D-Link® CORPORATION

D-Link VPN Application

Руководство по быстрой установке

Содержание

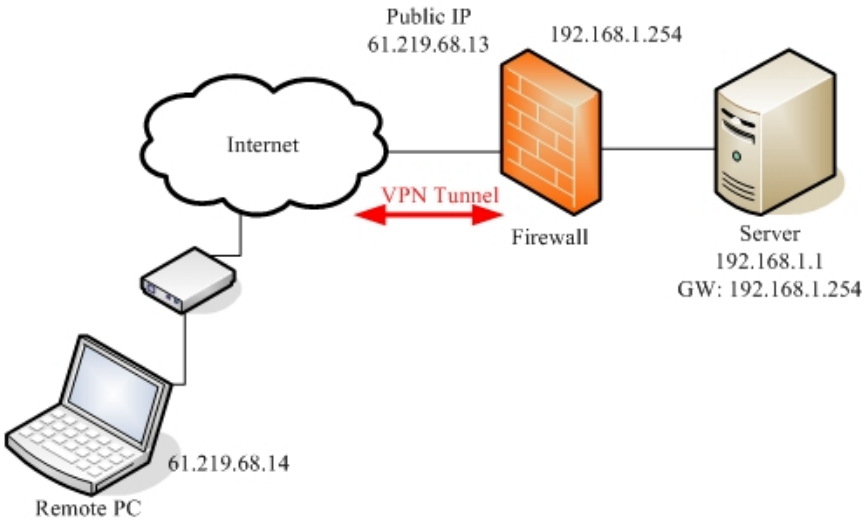
1. Удаленный доступ

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

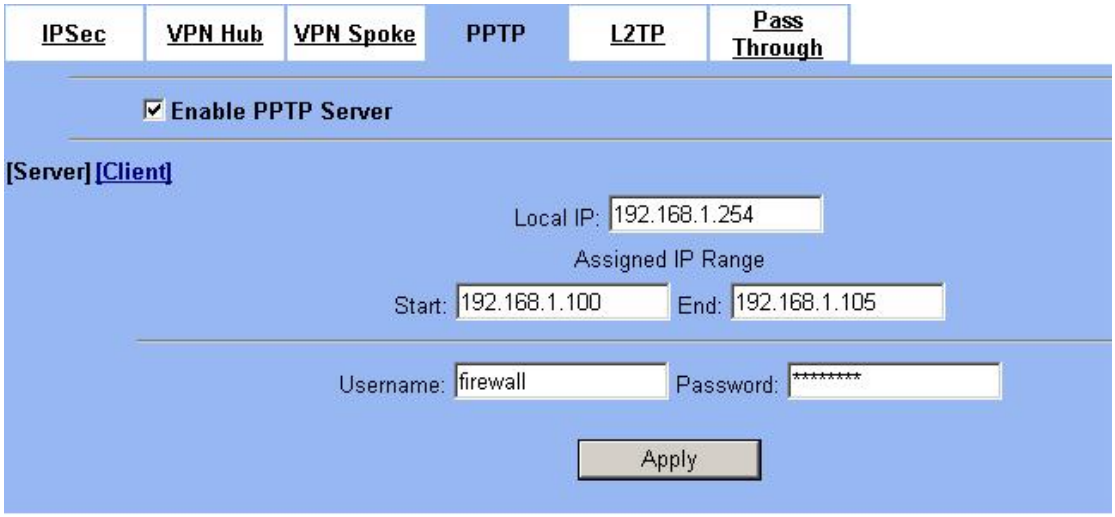
1-3-1 Сервер PPTP

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

Страница настройки параметров устройства

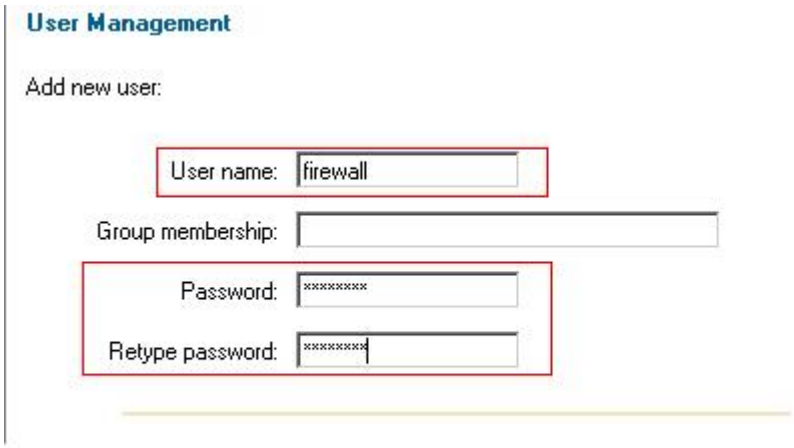
DFL-1500

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

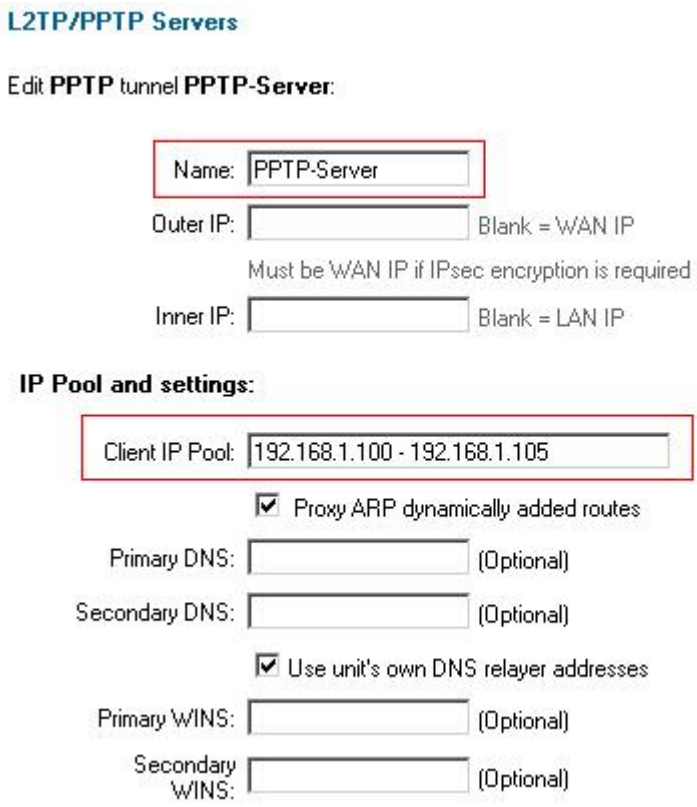


DFL-1100/700/200

01- Добавить пользователя (**Firewall -> Users**)



02- Включить сервер PPTP (**Firewall -> VPN**)



DFL-600

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

PPTP Settings / PPTP Account / PPTP Status

Add/New User Account

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 (VPN-адаптер ОС Microsoft XP PRO)

Шаг 1

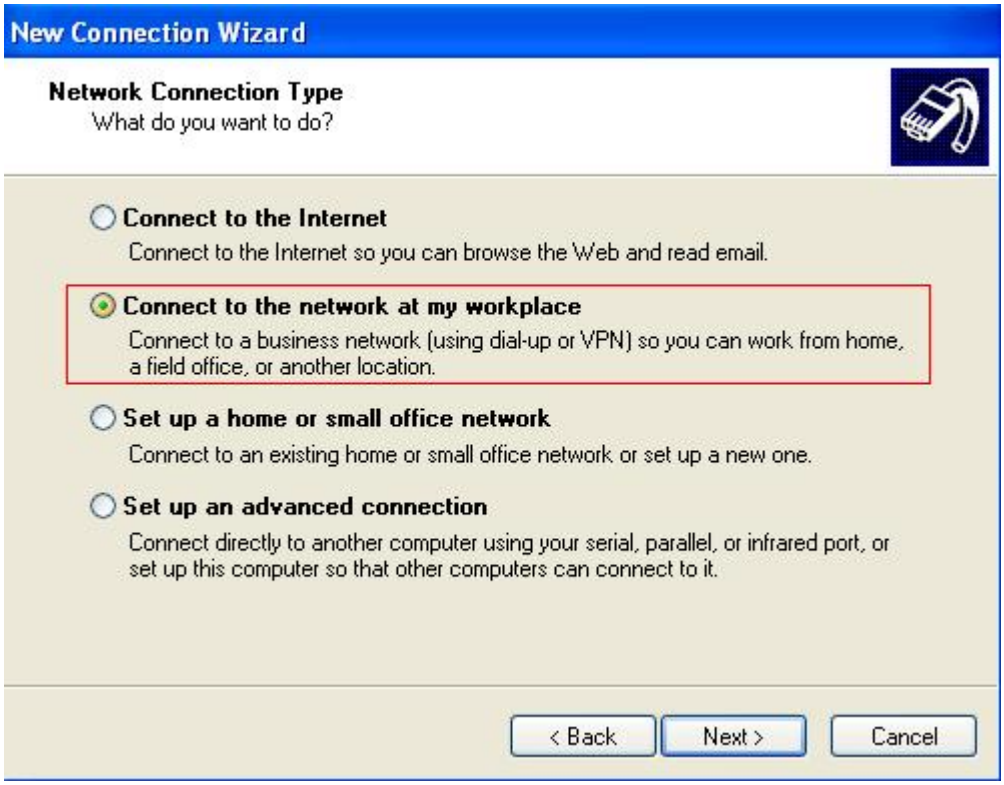
В свойствах сетевого окружения выберите “Новое подключение” для того, чтобы создать исходящее подключение VPN-PPTP.

Шаг 2

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

Шаг 3

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



Шаг 4

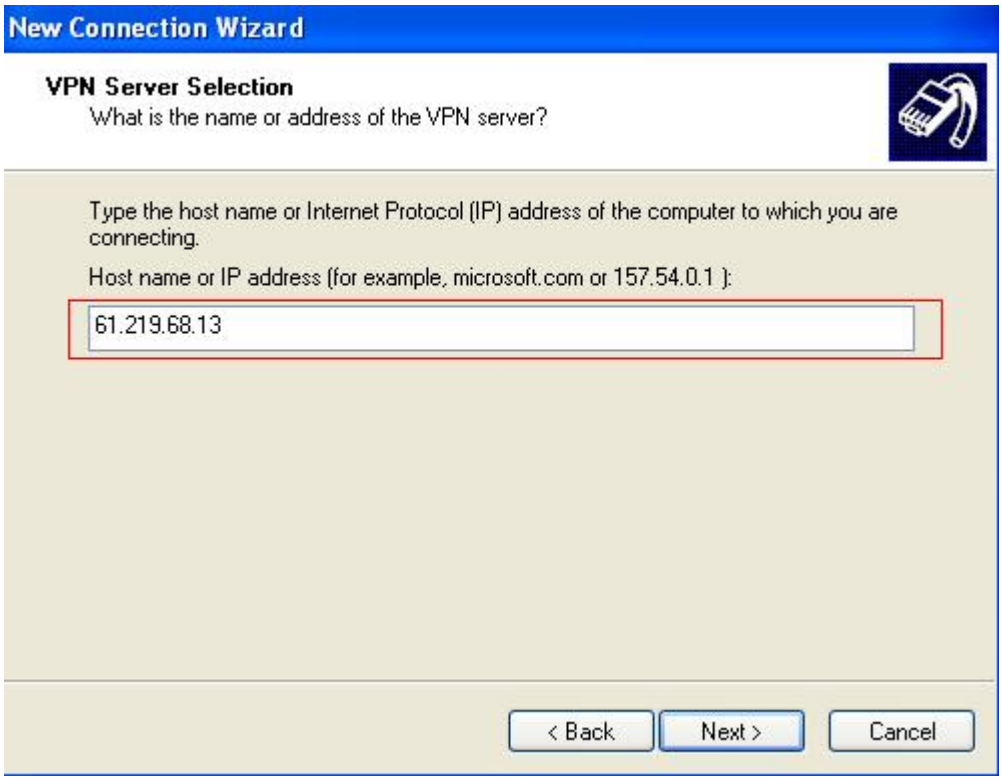
Выберите **Подключение к виртуальной частной сети**. Нажмите **Next** для перехода на следующий шаг.

Шаг 5

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

Шаг 6

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



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.

