

D-Link VPN Application Quick Installation Guide

Contents

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

1. Remote Access

1-1 Objective:

Someone is out off office and need to connect back to company by using VPN function (PPTP/L2TP/IPSec).

1-2 Environment:

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



1-3 Setup

1-3-1 PPTP Server

Remote PC settings	Firewall settings
01-Remote IP address: 61.219.68.13	01-Enable PPTP Server
02-VPN type: PPTP	02-Local IP address: 192.168.1.254
03-Username: firewall	03-IP pool: 192.168.1.100~105
04-Password: firewall	04-Username: firewall
	05-Password: firewall

Device setting page

DFL-1500

01- Enable PPTP Server (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	PTP Server				
[Server] [<u>Clic</u>	ent]					
			Local	IP: 192.168. Assigned IP	1.254 Range	
		Star	t: 192.168.1.1	100 Ei	nd: 192.168.1.105	
		Username	e: firewall	Pa	assword: *******	
				Apply		

DFL-1100/700/200

ser Managemei	it	
dd new user:		
User	name: firewall	
Group memb	ership:	
Pas	sword: ******	
Retype pas	sword:	

02- Enable PPTP Server (Firewall -> VPN)

L2TP/PPTP Servers

Edit PPTP tunnel PPTP-Server:

Name:	PPTP-Server	
Outer IP:	[Blank = WAN IP
Inner IP:	Must be WAN IP i	f IPsec encryption is require Blank = LAN IP
Pool and setting	s:	
Client IP Pool:	192.168.1.100 - 1	92.168.1.105
1	Proxy ARP dy	namically added routes
Primary DNS:		(Optional)
Secondary DNS:	<u> </u>	(Optional)
	🗹 Use unit's owr	n DNS relayer addresses
Primary WINS:		(Optional)
Secondary WINS:	[(Optional)

DFL-600

01- Add User (Advanced -> VPN-PPTP -> PPTP Account)

PPTP Settings / PPTP Account / PPTP Status

Add/New User Account

User Name	firewall
Password	*****
Confirm Password	******

02- Enable PPTP Server (Advanced -> VPN-PPTP -> PPTP settings)

PPTP Settings / PPTP Account / PPTP Status

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

Configuring PPTP Client (Microsoft XP PRO's VPN adapter) Setup1

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



Setup2

Click Next to the next step.

New Connection Wizard		
5A	Welcome to the New Connection Wizard	
	This wizard helps you:	
19	Connect to the Internet.	
VA C	 Connect to a private network, such as your workplace network. 	
I OT AS	 Set up a home or small office network. 	
	To continue, click Next.	
	< Back Next > Cancel	

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

New Connection Wizard	
Network Connection Type What do you want to do?	
Connect to the Internet Connect to the Internet so you can browse the Web and read email.	
Connect to the network at my workplace Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.	
 Set up a home or small office network Connect to an existing home or small office network or set up a new one. Set up an advanced connection Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it. 	
< Back Next > Cancel	

Steup4

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



Step5

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

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>

Step6

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

lew 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

Step7

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

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

Step8

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

Connect PPT	Р 🛛 🔀
User name:	firewall
Password:	•••••
Save this u	iser name and password for the following users:

1-3-2 L2TP without IPSec

Remote PC settings	Firewall settings

For example: DFL-1500 with Microsoft's VPN adapter (Windows 2K)

1-3-3 IPSec

Remote PC settings	Firewall settings
01- Profile name: test	01- Rule Name: IPSec
02- Communication media: LAN over IP	02- Local IP address: 192.168.1.0/24
03- Gateway: 61.219.68.13	03- Remote IP address: 61.219.68.14
04- IKE policy: DES+MD5	04- Negotiation mode: Main
05- IKE key group: DH2	05- Encapsulation mode: Tunnel
06- IPSec policy: DES+MD5 (ESP)	06- Peers's IP address: 61.219.68.14
07- IPSec key group: DH1	07- PSK: 1234567890
08- Exch_mode: Main	08- IKE policy: DES+MD5
09- Local identity: IP address	09- IKE key group: DH2
10- ID: 61.219.68.14	10- IPSec policy: DES+MD5 (ESP)
11- PSK: 1234567890	11- IPSec key group: DH1
12- Remote Networks: 192.168.1.0/24	
13- Disable firewall settings	

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

WAN1:

