Apply		

## DFL-1100/700/200

01- Добавить пользователя (Firewall -> Users)

i new us	er:		
	User name:	firewall	
19421174		r	
Grou	p membership:	I	
	Password:	*****	
Ret	ype password:	*****	

02- Включить сервер PPTP (Firewall -> VPN)

#### L2TP/PPTP Servers

Edit PPTP tunnel PPTP-Server:

Name:	PPTP-Server	
Outer IP:		Blank = WAN IP
	Must be WAN IF	if IPsec encryption is req
Inner IP:		Blank = LAN IP
Client IP Pool:	s. 192.168.1.100 -	192.168.1.105
	Proxy ARP	dynamically added routes
Primary DNS:	Proxy ARP	dynamically added routes
Primary DNS: Secondary DNS:	Proxy ABP	dynamically added routes (Optional) (Optional)
Primary DNS: Secondary DNS:	Proxy ARP	dynamically added routes (Optional) (Optional) wn DNS relayer addresses
Primary DNS: Secondary DNS: Primary WINS:	Proxy ARP	dynamically added routes (Optional) (Optional) wn DNS relayer addresses

## **DFL-600**

#### 01- Добавить пользователя (Advanced -> VPN-PPTP -> PPTP Account)

PPTP Settings /	PPTP Account / PPTP Status
Add/New User Ad	count
User Name	firewall
Password	*****
Confirm Password	****

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

PPTP Settings / PPTP Account / PPTP Status

PPTP Pass Through	🗖 Enable
PPTP Status	🗹 Enable
Starting IP address	192.168.1.100
Ending IP address	192.168.1.105

## Настройка клиента PPTP (VPNадаптер OC 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.



Шаг З

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.
<ul> <li>Set up a home or small office network</li> <li>Connect to an existing home or small office network or set up a new one.</li> <li>Set up an advanced connection</li> <li>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.</li> </ul>
< Back Next > Cancel

#### Шаг 4

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

How do you want to connect	to the network at your workplace?
Create the following connection	on:
O Dial-up connection	
Connect using a modem a Network (ISDN) phone lin	and a regular phone line or an Integrated Services Digital ie.
Virtual Private Networ	k connection
Connect to the network us Internet.	sing a virtual private network (VPN) connection over the
Connect to the network u Internet.	sing a virtual private network (VPN) connection over the
Connect to the network u Internet.	sing a virtual private network (VPN) connection over the
Connect to the network u Internet.	sing a virtual private network (VPN) connection over the
Connect to the network u Internet.	sing a virtual private network (VPN) connection over the

#### Шаг 5

Введите имя подключения РРТР. 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.
<pre></pre>

Шаг 6

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

<b>N</b> Serve	Selection			
What is t	he name or address of the VI	PN server?		8
Type the	host name or Internet Protoc	ol (IP) address of t	ne computer to wi	nich you are
Host nam	e or IP address (for example.	, microsoft.com or 1	57.54.0.1 ):	
61.219.6	8.13			
	20 - 130 AX			
		C & Back	Nevt	Carr

Шаг 7

Нажмите Готово для завершения настройки параметров VPN-PPTP.



Шаг 8

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

Connect PPT	p	? 🔀
		X
User name:	firewall	
Password:	•••••	
Save this u	iser name and password for the following who uses this computer	users:
Connect		Trop

## 1-3-2 L2TP без IPSec

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
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 <u>Service</u> <u>Sc</u>	hedule			
[Objects] [Groups]				
Address-> Objects -> Edit				
	Edit Ad	dress object numb	or 1	
Name	Luit Au	aress object numb		
	Address name: Remote			
Value				
Address Type:				
<ul> <li>Subnet</li> </ul>	: 61.219.68.0 Ma	ask: 255.255.255.0		
○ Range Start IP	: 0.0.0.0 End	d IP: 255.255.255.25	55	
⊖Host IP	0.0.0			
	Back	C Apply		
LAN1:				
Address <u>Service</u>	Schedule			
[Objects] [Groups]				
· · · · · · · · · · · · · · · · · · ·				
Address-> Objects -	> Edit			
		Edit Address	s object number 1	
Name		Curchadros	o object namber 1	
	Address name	e: LAN1		
Value				
Address Type:				
Subnet	IP: 192.168.1.0	Mask:	255.255.255.0	
O Range S	tart IP: 0.0.0.0	End IP:	255.255.255.255	
Ollast	ID.0.0.0.0			
Onost	0.0.0.0			
		<i>c</i>		
		Back	Apply	

02- Отредактировать правила межсетевого экрана (Advanced Settings -> Firewall ->

Edit Rules <u>Status</u>	S) Edit Rule	s <u>Show Ru</u>	iles Attack	<u>k Alert</u> Sum	imary		
Firewa	III->Edit Rule	s					
Edit	WAN1 🚩 to	LAN1 🗸	rules				
Defau Packets are	It action for t	his packet di	rection: BI	lock 🝸 🔽	Log Apply		
Item	S	tatus			Conc	lition	
#	Name	Schedule	S	ource IP	Dest. IP	Service	Action
0 1	Default	ALWAYS	W.	AN1_ALL	LAN1_ALL	ALL_SERVICE	Block
		Inser	Prev. Pag t	e Nex Edit	t Page Mor Delete	re Page 1 💌 Move Before: 1 🛩	
Firewall->E	dit Rules->Ir	nsert					
T WOWLIN ? E		iour					
			Insert a	new WAN1	-to-LAN1 Firewa	ill rule	
	Status	la name D	ulat				
	Rui	le name: R	uiei	e de la companya de l			
	Condition	chedule: A	dways 🚩				
	Secondition	ource IP: R	emote		Des	t. IP: LAN1	~
		Service: A	NY	~			
	Action						
	Fo	rward 🔽 ar	nd log	Y the r	natched session		
		For	ward ban	dwidth clas	s: def_class 💌		
		Re	verse ban	dwidth clas	s: def_class 👻		
					1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
				Back	Apply		