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

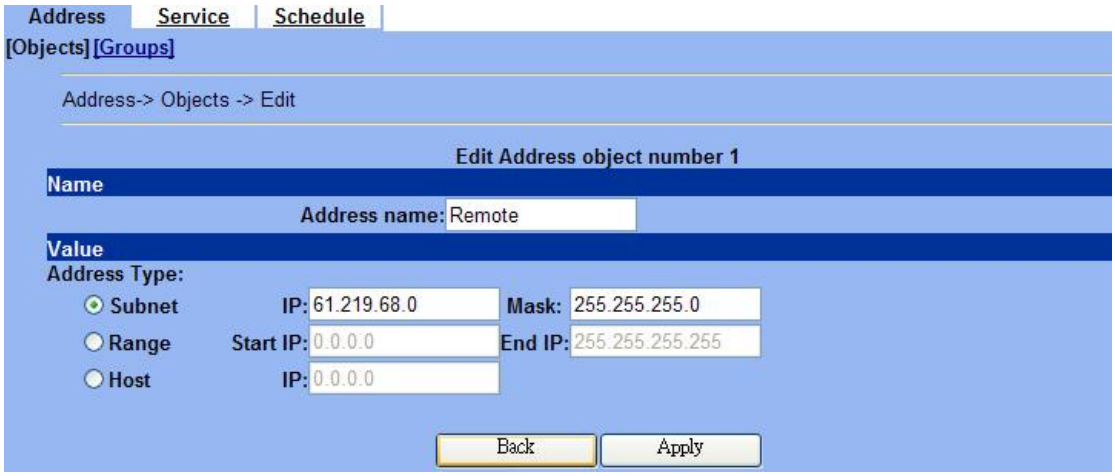
Настройки удаленного ПК	Настройки межсетевого экрана
01- Имя профиля: test	01- Имя политики: IPSec
02- Среда взаимодействия: LAN over IP	02- Локальный IP-адрес: 192.168.1.0/24
03- Шлюз: 61.219.68.13	03- Удаленный IP-адрес: 61.219.68.14
04- Политика IKE: DES+MD5	04- Режим согласования: Main
05- Группа 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
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

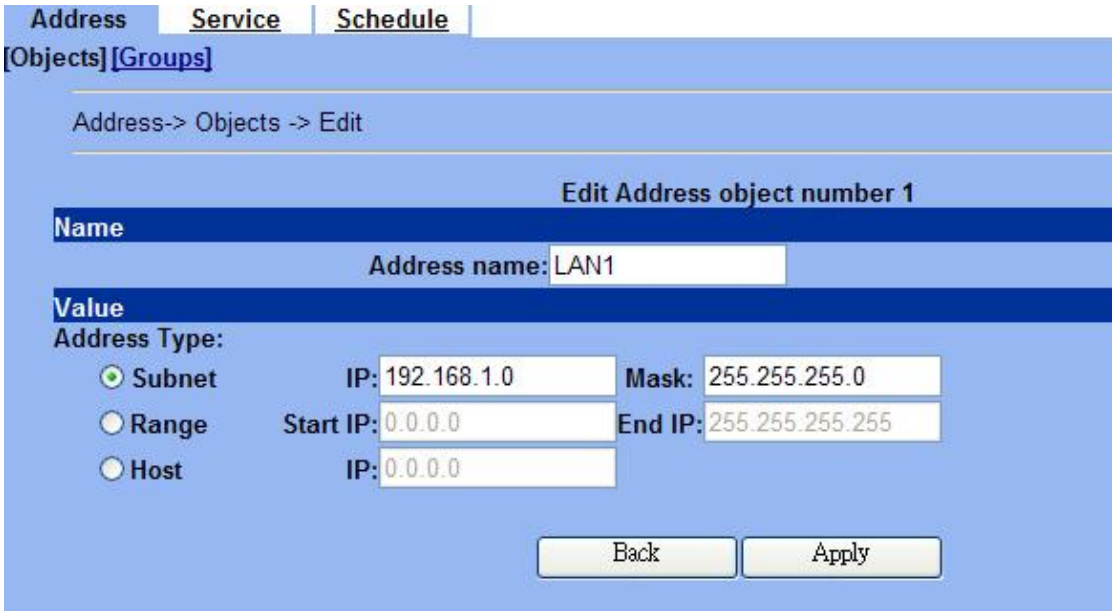
DFL-1500/900

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

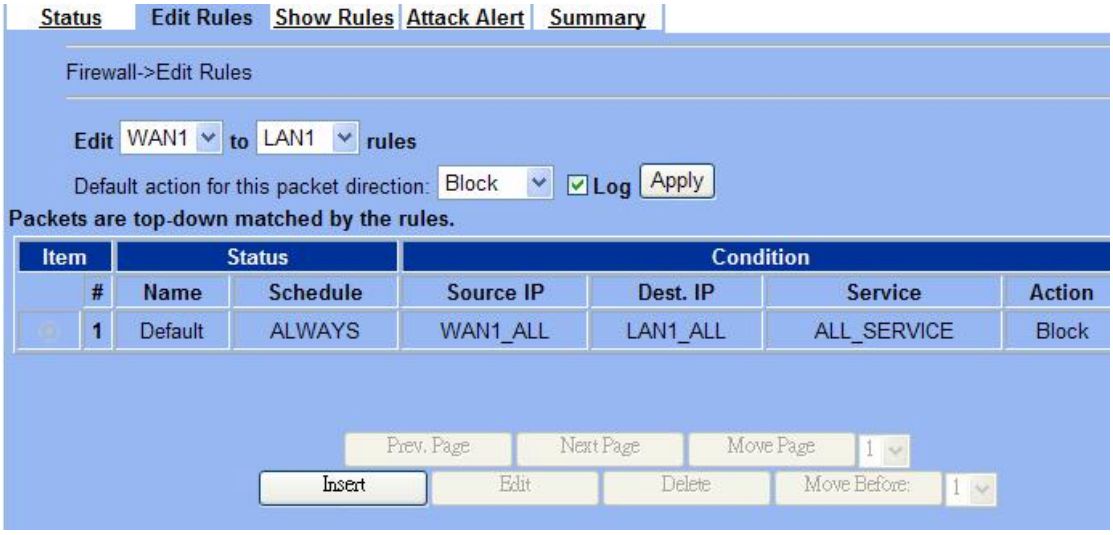
WAN1:

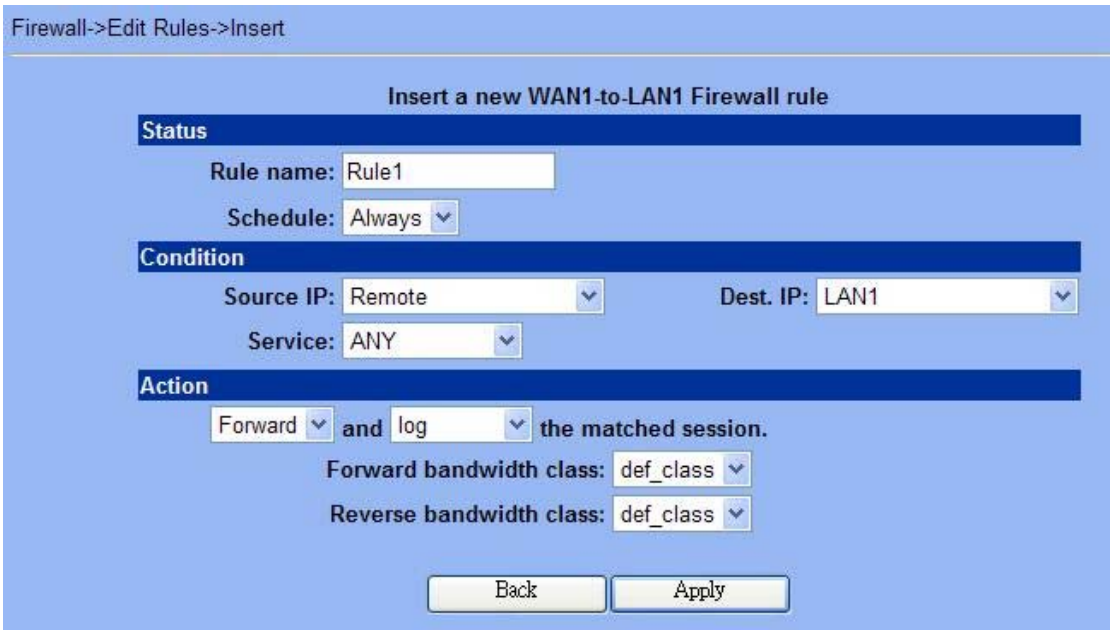


LAN1:



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





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

IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: ipsec

Condition

Local Address Type: Subnet Address

IP Address: 192.168.1.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Single Address

IP Address: 61.219.68.14

PrefixLen / Subnet Mask: 255.255.255.255

Action

Negotiation Mode: Main

Encapsulation Mode: Tunnel

Outgoing Interface: WAN1

Peer's IP Address: Static IP 61.219.68.14

My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

ESP Algorithm: Encrypt and Authenticate (DES, MD5)

AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890

Advanced

Phase 1

Negotiation Mode: Main

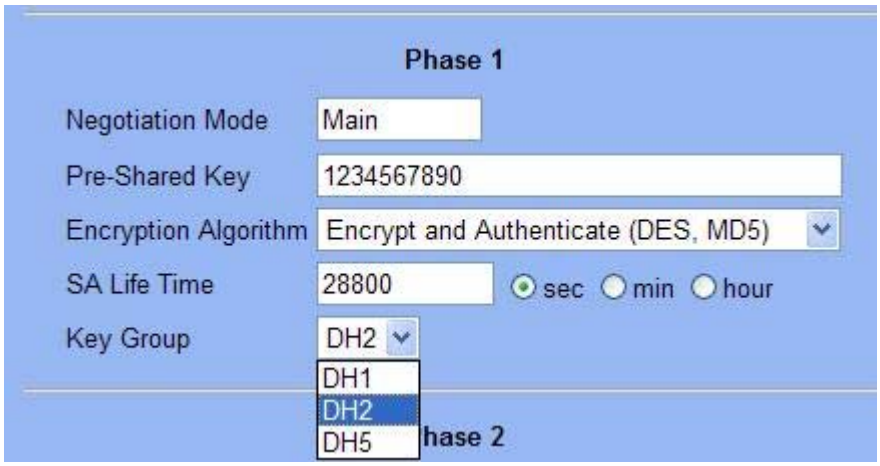
Pre-Shared Key: 1234567890

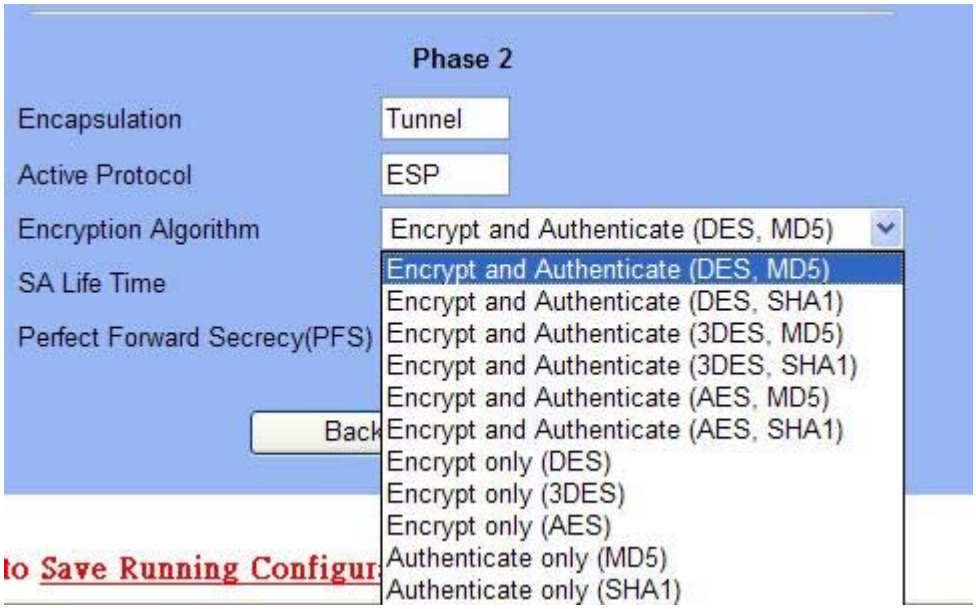
Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

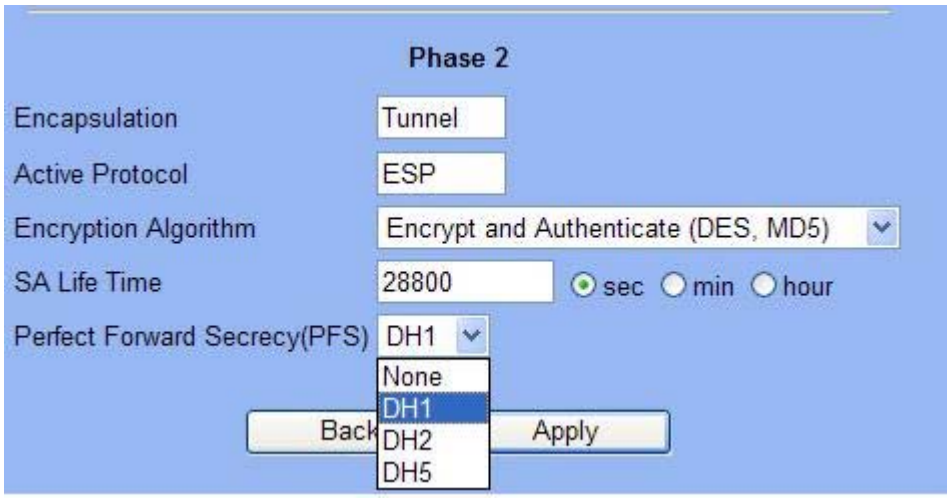
SA Life Time

Key Group

- Encrypt and Authenticate (DES, MD5)
- Encrypt and Authenticate (DES, SHA1)
- Encrypt and Authenticate (3DES, MD5)
- Encrypt and Authenticate (3DES, SHA1)

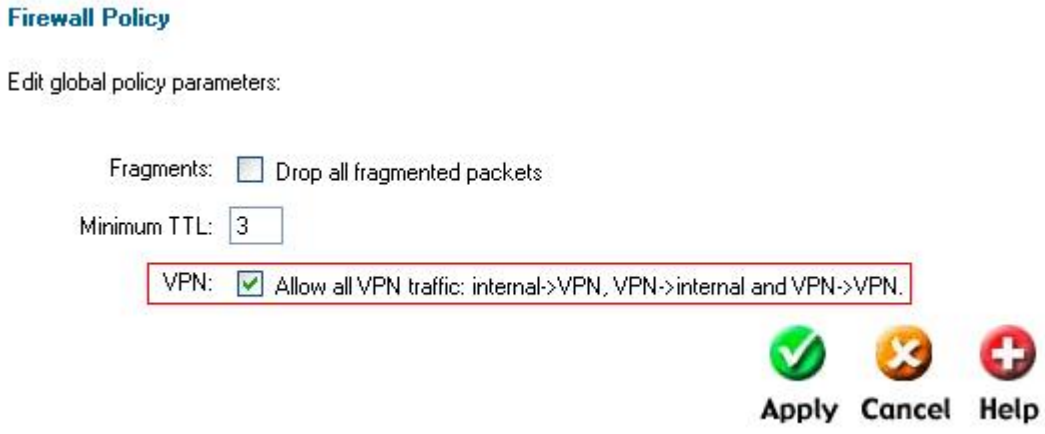

Phase 1
Negotiation Mode
Main
Pre-Shared Key
1234567890
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Key Group
DH2
DH1
DH2
DH5
hase 2


Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
Perfect Forward Secrecy(PFS)
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)
o Save Running Configur

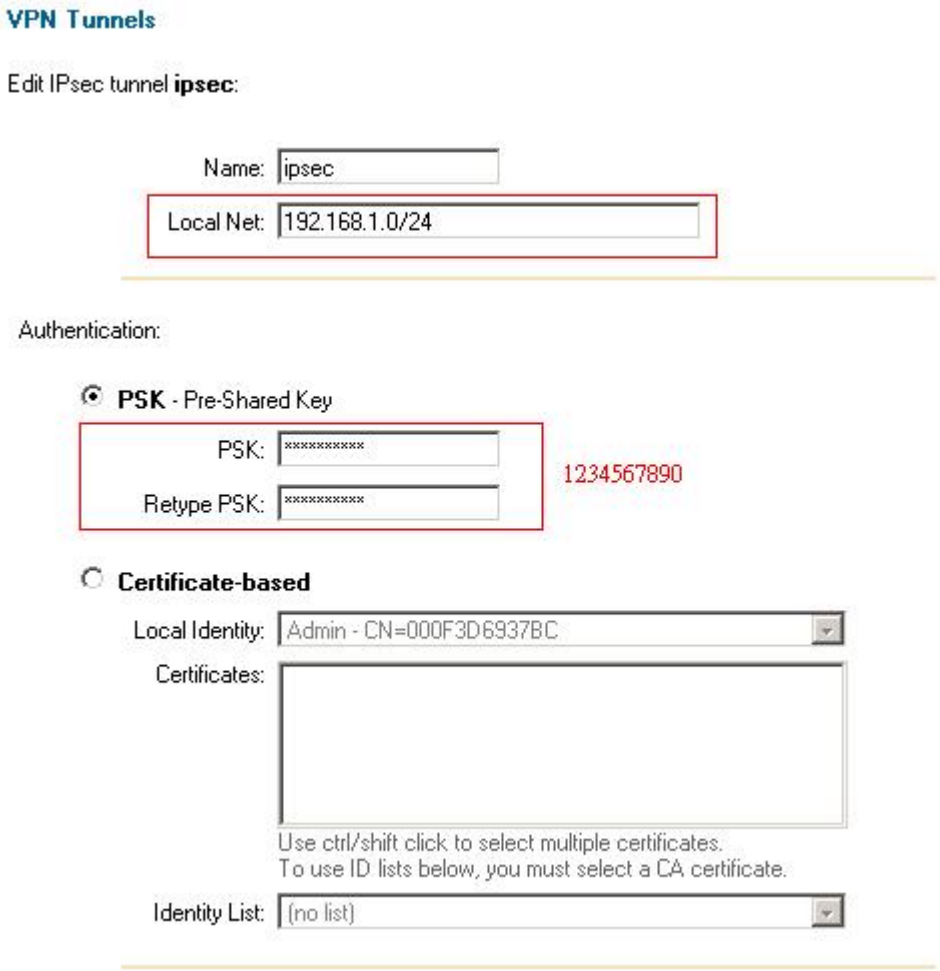

Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Perfect Forward Secrecy(PFS)
DH1
None
DH1
DH2
DH5
Back
Apply

DFL-1100/700/200

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



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



Tunnel type:

(•) **Roaming Users** - single-host IPsec clients

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

VPN Tunnels

Edit advanced settings of IPsec tunnel **ipsec**:

Limit MTU: 1424

IKE Mode: (•) Main mode IKE
( ) Aggressive mode IKE

IKE DH Group: 2 - modp 1024-bit

PFS: [x] Enable Perfect Forward Secrecy

PFS DH Group: 1 - modp 768-bit

NAT Traversal: ( ) Disabled.
(•) On if supported and needed (NAT detected between gateways)
( ) On if supported

Keepalives: (•) No keepalives.
( ) Automatic keepalives (works with other DFL-200/700/1100 units)
( ) Manually configured keepalives:

Source IP:

Destination IP:

IKE Proposal List

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

Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

IPsec Proposal List

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

Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

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

Phase 1 Proposal

Name	P1Param	
DH Group	Group 2	
IKE Life Duration	6000	seconds
IKE Encryption	DES	
IKE Hash	MD5	

Phase 2 Proposal

Name	P2Param
PFS Mode	Group 1
Encapsulation	ESP
IPSec Life Duration	6000 seconds
ESP Transform	DES
ESP Auth	HMAC-MD5
AH Transform	MD5

Click here to add P1 proposal

P1 Proposals	P1Param	NOT_SET
	NOT_SET	NOT_SET

Click here to add P2 proposal

P2 Proposals	P2Param	NOT_SET
	NOT_SET	NOT_SET

Target Host Range

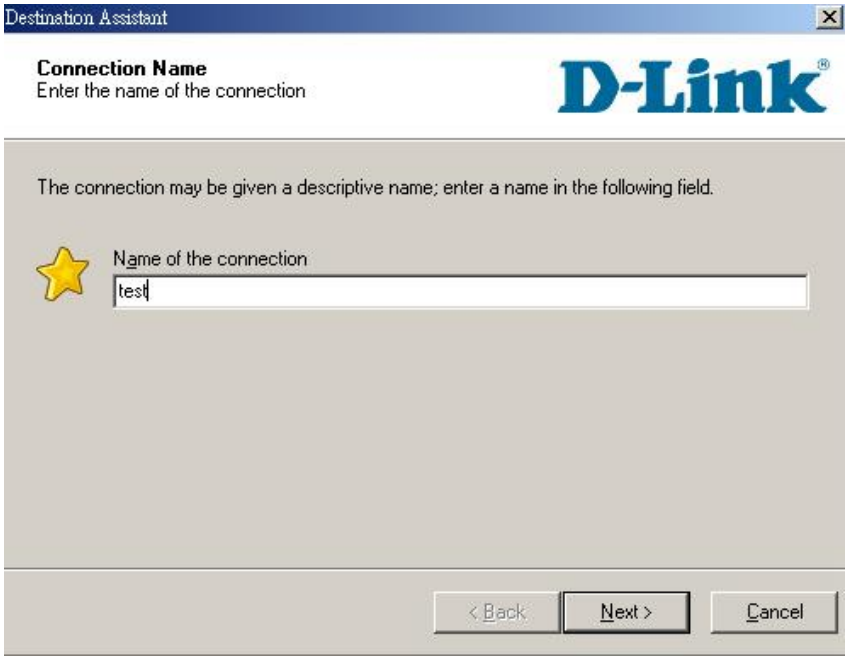
Starting Target Host	61.219.68.0
Subnet Mask	255.255.255.0

Настройка подключения IPSec (D-Link DS-601)

Шаг 1

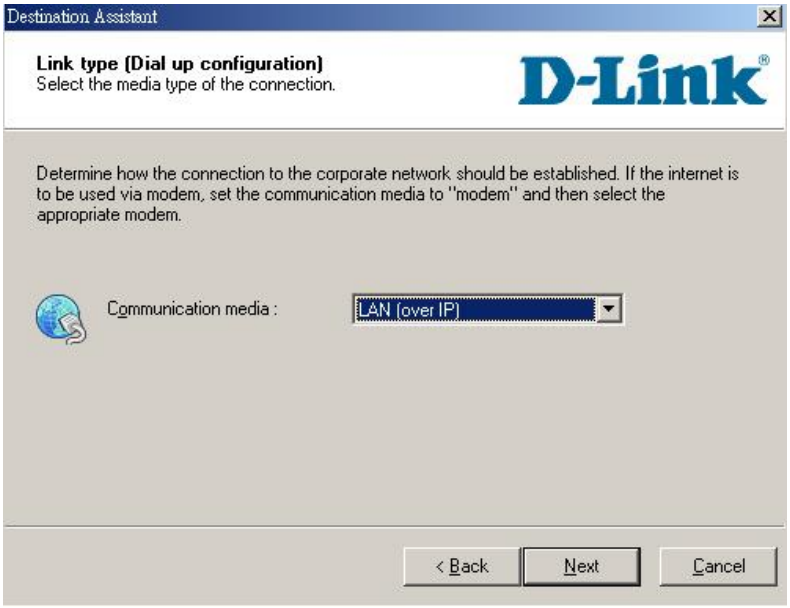
Configuration->Profile settings->New Entry

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



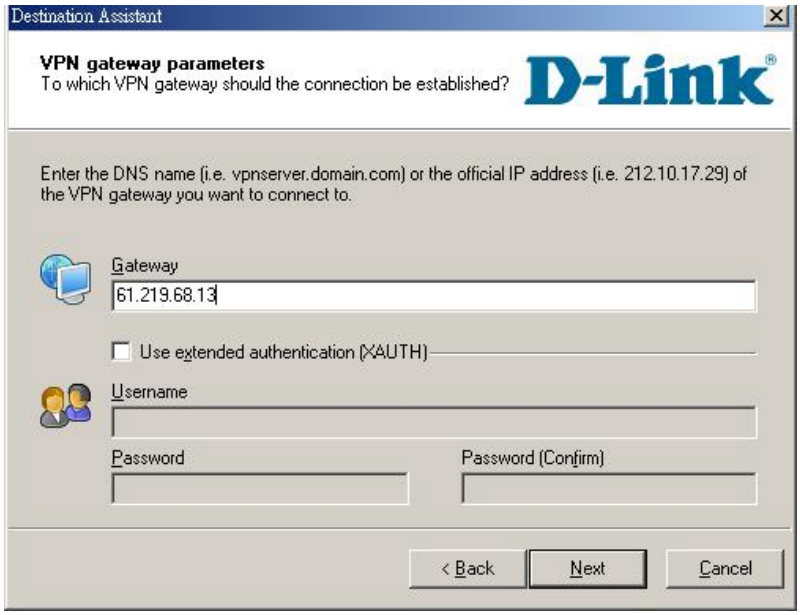
Шаг 2

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



Шаг 3

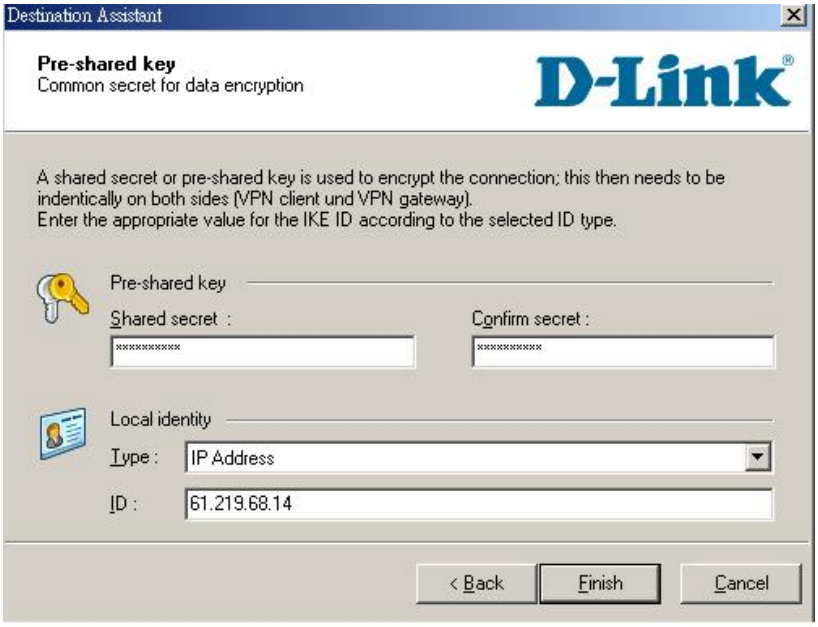
Введите адрес шлюза VPN (**61.219.68.13**) и нажмите кнопку **Next**



Шаг 4

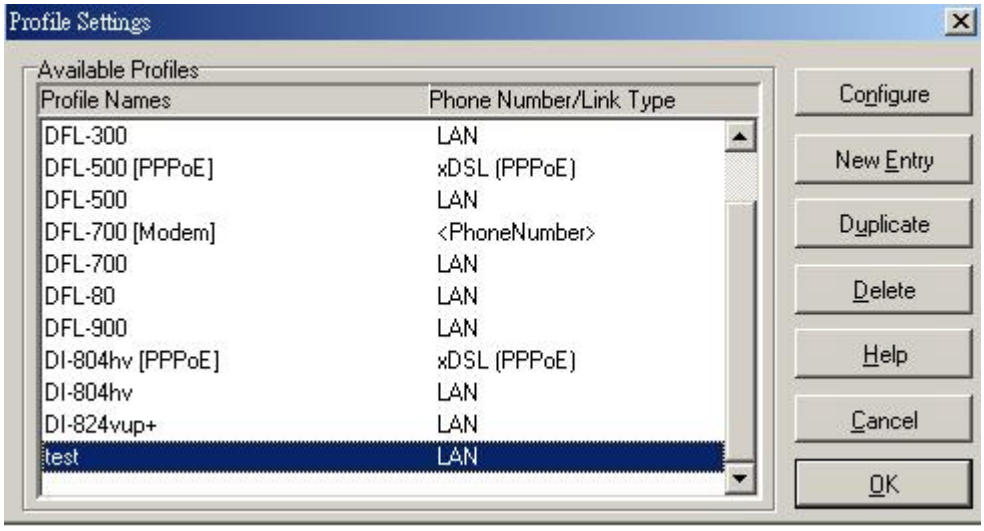
Введите ключ 1234567890 в поле **Shared secret** и затем повторно введите его в поле **Confirm secret.**

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



Шаг 5

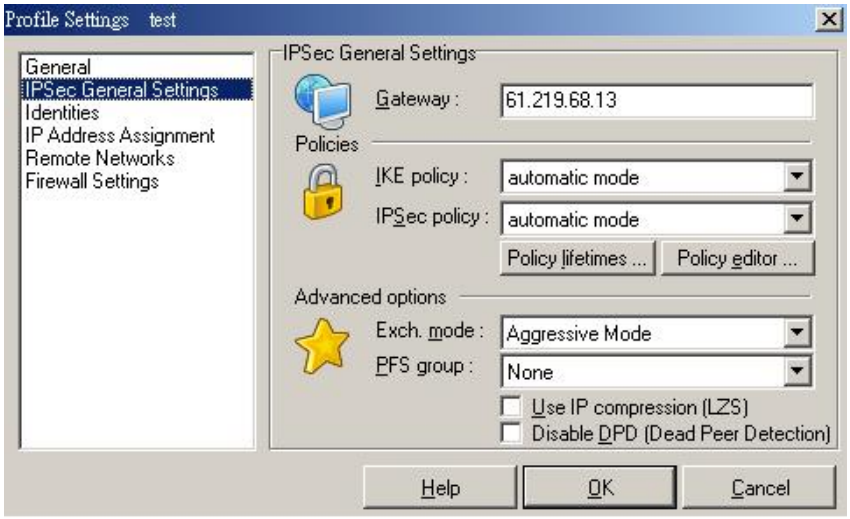
По завершении настройки параметров Вы увидите, что был добавлен новый профиль.