Address-> Objects -	-> Edit				
	Edit Addre	ss object numb	er 1		
ıme					
	Address name: Remote	and the second second			
Idress Type:					
Subnet	IP: 61.219.68.0 Mask:	255.255.255.0			
⊖ Range S	Start IP: 0.0.0.0 End IP	255.255.255.2	55		
OHost	IP: 0.0.0.0				
	Back	Apply			
:					
tress Serv	vice Schedule				
dress <u>Serv</u>	rice Schedule				
dress <u>Serv</u> cts][<u>Groups]</u>	<u>rice</u> Schedule				
: dress <u>Serv</u> cts][<u>Groups]</u> Address-> Obje	<u>rice</u> <u>Schedule</u> ects -> Edit				
: dress <u>Serv</u> cts][<u>Groups]</u> Address-> Obje	<u>rice</u> <u>Schedule</u> ects -> Edit		100000 10		
t ress <u>Serv</u> cts][<u>Groups]</u> Address-> Obje	<u>rice</u> <u>Schedule</u> ects -> Edit	Edit Address	s object nur	nber 1	
dress <u>Serv</u> cts][Groups] Address-> Obje ame	<u>vice</u> <u>Schedule</u> ects -> Edit	Edit Address	s object nur	nber 1	
dress <u>Serv</u> cts] [Groups] Address-> Obje ame	<u>vice</u> <u>Schedule</u> ects -> Edit Address name: L	Edit Address _AN1	s object nur	nber 1	
dress <u>Serv</u> cts] [<u>Groups]</u> Address-> Obje ame	<u>vice</u> <u>Schedule</u> ects -> Edit Address name: L	Edit Address _AN1	s object nur	nber 1	
dress <u>Serv</u> cts][<u>Groups</u>] Address-> Obje ame ame ddress Type:	vice <u>Schedule</u> ects -> Edit Address name: L	Edit Address _AN1	s object nur	nber 1	
dress <u>Serv</u> cts] [Groups] Address-> Obje ame ame ddress Type: ③ Subnet	vice <u>Schedule</u> ects -> Edit Address name: L IP: 192.168.1.0	Edit Address AN1 Mask:	s object nur 255.255.255	nber 1	
dress <u>Serv</u> cts] [Groups] Address-> Obje ame alue ddress Type: ③ Subnet ③ Range	vice <u>Schedule</u> ects -> Edit Address name: L IP: 192.168.1.0 Start IP: 0.0.0.0	Edit Address AN1 Mask: End IP:	s object nur 255.255.255 255.255.255	nber 1 5.0	
dress <u>Serv</u> cts] [Groups] Address-> Obje ame alue ddress Type: ③ Subnet ③ Range ④ Host	<u>vice</u> <u>Schedule</u> ects -> Edit Address name: L IP: 192.168.1.0 Start IP: 0.0.0.0 IP: 0.0.0.0	Edit Address AN1 Mask: End IP:	s object nur 255.255.255 255.255.255	nber 1 5.0	
dress <u>Serv</u> ects] [<u>Groups]</u> Address-> Obje lame /alue uddress Type: ③ Subnet ③ Range ④ Host	vice <u>Schedule</u> ects -> Edit Address name: L IP: 192.168.1.0 Start IP: 0.0.0.0 IP: 0.0.0.0	Edit Address AN1 Mask: End IP:	s object nur 255.255.255 255.255.255	nber 1	

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

Status Edit Rules Show Rules Attack Alert Summary Firewall->Edit Rules Edit WAN1 v to LAN1 v rules Default action for this packet direction: Block Log Apply Packets are top-down matched by the rules. Item Status Condition Name Schedule Source IP Dest. IP Service Action # 1 Default ALWAYS WAN1_ALL LAN1_ALL ALL_SERVICE Block Prev. Page Next Page Insert Delete 1 4 Firewall->Edit Rules->Insert

Rule name:	Rule1		
Schedule:	Always 💌		
Condition			
Source IP:	Remote	~	Dest. IP: LAN1
Service:	ANY 💌		
Action			
Forward 🛩	and log 🛛 🝸 t	he matched se	ssion.
F	orward bandwidth	class: def_class	•
	everse bandwidth	class: def class	*

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

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

IPSec->IKE->Edit Rule			
	Stat	us	
	⊠ Ad	tive	
	IKE Rule Name ipsec		
	Cond	tion	
	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		
Ν	legotiation Mode Mai	n 🗸	
E	ncapsulation Mode Tun	nel 🗸	
Outacing In	torface WAN1 w		
		C4 040 C0 44	-
Peers IP A	ddress Static IP	61.219.68.14	
My Identifier	IP Address	Auto_Assigned	
Peer's Identifier	IP Address	Auto_Assigned	
ESP Algorit	thm Encrypt and Auther	nticate (DES, MD5)	~
	thm Authenticate (MD5)	*	
-			
Pre-Shar	ed Key 1234567890		
	Advanced		
	Auvanced		