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

#### Settings)

IPSec	VPN Hub	VPN Spoke	<u>PPTP</u>	L2TP	Pass Through
	Enable IP	Sec Apply			

IPSec->IKE->Edit	Rule			
		Sta	tus	
		<b>∠</b> A	ctive	
		IKE Rule Name ipsec		
		Cond	lition	
		Local Address Type	Subnet Address 💌	
		IP Address	192.168.1.0	
		PrefixLen / Subnet Mas	k 255.255.255.0	
		Remote Address Type	Single Address 👻	
		IP Address	61.219.68.14	
		PrefixLen / Subnet Mas	k 255.255.255.255	
		Action		
	N	Vegotiation Mode	in 🗸	
	F	Encapsulation Mode Tu	nnel 🗸	
	Outgoing In	iterface VVAN1 🗠		-ie
	Peer's IP A	ddress Static IP	61.219.68.14	
Му	/ Identifier	IP Address	Auto_Assigned	
Pe	er's Identifier	IP Address	Auto_Assigned	
(	ESP Algorit	thm Encrypt and Authe	nticate (DES, MD5)	~
(		thm Authenticate (MD5		
	Jan Algoni	unin runomodio (m2 s		
	Pre-Shar	red Key 1234567890		
	i ic-ollar	1234307030		
		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)

	F	Phase	1
Negotiation Mode	Main		
Pre-Shared Key	123456	7890	
Encryption Algorithm	Encrypt	t and A	uthenticate (DES, MD5)
SA Life Time	28800		⊙sec ○min ○hour
Key Group	DH2 💙		
	DH1		
	DH2	hase	)

	Phase 2
Encapsulation	Tunnel
Active Protocol	ESP
Encryption Algorithm	Encrypt and Authenticate (DES, MD5)
SA Life Time Perfect Forward Secrecy(PFS)	Encrypt and Authenticate (DES, MD5) Encrypt and Authenticate (DES, SHA1) Encrypt and Authenticate (3DES, MD5) Encrypt and Authenticate (3DES, SHA1)
Bac	Encrypt and Authenticate (SDES, SHAT) Encrypt and Authenticate (AES, MD5) Encrypt and Authenticate (AES, SHA1) Encrypt only (DES)
lo <u>Save Running Configu</u>	Encrypt only (AES) Authenticate only (MD5) Authenticate only (SHA1)

	Phase 2	
Encapsulation	Tunnel	
Active Protocol	ESP	
Encryption Algorithm	Encrypt and	Authenticate (DES, MD5)
SA Life Time	28800	osec Omin Ohour
Perfect Forward Secrecy(PFS)	DH1 💌	
	None	
Back	DH1 DH2	Apply
	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:	3		
VPN:	Allow all VPN traffic: internal->VPN, VPN->internal and VPN->	VPN.	
	<b>S</b>	8	0
	Apply	Cancel	Help

02- Включить IPSec и отредактировать политику IPSec (**Firewall -> VPN -> IPSec Tunnels**)

#### **VPN Tunnels**

Edit IPsec tunnel ipsec:

Trans. Three	
Local Net: 192.168.1.0/24	

Authentication:

•	PSK ·	Pre-Shared Key	
---	-------	----------------	--

PSK:	*****	1024567000
Retype PSK:	****	1254507850

#### C Certificate-based

C		100
Certificates:		
	Use ctrl/shift click to select multiple certificates. To use ID lists below, you must select a CA certificate.	
	No. 1	Lange Street

Tunnel type:

Roaming Users - single-host IPsec clients

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

#### **VPN Tunnels**

Edit advanced settings of IPsec tunnel ipsec:

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

#### IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1	DES	MD5 💽	0	28800
#2	DES A	MD5 -	0	28800
#3:	CAST-128	SHA-1 💌	0	28800
#4:	Blowfish-40 Allowed: 40-448 Blowfish-128 Allowed: 40-448	MD5 💌	0	28800
#5:	Blowfish-256 Allowed: 40-448 Blowfish-128 Allowed: 128-448	SHA-1 💌	0	28800
#6:	Blowfish-256 Allowed:128-448 Blowfish-256 Allowed:256-448	MD5 💽	0	28800
#7:	Blowfish-448 Allowed:256-448	MD5 🖃	0	0
#8:	· •	MD5 💽	0	0

#### **IPsec Proposal List**

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

## **DFL-600**

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

Policy Rules / Global Policy Status / Policies

Inbound Port Filter	Outbound Port Filter
Enabled	Enabled
<ul> <li>Allow all except policy settings</li> </ul>	<ul> <li>Allow all except policy settings</li> </ul>
O Deny all except policy settings	O Deny all except policy settings