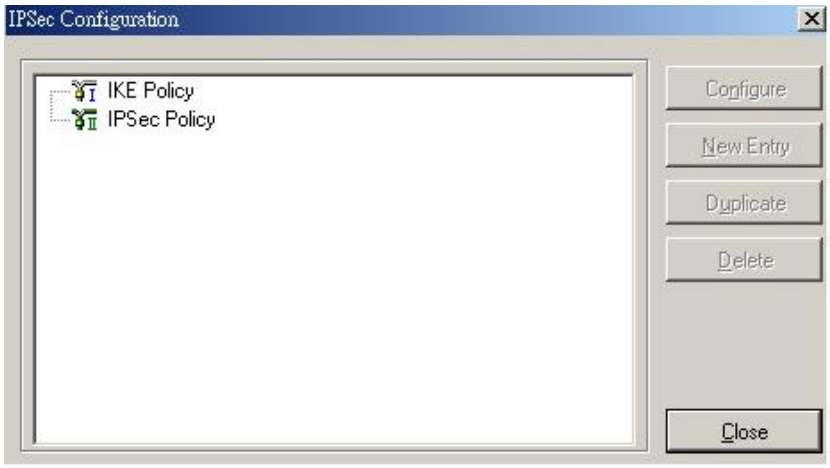


Шаг 6

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

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

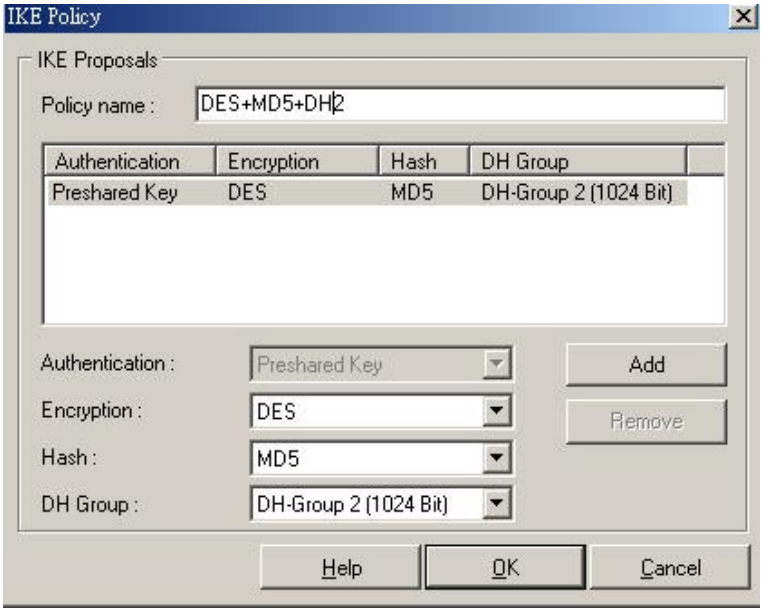




Шаг 7

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

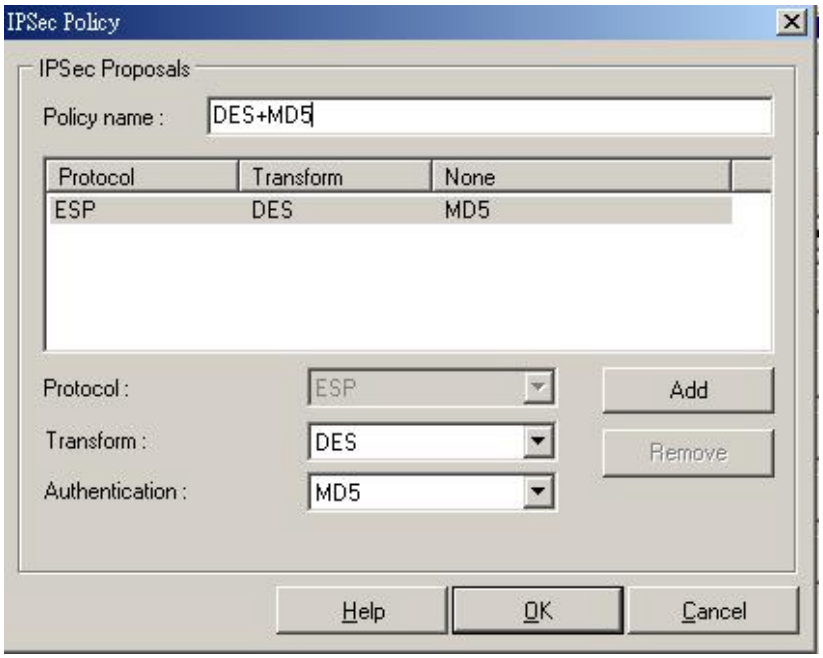
Выберите DES в качестве алгоритма шифрования в поле **Encryption**, MD5 в качестве алгоритма хеширования в поле **Hash**, DH2 в качестве группы ключей в поле **DH group** и нажмите кнопку **OK**.



Шаг 8

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

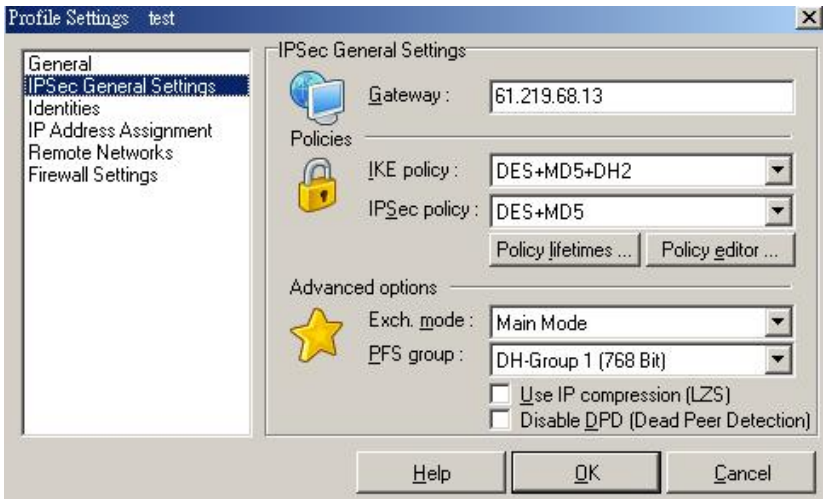
Выберите DES в качестве алгоритма шифрования в поле **Transform**, MD5 в качестве алгоритма аутентификации в поле **Authentication** и нажмите кнопку OK.



Шаг 9

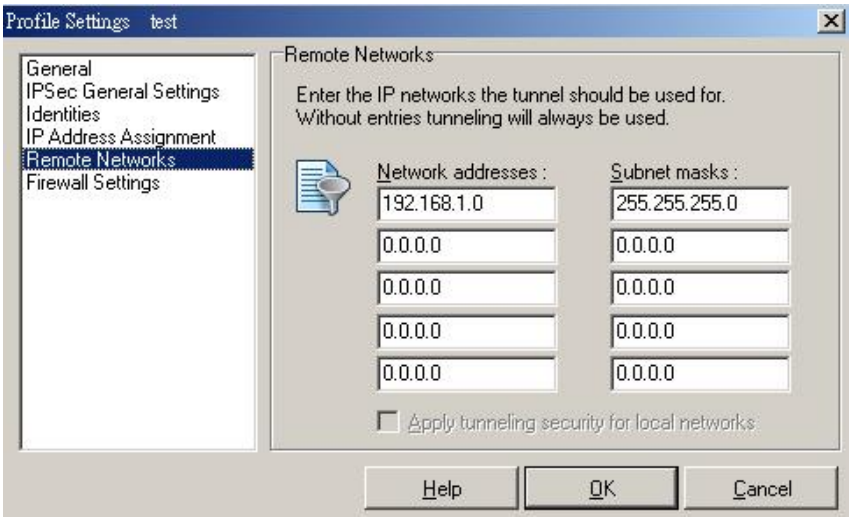
Configuration->Profile settings->test->IPSec General Settings

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**



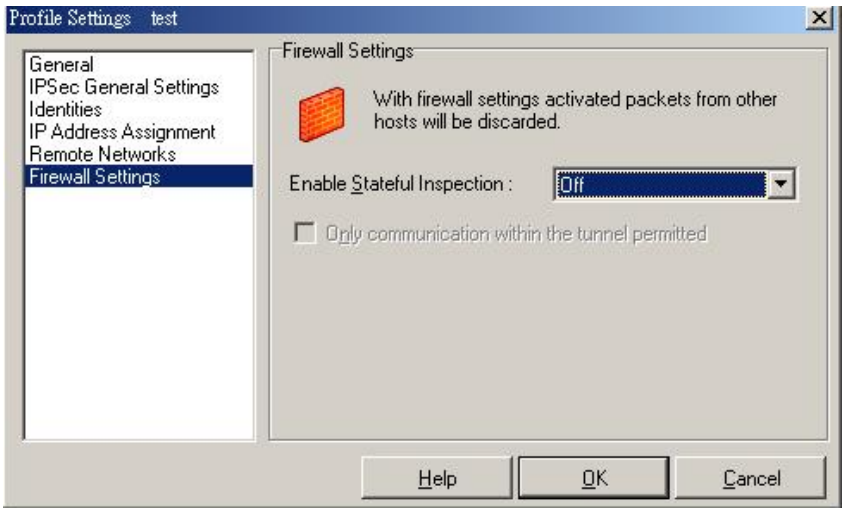
Шаг 10

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**.



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

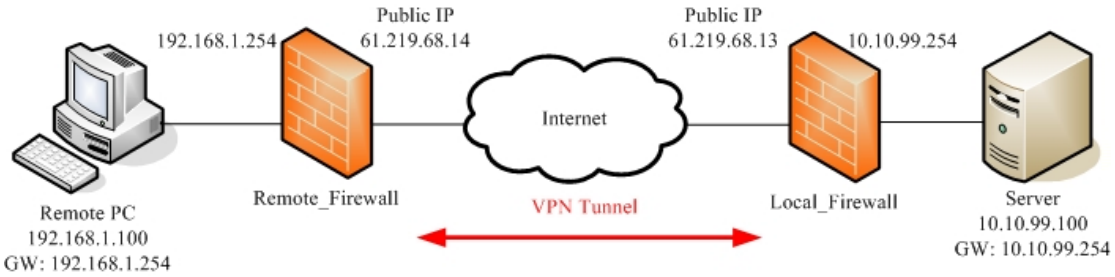
2. Туннель между двумя сетями (LAN to LAN).