#### 02- Включить IPSec и отредактировать политику IPSec (Firewall -> VPN -> IPSec

#### Tunnels)

IPSec Settings /	Manual Key / Tuni	nel Settings / <u>Tunnel Table</u> / <u>IPSec</u>
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	O Aggressive
Encapsulation	Tunnel	Transport mode
NAT traversal	Normal	ESP Over UDP (port 500)
IPSec Operation	ESP 💌	
Phase 1 Proposa	I to a to	
Name	P1Param	
DH Group	Group 2 💌	
IKE Life Duration	6000	seconds
IKE Encryption	DES 💌	
IKE Hash	MD5 🛩	

Phase 2 Propos	sal	
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 ac	ld P1 proposal	
P1 Proposals	P1Param 🚩	NOT_SET 🚩
	NOT_SET 🔽	NOT_SET 🔽
Click here to ac	ld P2 proposal	
P2 Proposals	P2Param 🚩	NOT_SET 👻
	NOT_SET 💌	NOT_SET 💌
Target Host Rar	nge	
Starting Target Host	61.219.68.0	
Subnet Mask	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

onnection Name		D.T Stal	
nter the name of the connection			1
he connection may be given a descriptiv	e name; enter a nam	ne in the following field.	
A Name of the connection			
test			

Шаг 2

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

estination Assistant	×
Link type (Dial up configuration) Select the media type of the connection.	<b>D-Link</b>
Determine how the connection to the corporate n to be used via modem, set the communication me appropriate modem.	etwork should be established. If the internet is dia to "modem" and then select the
Communication media :	over IP)
	< <u>B</u> ack <u>N</u> ext <u>C</u> ancel

Шаг 3

Введите адрес шлюза VPN (61.219.68.13) и нажмите кнопку Next

<b>VPN g</b> Towhic	ateway parameters ch VPN gateway should the conne	ection be established?	ink
Enter th the VPI	ie DNS name (i.e. vpnserver.dom/ Ngateway you want to connect to	ain.com) or the official IP address (i.e. 3	212.10.17.29) of
	Gateway		
3	61.219.68.13		
	Use extended authenticatio	n (XAUTH)	
88	Username		
	Password	Password (Confirm)	
	1	J	

#### 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.

Common	i secret for data encryption	D-Li	mk.
A shared indentica Enter the	J secret or pre-shared key is used to ally on both sides (VPN client und V e appropriate value for the IKE ID a Pre-shared key	/ encrypt the connection; this then need PN gateway). ccording to the selected ID type.	ls to be
0			
8	Local identity Iype : IP Address		<u>_</u>
	ID: 61.219.68.14		
	ID .  01.213.00.14	< Back	Finish

Шаг 5

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

Profile Names	Phone Number/Link Type	Configure
DFL-300	LAN 🔺	
DFL-500 (PPPoE)	xDSL (PPPoE)	New Entry
DFL-500	LAN	
DFL-700 [Modem]	<phonenumber></phonenumber>	D <u>u</u> plicate
DFL-700	LAN	
DFL-80	LAN	<u>D</u> elete
DFL-900	LAN	
DI-804hv [PPPoE]	xDSL (PPPoE)	<u>H</u> elp
DI-804hv	LAN	
DI-824vup+	LAN	<u>C</u> ancel
test	LAN	
		I <u>О</u> К

#### Шаг 6

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

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

rofile Settings test				×
General IPSec General Settings Identities	-IPSec Ge	neral Settings <u>G</u> ateway :	61.219.68.13	
IP Address Assignment Remote Networks Firewall Settings	Policies	<u>I</u> KE policy : IP <u>S</u> ec policy :	automatic mode	• •
	Advance	ed options	Policy lifetimes	Policy editor
	2	Exch. <u>m</u> ode : <u>P</u> FS group :	Aggressive Mode	<u> </u>
			Disable DPD (De	sion (LZS) ead Peer Detection) -
		Help	<u>0</u> K	<u>C</u> ancel
IPSec Configuration	_			Configure
¥∎ IPSec Policy				New Entry
				Duplicate
				Delete

<u>C</u>lose

#### 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**.

siloy risino .				
Authentication	Encryption	Hash	DH Group	p (
Preshared Key	DES	MD5	DH-Group	p 2 (1024 Bit)
uthentication :	Disabular	/		
Authentication :	Preshared 1	Key	<u>·</u>	Add
Authentication :	Preshared H	<ey< th=""><th><b>•</b></th><th>Add</th></ey<>	<b>•</b>	Add
Authentication : Encryption : Hash :	Preshared P DES MD5	Sey	¥ ¥	Add Remove

#### 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.

I ransform	None	
DES	MD5	
ECD	*	LF A
Inor		Auu
DES	•	Bemove
		The fire fire
	ESP DES	DES MD5

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** 

General	IPSec Ge	neral Settings		
IPSec General Settings Identities IP Address Assignment		<u>G</u> ateway :	61.219.68.13	
Remote Networks Firewall Settings	Policies	IKE policy :	DES+MD5+DH2	•
		IPSec policy :	DES+MD5	•
			Policy lifetimes Po	blicy <u>e</u> ditor
	Advanc	ed options	1997 - 1997 -	
	$\sim$	Exch. <u>m</u> ode :	Main Mode	•
	2	PFS group :	DH-Group 1 (768 Bit)	-
			☐ Use IP compression ☐ Disable <u>D</u> PD (Dead	i (LZS) Peer Detection
			1	