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



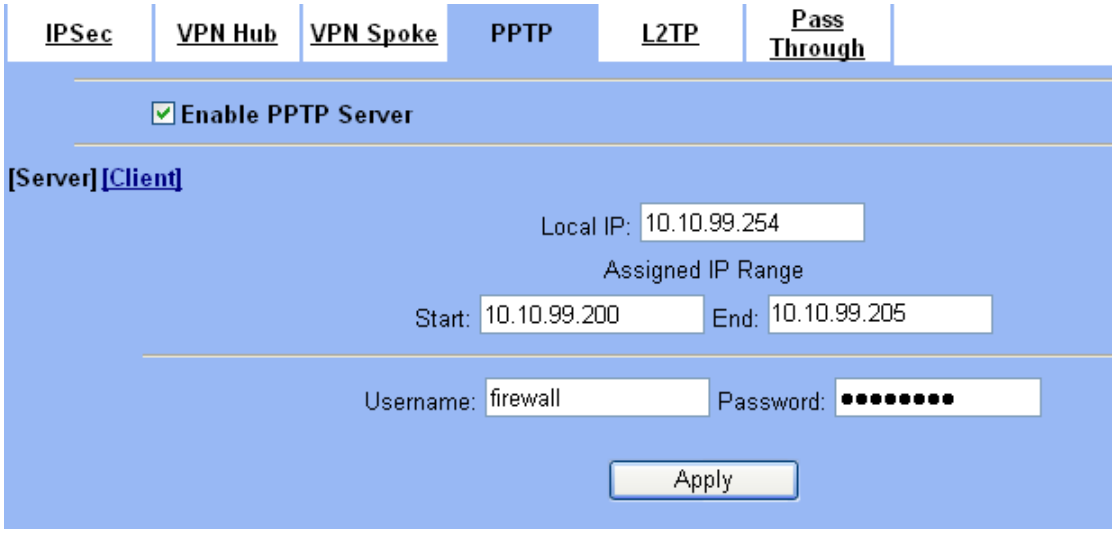
2-3 Параметры настройки:

2-3-1 Сервер PPTP и клиент PPTP

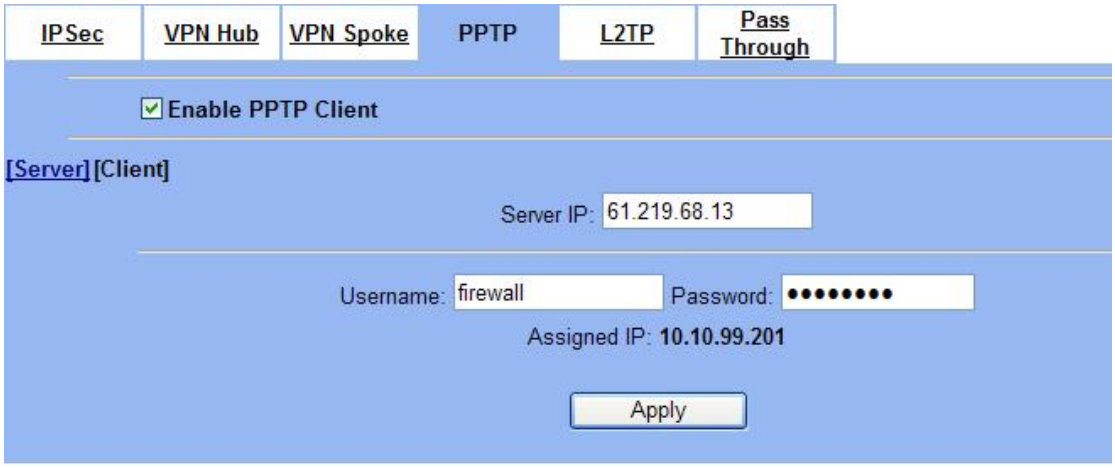
Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана
1- Включить клиент PPTP 2- IP-адрес сервера: 61.219.68.13 3- Имя пользователя: firewall 4- Пароль: firewall	1- Включить сервер PPTP 2- Локальный IP-адрес: 10.10.99.254 3- Диапазон IP-адресов: 10.10.99.200-205 4- Имя пользователя: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

DFL-1500

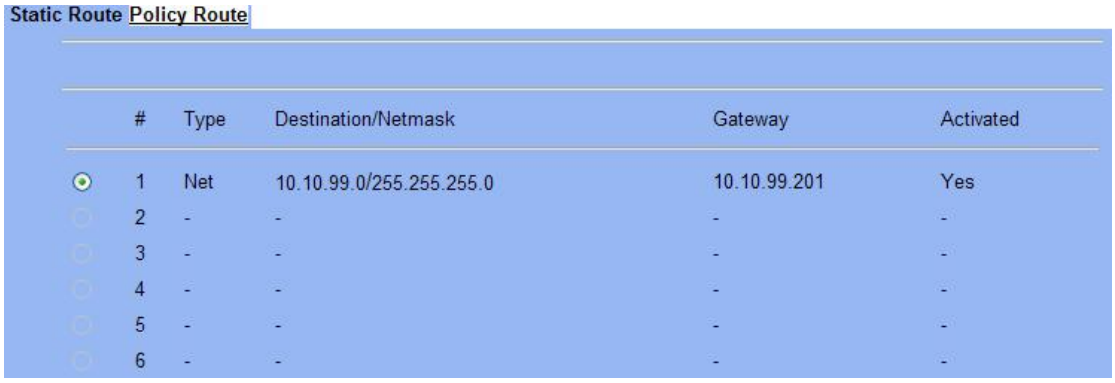
1- Включить сервер PPTP (**Advanced settings -> VPN settings -> PPTP**)



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



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



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

DFL-1100/700/200

1- Добавить пользователя (**Firewall -> Users**)

User Management

Add new user:

User name: firewall

Group membership:

Password: ********

Retype password: ********

L2TP/PPTP settings:

Static client IP:

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

Networks behind user: 192.168.1.0/24

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: 10.10.99.200 - 10.10.99.205

☑ Proxy ARP dynamically added routes

Primary DNS: (Optional)

Secondary DNS: (Optional)

☑ Use unit's own DNS relayer addresses

Primary WINS: (Optional)

Secondary WINS: (Optional)

3- Включить сервер PPTP (**Firewall -> VPN**)

L2TP/PPTP Clients

Add **PPTP** Client :

Name: pptp-client

Basic settings:

Username: firewall

Password: ********

Retype Password: ********

Interface IP: Blank = get IP from server

Remote Gateway: 61.219.68.13

Remote Net: 10.10.99.0/24

☑ Use primary DNS server from tunnel as primary DNS

☐ Use secondary DNS server from tunnel as secondary DNS

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

2-3-2 Сервер L2TP и клиент L2TP

Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана

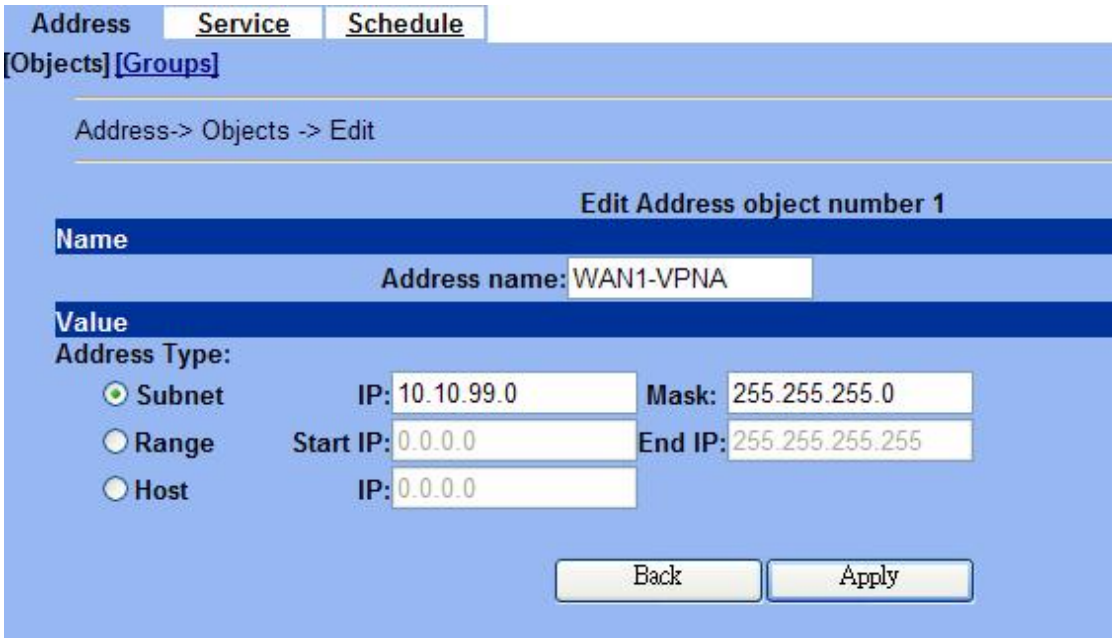
2-3-3 IPSec

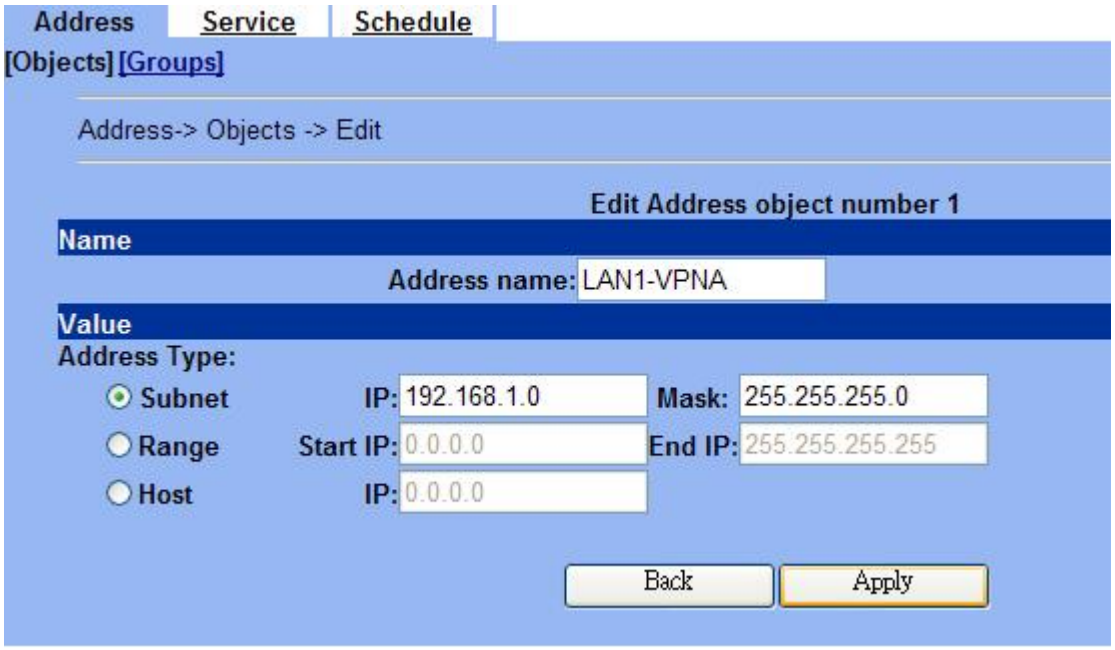
Настройки удаленного межсетевого экрана	Настройки локального межсетевого экрана
1- Включить IPSec	1- Включить IPSec
2- Локальный IP-адрес: 192.168.1.0/24	2- Локальный IP-адрес: 10.10.99.0/24
3- Удаленный IP-адрес: 10.10.99.0/24	3- Удаленный IP-адрес: 192.168.1.0/24
4- Режим согласования: Main mode	4- 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

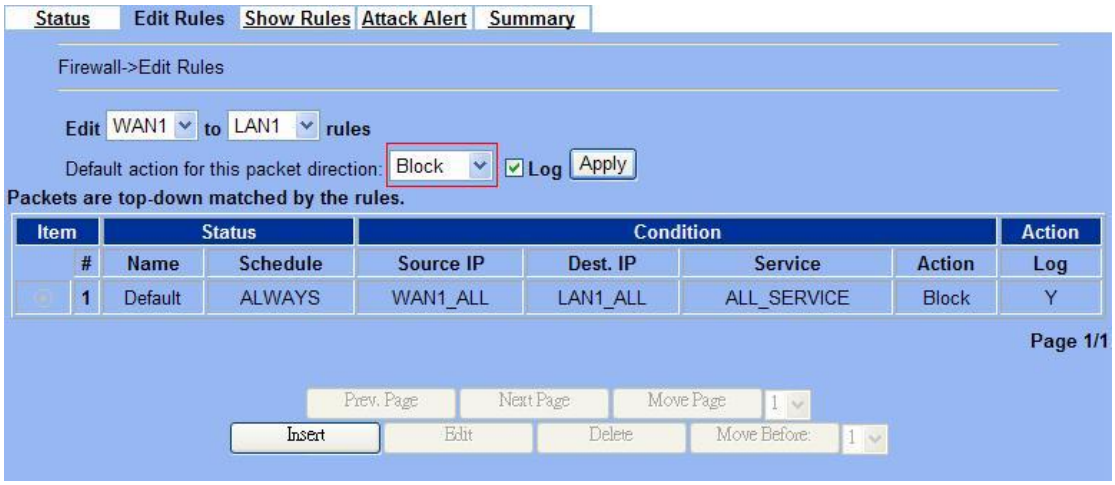
Удаленный межсетевой экран:

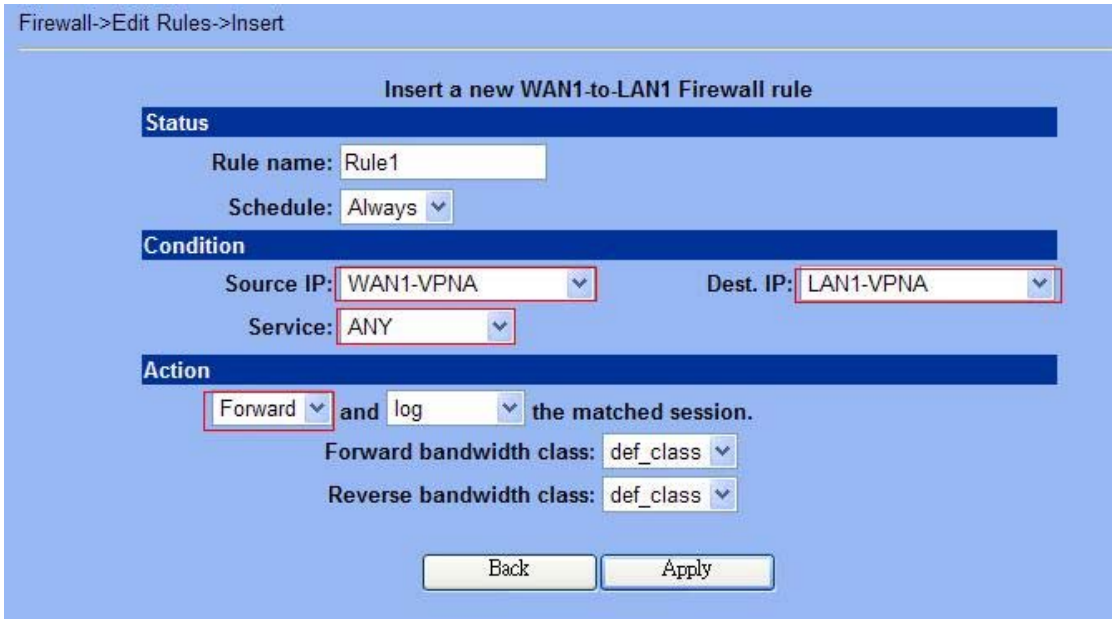
01- Добавить адреса (**Basic -> Books**)