#### 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.

General IPSec General Settings Identities IP Address Assignment	Enter th Without	Networks ie IP networks the tunnel : entries tunneling will alwa	should be used for. ays be used.	
Remote Networks Firewall Settings		Network addresses :	Subnet masks :	
		192.168.1.0	255.255.255.0 0.0.0.0 0.0.0.0 0.0.0.0	
		0.0.0.0		
		0.0.0.0		
		0.0.0.0		
		0.0.0.0	0.0.0.0	
		E Apply tunneling sec	urity for local networks	
		Help	<u>D</u> K <u>C</u> ancel	

Шаг 11

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



#### Шаг 12

Нажмите кнопку Connect для установления туннеля IPSec

D D-Link VPN Clie	ent		
Connection Confi	iguration <u>L</u> o	g <u>W</u> indow	<u>H</u> elp
Profile :			<u>O</u> utside Line :
test		•	
0 1 STORE 1 1111	ALC: UNITED IN COMPANY		
Concount ind	1.HIII.		
ALL HELE			-
CI. 210010001	Connection	is established	C
Client	Connection	is established	Server
Client Client	Connection	is established	Server
Client Connect	Connection	is established	Server
Client Connect Statistics: Time online:	Connection	is established	Server
Client Client Connect Statistics: Time online: Data (Tx) in Byte:	Connection Disconnect	is established	Server <b>D-Link</b> :): 0 sec out
Client Connect Statistics: Time online: Data (Tx) in Byte: Data (Rx) in Byte:	Connection Disconnect 00:00:30 240 240	is established	Server Server

# 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 РРТР и клиент РРТ	Ρ
--------------------------------	---

На	стройки удаленного межсетевого экрана	На	стройки локального межсетевого экрана
1-	Включить клиент РРТР	1-	Включить сервер РРТР
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)

<u>IPSec</u>	<u>VPN Hub</u>	<u>VPN Spoke</u>	РРТР	L2TP	<u>Pas</u> <u>Throu</u>	<u>s</u> Igh	
	🗹 Enable PP	TP Server					
[Server] [ <mark>Cli</mark>	<u>ent]</u>						
			Local	IP: 10.10.	99.254		
				Assigned I	P Range		
		Start:	10.10.99.20	)0	End: 10.10.	99.205	]
			с. н				
		Username	firewall		Password:	•••••	
				Арр	ly		

2- Включить клиент PPTP (Advanced settings -> VPN settings -> PPTP -> Client)

<u>IPSec</u>	VPN Hub	VPN Spoke	РРТР	L2TP	Pass Through	
	Enable PP	TP Client				
[Server][Clie	ent]					
			Serve	er IP: 61.219.	68.13	
2		Username	firewall	F	assword:	
			As	signed IP: 10	.10.99.201	
				Apply	/	

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

	#	Туре	Destination/Netmask	Gateway	Activated
•	1	Net	10.10.99.0/255.255.255.0	10.10.99.201	Yes
	2	2	-	÷_	120
	3	2	-	<u>.</u>	-
	4	2	-	2	120
	5	2		2	121
	6	2	-	2	20

## DFL-1100/700/200

1- Добавить пользователя (Firewall -> Users)

#### User Management

Add new user:

User name:	firewall	
Group membership:	[	
Password:	*****	

#### L2TP/PPTP settings:

Static client IP:	If empty, the IP address will be taken from the server's IP p
Networks behind user:	192.168.1.0/24

#### 2- Включить сервер PPTP (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: 10.10.99.2	00 - 10.10.99.205
Proxy /	ARP dynamically added routes
Primary DNS:	(Optional)
Secondary DNS:	(Optional)
💌 Use un	it's own DNS relayer addresses
Primary WINS:	(Optional)
Secondary WINS:	(Optional)

3- Включить сервер PPTP (Firewall -> VPN)

#### L2TP/PPTP Clients

Add PPTP Client :

ettings:		
Username:	firewall	
Password:	*****	
Retype Password	*****	
Interface IP:		Blank = get IP from s
Remote Gateway:	61.219.68.13	
Remote Net:	10.10.99.0/24	

☑ Use primary DNS server from tunnel as primary DNS

□ Use secondary DNS server from tunnel as secondary DNS Hint: Use Servers -> DNS Relayer to easily make DNS servers available to internal clients.

## 2-3-2 Сервер L2TP и клиент L2TP

Настройки удаленного межсетевого экрана Настройки локального межсетевого экрана

## 2-3-3 IPSec

Had	стройки удаленного межсетевого экрана	Ha	стройки 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:	6-	Конечный IP-адрес туннеля:
	61.219.68.13		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)