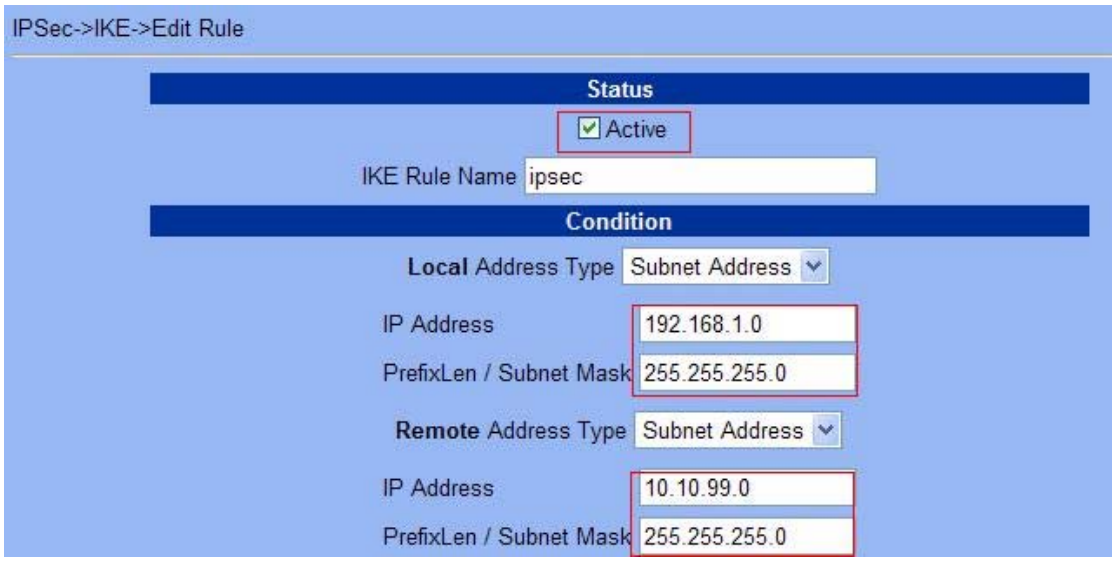


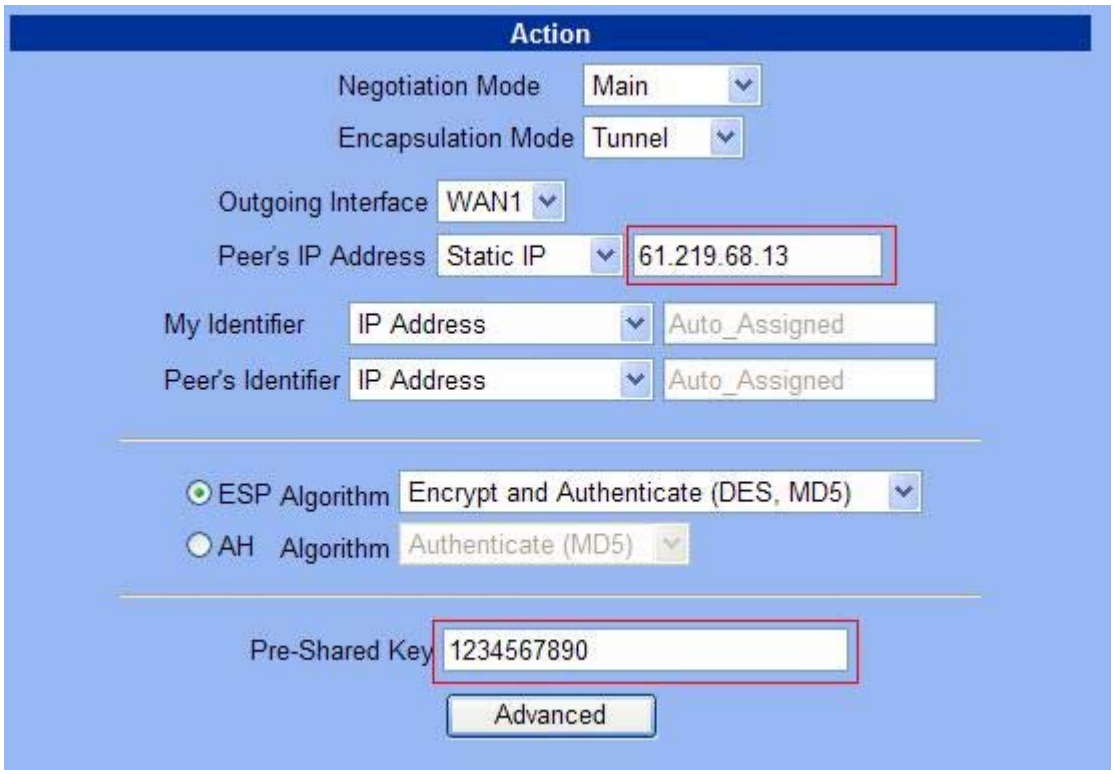
02- Отредактировать правила межсетевого экран (**Advanced Settings -> Firewall -> Edit Rules**)

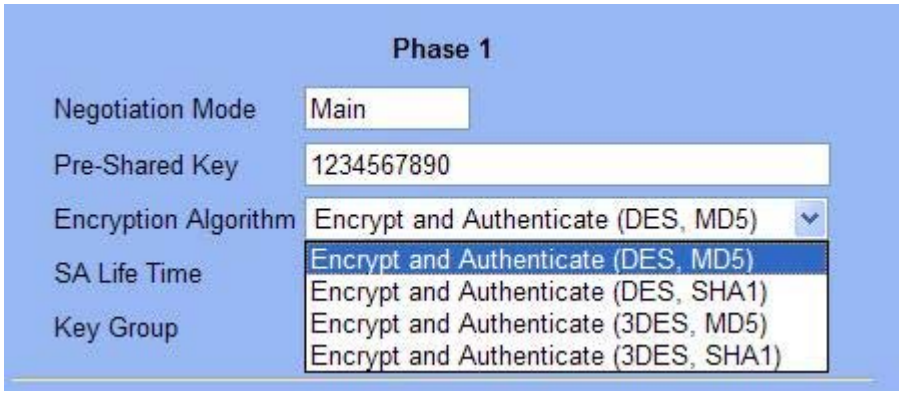


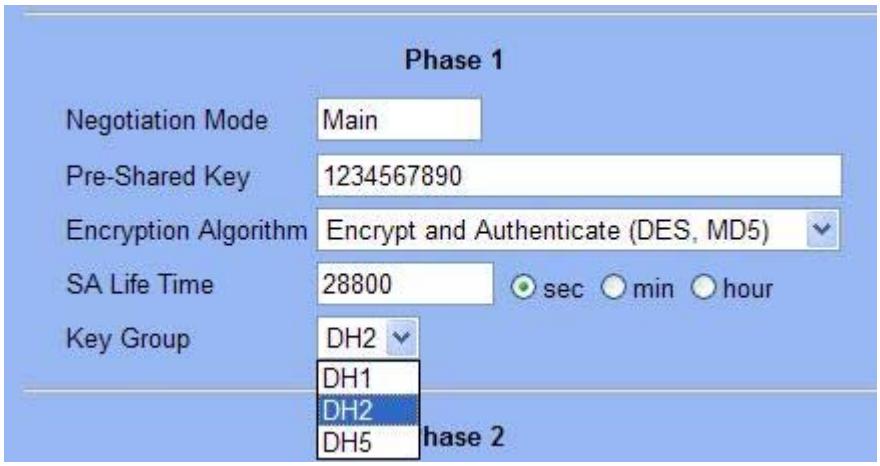


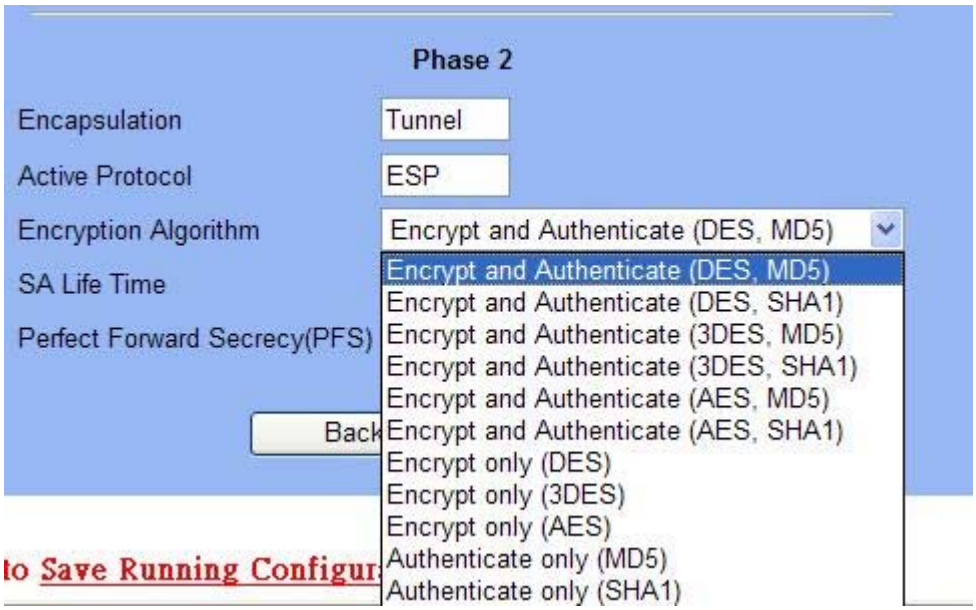
03- Включить IPSec и отредактировать политику IPSec (**Advanced Settings -> VPN Settings**)

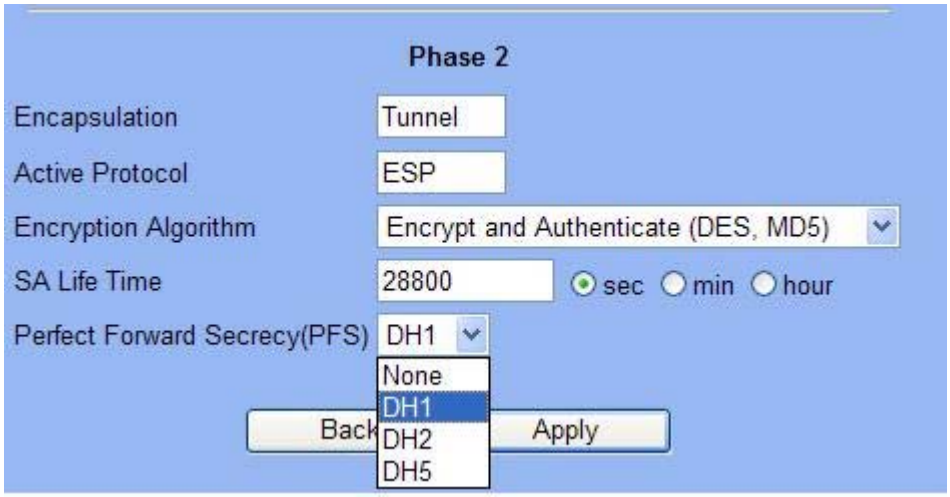





Phase 1
Negotiation Mode
Main
Pre-Shared Key
1234567890
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
Key Group
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)

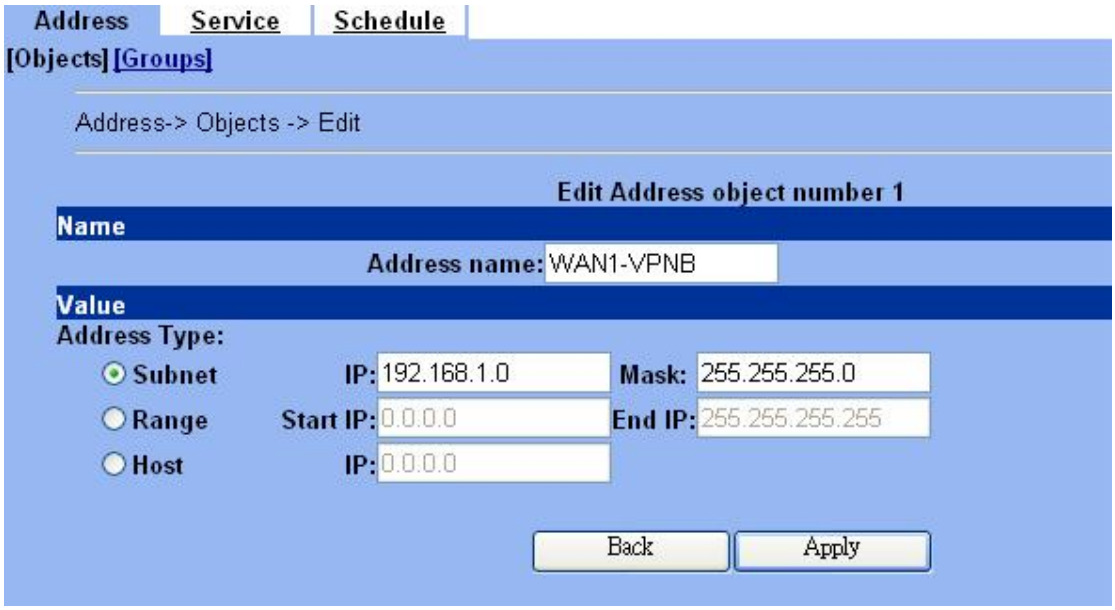

Phase 1
Negotiation Mode
Main
Pre-Shared Key
1234567890
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Key Group
DH2
DH1
DH2
DH5
hase 2