ddress	Service	<u> </u>	leuule								
jects] [Gro	ups]										
Address	-> Object	s -> Edit									
				Edit Ad	Iros	e oh	iect	tnu	mho	r 1	
Name				Luit Au	in cos	5 00	Jee		moe		
		1	Address na	ame: WAN1-V	PNA						
Value	· · · · · · · · · · · · · · · · · · ·										
Address 7	Type:										
💿 Su	bnet	IP:	10.10.99.0	) Ma	sk:	255	.255	5.25	5.0		
ORa	nge	Start IP:	0.0.0.0	End	I IP:	255	255	5.25	5.25	5	
OHo	st	IP:	0.0.0.0								
				Back	:		_	Aı	oply		ר
	<u> </u>		• Ast _ 100-007 [ ] 1	Back	:			Aı	oply		]
ddress jects] [Gro	<u>Servic</u> ups]	e <u>Sc</u>	hedule	Back	:	_)(		A	oply		]
ddress jects] [Gro Address	<u>Servic</u> ups] -> Object	<u>e</u> <u>Sc</u> s -> Edit	<u>hedule</u>	Back	:	_)(		Aı	oply		)
ddress jects] [ <u>Gro</u> Address	<u>Servic</u> ups] :-> Object	<u>e</u>	<u>hedule</u>	Edit Ad	dre	)( ss ol	bjed	A <sub>I</sub>	ply	er 1	)
ddress jects] [ <u>Gro</u> Address Name	<u>Servic</u> • <u>ups]</u> :-> Object	<u>e</u>	hedule	Back Edit Ad	dre	ss ol	bje	A <sub>I</sub>	pply	er 1	)
ddress jects] [ <u>Gro</u> Address Name	<u>Servic</u> u <u>ps]</u> -> Object	<u>≊ Sc</u> :s -> Edit	<u>hedule</u> Address na	Edit Ad	dre:	ss ol	bjed	A <sub>I</sub>	umb	er 1	)
ddress jects] [ <u>Gro</u> Address Name Value	<u>Servic</u> oups] -> Object	<u>e</u> ∣ <u>Sc</u> :s -> Edit	hedule Address na	Edit Ad	: d <b>dre</b> :	ss ol	bjeo	Ap ct nu	pply	er 1	)
ddress jects] [ <u>Gro</u> Address Name Value Address	<u>Servic</u> oups] -> Object	<u>≅ Sc</u> :s -> Edit	<u>hedule</u> Address na	Edit Ad	: dre:	ss ol	bje	Ap ct nu	umb	er 1	)
ddress jects] [ <u>Gro</u> Address Name Value Address	<u>Servic</u> oups] )-> Object )-> Type: bnet	<u>e</u> ∣ <u>Sc</u> :s -> Edit IP	hedule Address na	Edit Ad ame: LAN1-VI	idre: PNA	ss ol	<b>bje</b>	A <sub>I</sub>	umb	er 1	
ddress jects] [ <u>Gro</u> Address Name Value Address © Su © Su	<u>Servic</u> oups] s-> Object s-> Dbject bject nge	:e <u>Sc</u> :s -> Edit IP Start IP	hedule Address na 192.168.1	Edit Ad ame: LAN1-VI	: onA ask: d IP	ss ol : 25: 25:25	bje 5.28	AI ct nu 55.2(	oply umb 55.0	er 1	
ddress jects] [Gro Address Name Value Address © Su © Ra © Ho	<u>Servic</u> oups] )-> Object )-> Dbject bipet nge st	e <u>Sc</u> s -> Edit IP Start IP	hedule Address na : 192.168.1 : 0.0.0 : 0.0.0	Edit Ad ame: LAN1-VI	idree PNA ask: d IP	ss ol : 25 2: 25	bjec 5.26	A <sub>I</sub> ct nu 555.2!	oply umb 55.0	er 1	
ddress jects] [Gro Address Name Value Address © Su © Ra O Ho	<u>Servic</u> oups] s-> Object s-> Dbject nge st	e <u>Sc</u> s -> Edit IP Start IP IP	hedule Address na 192.168.1 0.0.0.0	Edit Ad ame: LAN1-VI	idre: PNA ask: d IP	ss ol : 25: 25: 25:	bjec 5.26	AI ct nu 55.2(	oply umb 55.0	er 1	
ddress jects] [Gro Address Name Value Address © Su © Ra O Ho	Servic oups] -> Object -> St	e <u>Sc</u> s -> Edit IP Start IP IP	hedule Address na 192.168.1 0.0.0.0 0.0.0.0	Edit Ad ame: LAN1-VI	dre: PNA ask: d IP	ss ol : 25 25	bjec 5.25 5.25	AI ct nu 55.2!	pply umb 55.0 55.2	er 1	

#### 02- Отредактировать правила межсетевого экран (Advanced Settings -> Firewall -> Edit

Rule	es)							
St	<u>atus</u>	Edit Rul	es Show Rules	Attack Alert Sun	nmary			
	Firewa	all->Edit Rul	es					
	Edit	WAN1 V	to LAN1 V rul					
	Dofa	ult action for	this nacket direct	ion Block V				
Pack	ets are	e top-down	matched by the	rules.				
lte	em		Status		Cond	ition		Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y
								Page 1/1
			F	vev. Page Ne	st Page Mov	e Page 1		
			Insert	Edit	Delete	Move Before: 1		
					A		5	
Fire	wall->	Edit Rules	s->Insert					
					ana			
		Contraction of the local division of the loc		Insert a new	WAN1-to-LAN1	Firewall rule		-
		Status	Dula series [	Nul-4				
			Rule name: F	kule i				
		Property and the second	Schedule: /	Always 📉				_
		Condi	tion					(CONT)
			Source IP:	WAN1-VPNA	~	Dest. IP: LAN1-VF	'NA	~
			Service:	ANY 💌				
		Action	1					
			Forward 🚩 a	nd log 🗡	the matched s	ession.		
			Fo	rward bandwidt	h class: def_cla	ss 💙		
			Re	verse bandwidt	h class: def_cla	ss 👻		
					19			
				Bac	k Aj	ply		
						121		