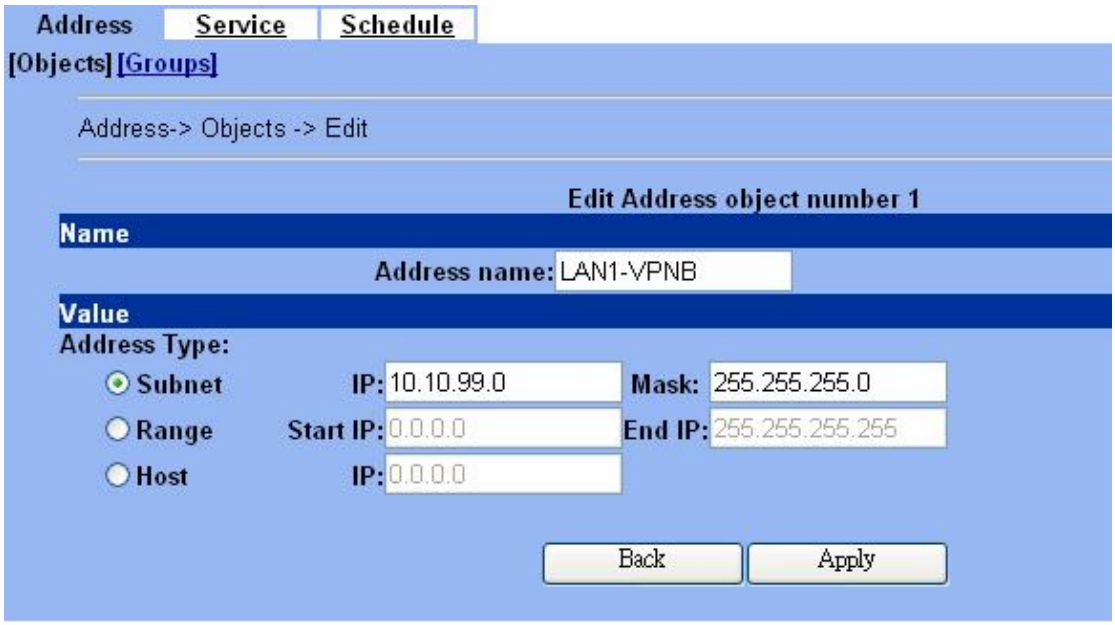

Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
Perfect Forward Secrecy(PFS)
Back
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)
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



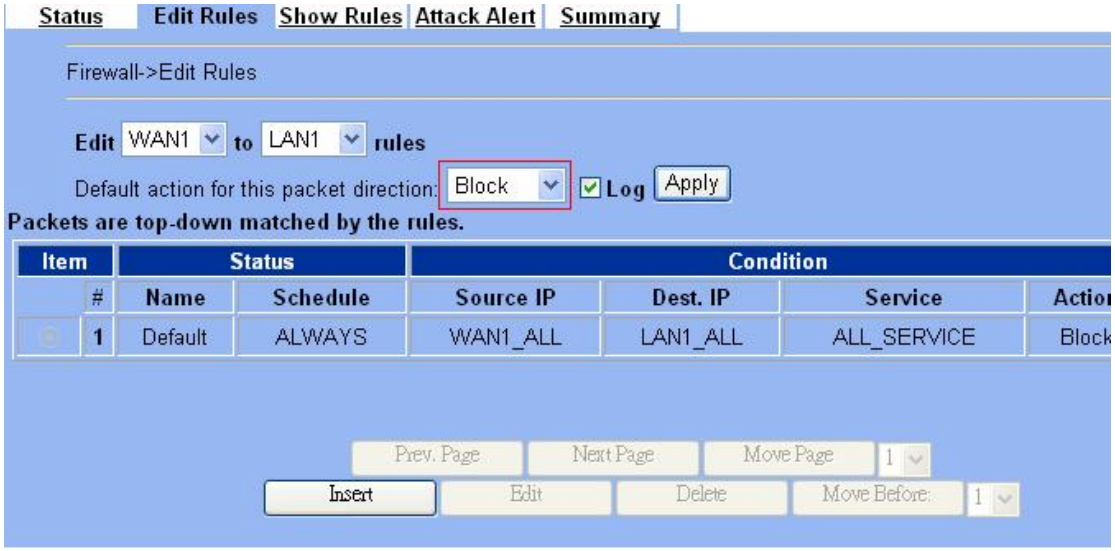
Локальный межсетевой экран:

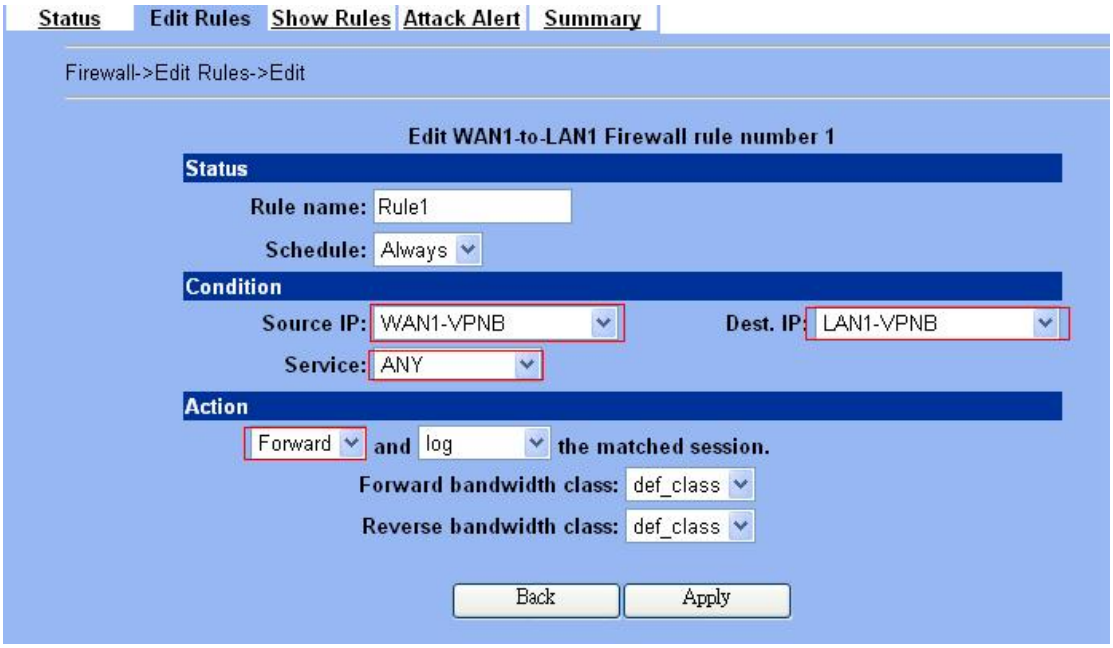
01- Добавить адреса (**Basic -> Books**)



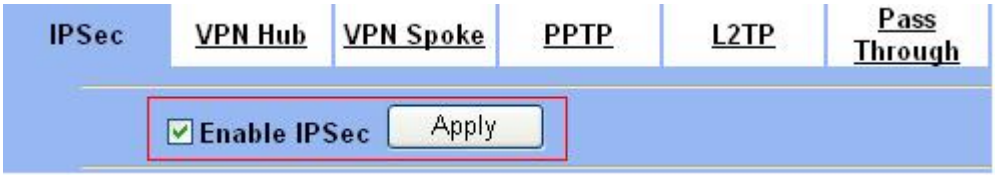


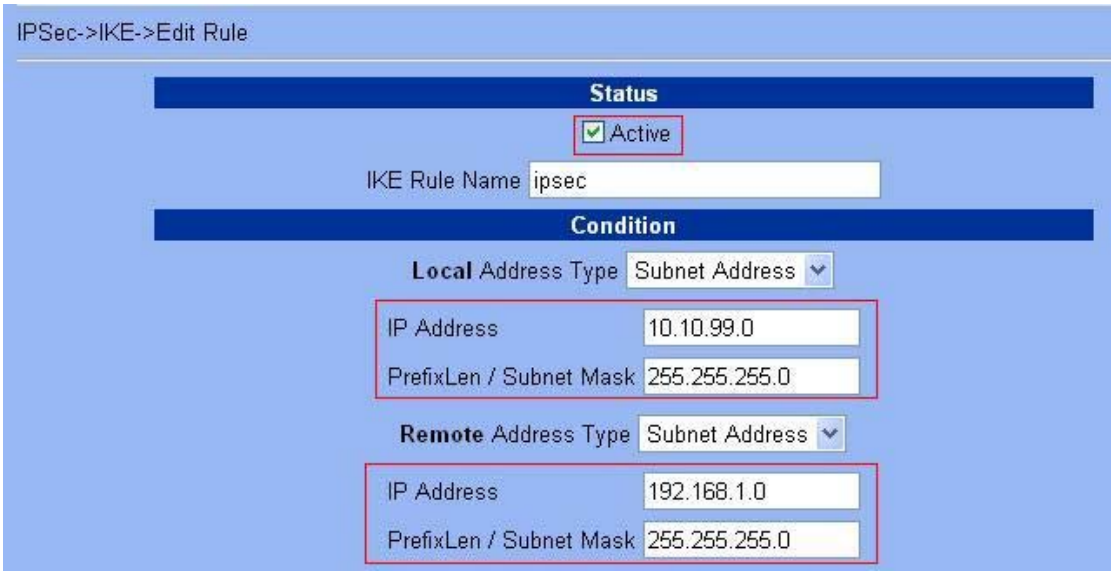
02- Отредактировать правила межсетевого экрана (**Advanced Settings -> Firewall -> Edit Rules**)





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





Action

Negotiation Mode: Main
Encapsulation Mode: Tunnel
Outgoing Interface: WAN1
Peer's IP Address: Static IP 61.219.68.14
My Identifier: IP Address Auto_Assigned
Peer's Identifier: IP Address Auto_Assigned

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

Pre-Shared Key: 1234567890
Advanced
Back Apply

Phase 1

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

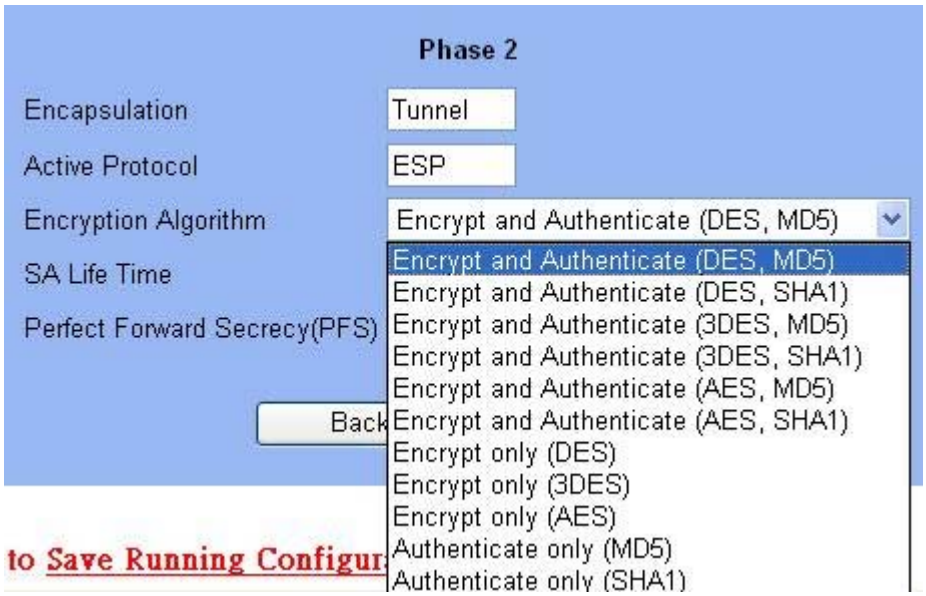
- Encrypt and Authenticate (DES, MD5)
- Encrypt and Authenticate (DES, SHA1)
- Encrypt and Authenticate (3DES, MD5)
- Encrypt and Authenticate (3DES, SHA1)

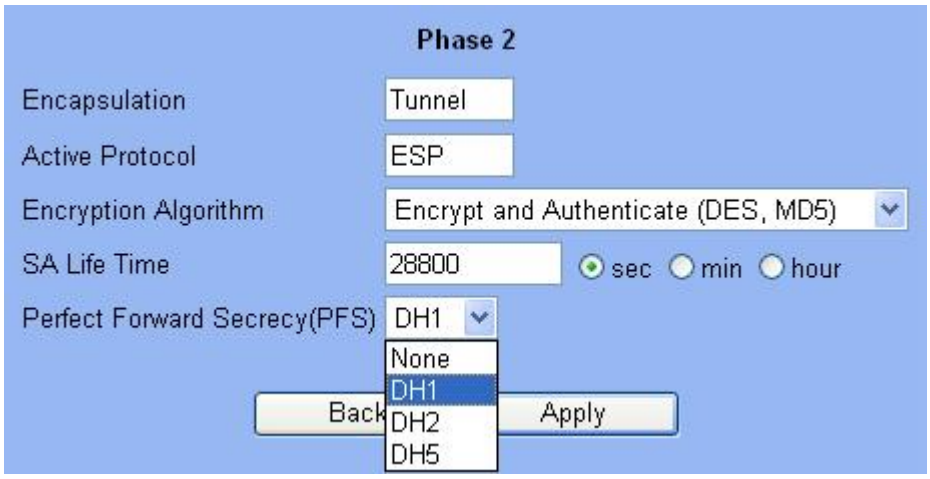
Phase 1

Negotiation Mode: Main
Pre-Shared Key: 1234567890
Encryption Algorithm: Encrypt and Authenticate (DES, MD5)
SA Life Time: 28800 sec min hour
Key Group: DH2