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

IPSec	VPN Hub	<u>VPN Spoke</u>	<u>PPTP</u>	L2TP	Pass Through
	Enable IP:	Sec Apply			
IPSec->IKE->E	Edit Rule				
			Status		
			Active		
		IKE Rule Name	Condition	1	
		Local Add	ress Type Sul	onet Address 👻	
		IP Address	19	2.168.1.0	
		PrefixLen / S	ubnet Mask 25	5.255.255.0	
		Remote Ad	dress Type Su	ubnet Address	~
		IP Address	10	).10.99.0	
		PrefixLen / S	ubnet Mask 25	5.255.255.0	
			Action		
		Negotiation Mod	Action de Main		
		Negotiation Mod Encapsulation I	Action de Main Mode Tunne	<b>~</b>	
	Outgoing	Negotiation Mod Encapsulation I Interface WAN1	Action de Main Mode Tunne		
	Outgoing Peer's IP	Negotiation Mod Encapsulation I Interface WAN <sup>1</sup> Address Static	Action de Main Mode Tunne I 👻 IP 👻 61	.219.68.13	
	Outgoing Peer's IP My Identifier	Negotiation Mod Encapsulation I Interface WAN <sup>4</sup> Address Static	Action de Main Mode Tunne I 👻 IP 🛩 61	✓ I ✓ .219.68.13 Auto_Assign	ed
	Outgoing Peer's IP My Identifier Peer's Identifie	Negotiation Mod Encapsulation I Interface WAN <sup>1</sup> Address Static IP Address	Action de Main Mode Tunne I 👻 IP 👻 61	✓ I ✓ .219.68.13 Auto_Assign Auto_Assign	ed
	Outgoing Peer's IP My Identifier Peer's Identifie O ESP Algo O AH Algo	Negotiation Mod Encapsulation Mod Interface WAN Address Static IP Address IP Address IP Address IP Address	Action de Main Mode Tunne I V 61 IP V 61 V and Authentic ate (MD5)	✓         .219.68.13         Auto_Assign         Auto_Assign         ate (DES, MI	ed 25)

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

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

	Phase 2		
Encapsulation	Tunnel		
Active Protocol	ESP		
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) Encrypt and Authenticate (AES, MD5)		
Back	Encrypt and Authenticate (AES, SHA1) Encrypt only (DES) Encrypt only (3DES)		
o <u>Save Running Configur</u>	Encrypt only (AES) Authenticate only (MD5) Authenticate only (SHA1)		

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

#### Локальный межсетевой экран:

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

lress-> Obje	cts -> Edit	
		Edit Address object number 1
пе	Address name: V	VAN1-VPNB
le		
dress Type:	IP-192 168 1 0	Mask: 255 255 255 0
○ Range	Start IP: 0.0.0.0	End IP: 255.255.255.255
OHost	IP:0.0.0.0	

Iress-> Obje	cts -> Edit	
		Edit Address object number 1
ne	Address name:	LAN1-VPNB
lue		
oress 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
O Host	IP: 0.0.0.0	

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

Firewal	I->Edit Rule	is	Autock Alen Sun	intary		
Edit C Defaul ackets are	VAN1 🗡 t It action for t top-down i	o LAN1 🗡 rub this packet direct matched by the	es ion: <mark>Block →</mark> ✓ rules.	Log Apply		
ltem	s	tatus		Condi	tion	
#	Name	Schedule	Source IP	Dest. IP	Service	Actio
	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block
	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	E

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 🗸

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

IPSec <u>VF</u>	PN Hub VPN Spoke	<u>PPTP</u>	<u>L2TP</u>	<u>Pass</u> <u>Through</u>	
Er	able IPSec Apply				
IPSec->IKE->Edit Ru	le				
		Status			
		Active	]		
12	IKE Rule Name ipsec				
		Condition		Mie -	
	Local Addr	ress Type Subr	net Address 💊		
	IP Address	10.	10.99.0		
	PrefixLen / St	ubnet Mask <mark>255</mark>	5.255.255.0		
	Remote Add	dress Type Sul	onet Address	~	
	IP Address	192	2.168.1.0		
	PrefixLen / St	ubnet Mask 255	5.255.255.0		

	Action	1		
Ne	egotiation Mode	Main 🗸		
Er	ncapsulation Mode	Tunnel 💌		
Outgoing Inte	erface WAN1 💌			
Peer's IP Ad	dress Static IP	✓ 61.219.68.14		
My Identifier	P Address	Auto_Assigned		
Peer's Identifier	P Address	Auto_Assigned		
<ul> <li>● ESP Algorith</li> <li>○ AH Algorith</li> </ul>	m Encrypt and Au m Authenticate (N	uthenticate (DES, 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 💌 DH1		
	DH2 DH5 hase	2	

	Phase 2
Encapsulation	Tunnel
Active Protocol	ESP
Encryption Algorithm	Encrypt and Authenticate (DES, MD5)
SA Life Time Perfect Forward Secrecy(PFS)	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)
to <u>Save Running Configur</u>	Encrypt only (AES) Authenticate only (MD5) Authenticate only (SHA1) 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 V None DH1 Apply DH2 Apply DH5

## 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:	3		
VPN:	Allow all VPN traffic: internal->VPN, VPN->internal and VPN-	>VPN.	
	🧭	8	0
	Apply	Cancel	Help

2- Включить IPSec и отредактировать политику IPSec (Firewall -> VPN -> IPSec Tunnels)

#### **VPN Tunnels**

Edit IPsec tunnel ipsec:

Name, ppsec	
Local Net: 192.168.1.0/24	

Authentication:

•	PSK ·	Pre-Shared Key	
---	-------	----------------	--

PSK:	****	1224567000
Retype PSK:	****	1234307890

#### C Certificate-based

Cortificatos:	r
Certificates.	
	Use ctrl/shift click to select multiple certificates
	To use ID lists below, you must select a CA certificate.
	12 W.X.

Tunnel type:

C Roaming Users - single-host IPsec clients

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

#### EAN-to-LAN tunnel

Remote Net:	10.10.99.0/24
Remote Gateway:	61.219.68.13
	The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.
Route:	Automatically add a route for the remote network.
Proxy ARP:	Publish remote network on all interfaces via Proxy ARP.
IKE XAuth client:	$\square$ 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**:

INE Mode:	Main mode IKE
	O Aggressive mode IKE
IKE DH Group:	2 - modp 1024-bit 💌
PFS:	Enable Perfect Forward Secrecy
PFS DH Group:	1 - modp 768-bit 💌
NAT Traversal:	C Disabled.
	• On if supported and needed (NAT detected between gateway
	C On if supported
Keepalives:	• No keepalives.
	C Automatic keepalives (works with other DFL-200/700/1100 u
	C Manually configured keepalives:
	Source IP:

#### IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1	DES	MD5 💽	0	28800
#2	DES A	MD5 -	0	28800
#3:	CAST-128	SHA-1 💌	0	28800
#4:	Blowfish-40 Allowed: 40-448 Blowfish-128 Allowed: 40-448	MD5 💌	0	28800
#5:	Blowfish-256 Allowed: 40-448 Blowfish-128 Allowed: 128-448	SHA-1 💌	0	28800
#6:	Blowfish-256 Allowed:128-448 Blowfish-256 Allowed:256-448	MD5 💽	0	28800
#7:	Blowfish-448 Allowed:256-448	MD5 🖃	0	0
#8:	· •	MD5 💽	0	0

#### **IPsec Proposal List**

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

#### Локальный межсетевой экран:

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

#### **Firewall Policy**

Edit global policy parameters:

Fragments:	Drop all fragmented packets		
Minimum TTL:	3		
VPN:	Allow all VPN traffic: internal->VPN, VPN->internal and VPN->	VPN.	
	<b>S</b>	8	0
	Apply	Cancel	Help

2- Включить IPSec и отредактировать политику IPSec (Firewall -> VPN -> IPSec Tunnels)

#### **VPN Tunnels**

Edit IPsec tunnel **ipsec**:

Name:	ipsec	
Local Net:	10.10.99.0/24	

#### Authentication:

PSK:		1	
Retype PSK:	•••••	1234567890	
ertificate-ba	sed		
ocal Identity:	Admin - CN=000E3D596564		~
	Mathin - Cheropol of Samana		11.20
Certificates:		~	
Certificates:		~	
Certificates:		~	
Certificates:	Use ctrl/shift click to select m To use ID lists below, you mus	ultiple certificates. st select a CA certificate.	

Tunnel type:

O Roaming Users - single-host IPsec clients

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

#### ● LAN-to-LAN tunnel

Remote Net:	192.168.1.0/24
Remote Gateway:	61.219.68.14
	The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.
Route:	Automatically add a route for the remote network.
Proxy ARP:	Publish remote network on all interfaces via Proxy ARP.
IKE XAuth client:	Pass username and password to peer via IKE XAuth, if the remote gateway requires it.
XAuth Username:	
XAuth Password:	

#### **VPN Tunnels**

Edit advanced settings of IPsec tunnel ipsec:

Limit MTU:	1424
IKE Mode:	Main mode IKE
	O Aggressive mode IKE
IKE DH Group:	2 - modp 1024-bit 💌
PFS:	Enable Perfect Forward Secrecy
PFS DH Group:	1 - modp 768-bit 💌
NAT Traversal:	O Disabled.
	<ul> <li>On if supported and needed (NAT detected between gateways)</li> </ul>
	On if supported
Keepalives:	No keepalives.
	O 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 3DES	MD5 💌	0	28800
#3:	CAST-128	SHA-1 💌	0	28800
#4:	Blowfish-40 Allowed:40-448 Blowfish-128 Allowed:40-448	MD5 💌	0	28800
#5:	Blowfish-256 Allowed: 40-448 Blowfish-128 Allowed: 128-448	SHA-1 💌	0	28800
#6:	Blowfish-256 Allowed:128-448 Blowfish-256 Allowed:256-448	MD5 🔽	0	28800
#7:	Blowfish-448 Allowed:256-448 Blowfish-448 Allowed:448-448	MD5 💌	0	0
#8:	- Twofish-128 Allowed: 128-256 Twofish-256 Allowed: 128-256 Twofish-255 Allowed: 256-256	MD5 💌	0	0
IPse	q -			
	AES-128 Allowed:128-256 AES-256 Allowed:128-256	HMAC	Life KB	Life Sec
#1:	AES-256 Allowed:256-256	MD5 💌	0	3600