- DH1
- DH2
- DH5

hase 2

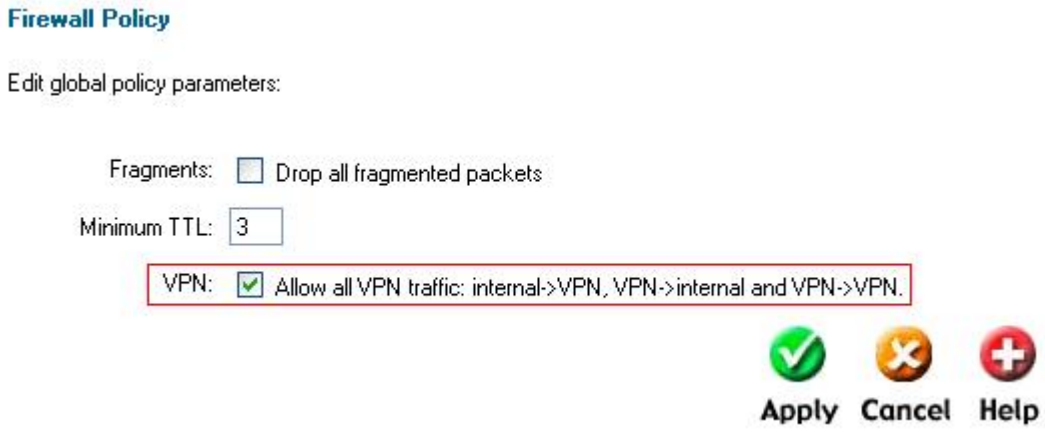

Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
Perfect Forward Secrecy(PFS)
Encrypt and Authenticate (DES, MD5)
Encrypt and Authenticate (DES, SHA1)
Encrypt and Authenticate (3DES, MD5)
Encrypt and Authenticate (3DES, SHA1)
Encrypt and Authenticate (AES, MD5)
Encrypt and Authenticate (AES, SHA1)
Encrypt only (DES)
Encrypt only (3DES)
Encrypt only (AES)
Authenticate only (MD5)
Authenticate only (SHA1)
Back
to Save Running Configur


Phase 2
Encapsulation
Tunnel
Active Protocol
ESP
Encryption Algorithm
Encrypt and Authenticate (DES, MD5)
SA Life Time
28800
sec
min
hour
Perfect Forward Secrecy(PFS)
DH1
None
DH1
DH2
DH5
Back
Apply

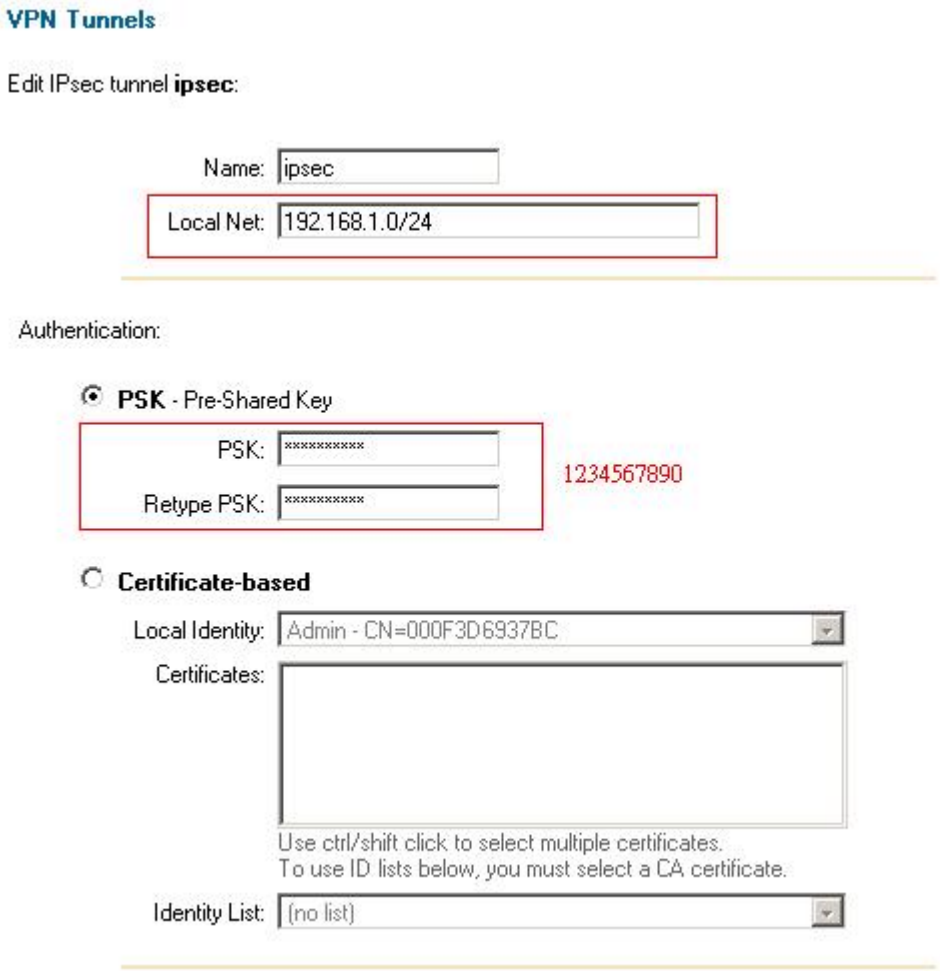
DFL-1100/700/200

Удаленный межсетевой экран:

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



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



Tunnel type:

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

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

◉ **LAN-to-LAN tunnel**

Remote Net: 10.10.99.0/24

Remote Gateway: 61.219.68.13

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

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

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: ☐ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

VPN Tunnels

Edit advanced settings of IPsec tunnel **ipsec**:

Limit MTU: 1424

IKE Mode: ◉ Main mode IKE
○ Aggressive mode IKE

IKE DH Group: 2 - modp 1024-bit

PFS: ☑ Enable Perfect Forward Secrecy

PFS DH Group: 1 - modp 768-bit

NAT Traversal: ○ Disabled.
◉ On if supported and needed (NAT detected between gateways)
○ On if supported

Keepalives: ◉ No keepalives.
○ Automatic keepalives (works with other DFL-200/700/1100 units)
○ Manually configured keepalives:

Source IP:

Destination IP:

IKE Proposal List

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

Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

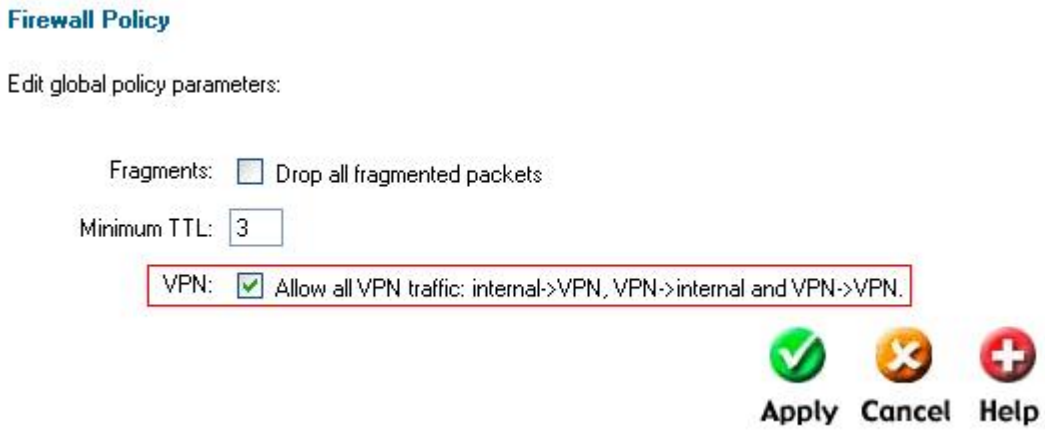
IPsec Proposal List

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

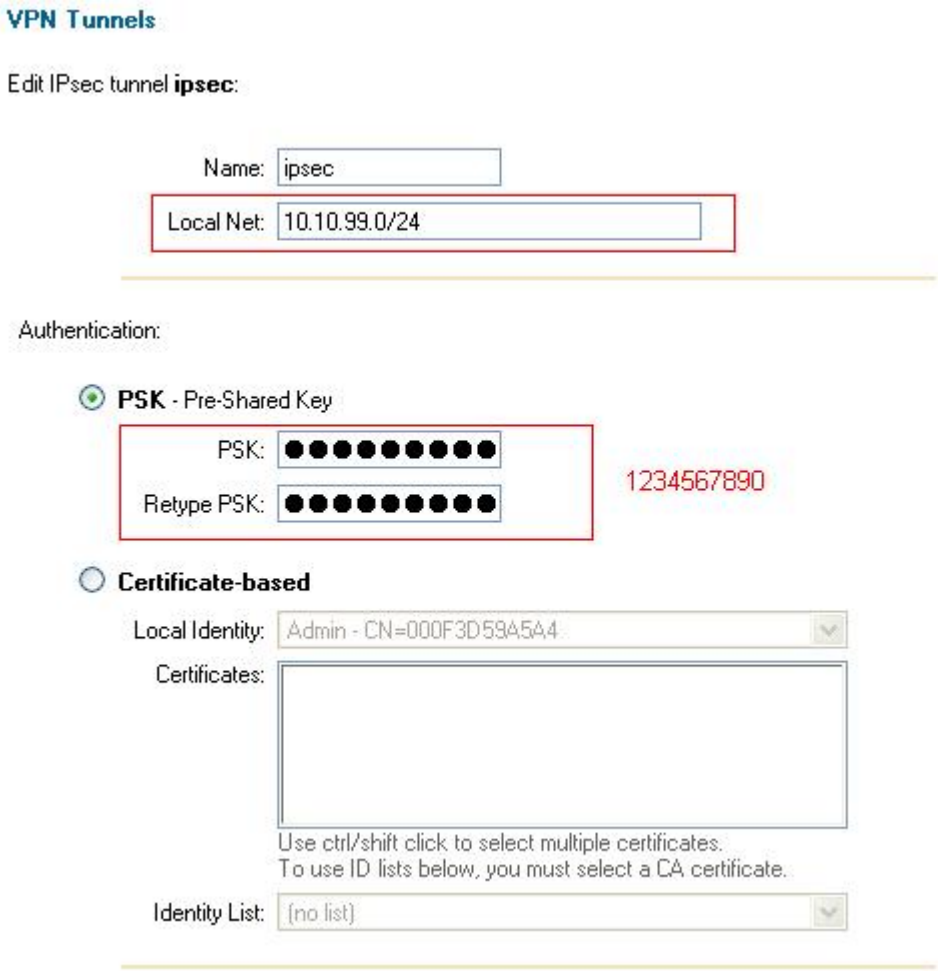
Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448

Локальный межсетевой экран:

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



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



Tunnel type:

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

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

◉ **LAN-to-LAN tunnel**

Remote Net: 192.168.1.0/24

Remote Gateway: 61.219.68.14

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

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

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: ☐ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

VPN Tunnels

Edit advanced settings of IPsec tunnel **ipsec**:

Limit MTU: 1424

IKE Mode: ◉ Main mode IKE
○ Aggressive mode IKE

IKE DH Group: 2 - modp 1024-bit

PFS: ☑ Enable Perfect Forward Secrecy

PFS DH Group: 1 - modp 768-bit

NAT Traversal: ○ Disabled.
◉ On if supported and needed (NAT detected between gateways)
○ On if supported

Keepalives: ◉ No keepalives.
○ Automatic keepalives (works with other DFL-200/700/1100 units)
○ Manually configured keepalives:

Source IP:

Destination IP:

IKE Proposal List

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

Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448
Blowfish-448 Allowed:448-448
-
Twofish-128 Allowed:128-256
Twofish-256 Allowed:128-256
Twofish-256 Allowed:256-256
-
AES-128 Allowed:128-256
AES-256 Allowed:128-256
AES-256 Allowed:256-256

IPsec

	HMAC	Life KB	Life Sec
#1:	MD5	0	3600

IPsec Proposal List

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

Blowfish-256 Allowed:128-448
Blowfish-256 Allowed:256-448
Blowfish-448 Allowed:256-448
Blowfish-448 Allowed:448-448
-
Twofish-128 Allowed:128-256
Twofish-256 Allowed:128-256
Twofish-256 Allowed:256-256
-
AES-128 Allowed:128-256
AES-256 Allowed:128-256
AES-256 Allowed:256-256

"AES- his unit will propose 128 bit encryption to the rem
establi ccept any cipher key sizes between 128 and 2
receiv

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

Phase 1 Proposal

Name	P1Param	
DH Group	Group 2	
IKE Life Duration	6000	seconds
IKE Encryption	DES	
IKE Hash	MD5	

Phase 2 Proposal

Name	P2Param
PFS Mode	Group 1
Encapsulation	ESP
IPSec Life Duration	6000 seconds
ESP Transform	DES
ESP Auth	HMAC-MD5
AH Transform	MD5

Click here to add P1 proposal

P1 Proposals	P1Param	NOT_SET
	NOT_SET	NOT_SET

Click here to add P2 proposal

P2 Proposals	P2Param	NOT_SET
	NOT_SET	NOT_SET

Target Host Range

Starting Target Host	10.10.99.0
Subnet Mask	255.255.255.0

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	◉ Allow all except policy settings
○ 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 / Tunnel Settings / Tunnel Table / IPSec Status

Add/New Tunnel

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

Phase 1 Proposal

Name	P1Param	
DH Group	Group 2	
IKE Life Duration	6000	seconds
IKE Encryption	DES	
IKE Hash	MD5	

Phase 2 Proposal

Name	P2Param
PFS Mode	Group 1
Encapsulation	ESP
IPSec Life Duration	6000 seconds
ESP Transform	DES
ESP Auth	HMAC-MD5
AH Transform	MD5

Click here to add P1 proposal

P1 Proposals	P1Param	NOT_SET
	NOT_SET	NOT_SET

Click here to add P2 proposal

P2 Proposals	P2Param	NOT_SET
	NOT_SET	NOT_SET

Target Host Range

Starting Target Host	192.168.1.0
Subnet Mask	255.255.255.0