#### IPsec Proposal List

	Cipher	H
#1:_	DES	
#2:	DES ODES	
#3:	CAST-128	Ē
#4:	Blowfish-40 Allowed: 40-448 Blowfish-128 Allowed: 40-448	Ē
#5:	Blowfish-256 Allowed:40-448 Blowfish-128 Allowed:128-448	
#6:	Blowfish-256 Allowed:128-448 Blowfish-256 Allowed:256-448	Ē
#7:	Blowfish-448 Allowed:256-448 Blowfish-448 Allowed:448-448	
#8:	- Twofish-128 Allowed:128-256 Twofish-256 Allowed:128-256 Twofish-256 Allowed:256-256	
"AES estab receiv	AES-256 Allowed:128-256 AES-256 Allowed:128-256 AES-256 Allowed:128-256 AES-256 Allowed:256-256	nis un Iccep

HMAC	Life KB	Life Sec
MD5 💌	0	3600
MD5 💌	0	3600
SHA-1 🐱	0	3600
MD5 💌	0	3600
SHA-1 💌	0	3600
MD5 💌	0	3600
MD5 💌	0	0
MD5 💌	0	0

is unit will propose 128 bit encryption to the rem ccept any cipher key sizes between 128 and 2



## **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
Enabled	🗹 Enabled
Allow all except policy settings	Allow all except policy settings
🔿 Deny all except policy settings	O Deny all except policy settings

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

<u>IPSec Settings</u> / Status	<u>Manual Key</u> / Tun	nel Settings / <u>Tunnel Table</u> / <u>IPSe</u>
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	Π
IKE Mode	💿 Main	O Aggressive
Encapsulation	Tunnel	🔿 Transport mode
NAT traversal	Normal	O 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 💌	

1 11436 2 1 10/03	al	
Name	P2Param	
PFS Mode	Group 1 💌	
Encapsulation	ESP 👻	
IPSec Life Duration	6000	seconds
ESP Transform	DES 💌	105
ESP Auth	HMAC-MD5	A A A A A A A A A A A A A A A A A
AH Transform	MD5 ~	
Click here to ad	P1 proposal	
ттторозаіз		NOT_SET
1 1 1 10003013	NOT_SET	NOT_SET
Click here to ad	NOT_SET V	NOT_SET
Click here to ad	NOT_SET V Id P2 proposal	NOT_SET V
<u>Click here to ad</u> P2 Proposals	NOT_SET V Id P2 proposal P2Param V NOT_SET V	NOT_SET V NOT_SET V NOT_SET V
<u>Click here to ad</u> P2 Proposals Target Host Rar	NOT_SET V Id P2 proposal P2Param V NOT_SET V	NOT_SET V NOT_SET V NOT_SET V
Click here to ad P2 Proposals Target Host Rar Starting Target Host	NOT_SET V NOT_SET V NOT_SET V NOT_SET V NOT_SET V 10.10.99.0	NOT_SET V NOT_SET V NOT_SET V

#### 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
🗹 Enabled	🗹 Enabled
Allow all except policy settings	<ul> <li>Allow all except policy settings</li> </ul>
O Deny all except policy settings	○ Deny all except policy settings

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

IPSec Settings /	Manual Key / Tun	nel Settings / <u>Tunnel Table</u> / <u>IPS</u>
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	20
IKE Mode	💿 Main	O Aggressive
Encapsulation	Tunnel	🔿 Transport mode
NAT traversal	Normal	ESP Over UDP (port 500)
IPSec Operation	ESP 💌	
Phase 1 Proposal	Por a secondaria i	
Name	P1Param	
DH Group	Group 2 💌	
IKE Life Duration	6000	seconds
IKE Encryption	DES 💌	
IKE Hash	MD5 💌	

Phase Z Propos	ai	
Name	P2Param	2
PFS Mode	Group 1 💌	
Encapsulation	ESP 💌	
IPSec Life Duration	6000	seconds
ESP Transform	DES 💌	
ESP Auth	HMAC-MD5 💌	
AH Transform	MD5 V	
	INDO P	
<u>Click here to ad</u> P1 Proposals	Id P1 proposal P1Param	NOT_SET ¥
<u>Click here to ad</u> P1 Proposals	Id P1 proposal P1Param V NOT_SET V	NOT_SET ¥
<u>Click here to ad</u> P1 Proposals <u>Click here to ad</u>	Id P1 proposal P1Param V NOT_SET V Id P2 proposal	NOT_SET V
<u>Click here to ad</u> P1 Proposals <u>Click here to ad</u> P2 Proposals	Id P1 proposal P1Param V NOT_SET V Id P2 proposal P2Param V	NOT_SET V NOT_SET V
<u>Click here to ad</u> P1 Proposals <u>Click here to ad</u> P2 Proposals	Id P1 proposal       P1Param       NOT_SET       Id P2 proposal       P2Param       NOT_SET	NOT_SET V NOT_SET V NOT_SET V
<u>Click here to ad</u> P1 Proposals <u>Click here to ad</u> P2 Proposals Target Host Rar	Id P1 proposal P1Param V NOT_SET V Id P2 proposal P2Param V NOT_SET V	NOT_SET V NOT_SET V NOT_SET V
<u>Click here to ad</u> P1 Proposals <u>Click here to ad</u> P2 Proposals Target Host Rar Starting Target Host	A P1 proposal P1Param V NOT_SET V A P2 proposal P2Param V NOT_SET V Ige 192.168.1.0	NOT_SET V NOT_SET V NOT_SET V