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

	F	Phase	1
Negotiation Mode	Main		
Pre-Shared Key	123456	7 <mark>890</mark>	
Encryption Algorithm	Encrypt	t and A	uthenticate (DES, MD5)
SA Life Time	28800		⊙sec ○min ○hour
Key Group	DH2 🗸		
	DH1		
	DH2	hase	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)
Perfect Forward Secrecy(PFS)	Encrypt and Authenticate (3DES, MD5) Encrypt and Authenticate (3DES, SHA1)
Bacl	Encrypt and Authenticate (AES, MD5) Encrypt and Authenticate (AES, SHA1) Encrypt only (DES)
	Encrypt only (3DES)
to <u>Save Running Configu</u>	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 💌	
Back	None DH1 DH2 DH5	Apply

DFL-1100/700/200

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

Firewall Policy

Edit global policy parameters:

Fragme	ents:	Drop all fragmented packets		
Minimum T	TTL:	3		
V	PN:	Allow all VPN traffic: internal->VPN, VPN->internal and VPN	->VPN.	
		S	8	0
		Apply	Cancel	Help

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

VPN Tunnels

Edit IPsec tunnel ipsec:

Name:	ipsec	
Local Net:	192.168.1.0/24	

Authentication:

PSK:	*****	1024562000
Retype PSK:	1234567890	
ertificate-ba	sed	
Local Identity:	Admin - CN=000F	3D6937BC
	Provide the second se	
Certificates:		
Certificates:	Use ctrl/shift click To use ID lists belo	to select multiple certificates. ow, you must select a CA certificate.

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

Policy Rules / Global Policy Status / Policies

Inbound Port Filter	Outbound Port Filter	
Enabled	Enabled	
 Allow all except policy settings 	 Allow all except policy settings 	
○ Deny all except policy settings	O Deny all except policy settings	

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

IPSec Settings /	Manual Key / Tur	nel 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 Proposa	I	
Name	P1Param	
DH Group	Group 2 💌	
IKE Life Duration	6000	seconds
IKE Encryption	DES 🔽	
IKE Hash	MD5 🐱	
Phase 2 Proposa	I	
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	d P2 proposal	
P2 Proposals	P2Param 💌	NOT_SET 💌
	NOT_SET 💌	NOT_SET 💌
Target Host Rai	nge	
Starting Target Host	61.219.68.0	
Subnet Mask	255.255.255.0	

Configuring IPSec connection (D-Link DS-601) Setup1 Configuration->Profile settings->New Entry Input your profile name and click Next button Destination Assistant **D-Link Connection Name** Enter the name of the connection The connection may be given a descriptive name; enter a name in the following field. Name of the connection test

< Back Next> Cancel

X

Setup2

Select Communication media as LAN over IP and click Next Button

Destination Assistant			×
Link type (Dial up configuration Select the media type of the connection) on.	D-L	ink
Determine how the connection to the to be used via modem, set the commu appropriate modem.	corporate network should nication media to ''moden	be established. If t " and then select	the internet is the
Communication media :	LAN (over IP)		
	<u> </u>	<u>N</u> ext	<u>C</u> ancel

Setup3

Input VPN gateway (61.219.68.13) and click Next button

Destination	Assistant	
VPN g To whic	ateway parameters h VPN gateway should the cor	nnection be established?
Enter th the VPN	e DNS name (i.e. vpnserver.do I gateway you want to connect	main.com) or the official IP address (i.e. 212.10.17.29) of to.
	Gateway	
4	61.219.68.13	
	Use extended authentica	tion (XAUTH)
00	<u>U</u> sername	
200		
	Password	Password (Confirm)
-		
		< <u>B</u> ack <u>N</u> ext <u>C</u> ancel

Setup4

Input 1234567890 in the Shared secret and retype it in the Confirm secret.

Input your local IP address in the Local identity, and click Finish button.

Destination	Assistant	×
Pre-sh Commo	ared key n secret for data encryption	D-Link
A share indentic Enter th	ed secret or pre-shared key is used cally on both sides (VPN client und le appropriate value for the IKE ID Pre-shared key <u>S</u> hared secret :	to encrypt the connection; this then needs to be VPN gateway), according to the selected ID type.
8	Local identity <u>I</u> ype : IP Address <u>I</u> D : 61.219.68.14	
		< <u>B</u> ack <u>F</u> inish <u>C</u> ancel

Setup5

After finishing the previous wizard, you can find out that add a new profile here.

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	
		1 <u>o</u> k

Setup6

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

Click **Policy editor** to edit IPSec and IKE policy

General	IPSec Ge	eneral Settings		
IPSec General Settings Identities IP Address Assignment	Policies	<u>G</u> ateway :	61.219.68.13	
Remote Networks Firewall Settings	Q	<u>I</u> KE policy : IP <u>S</u> ec policy :	automatic mode	
			automatic mode	•
			Policy lifetimes F	olicy <u>e</u> ditor
	Advanc	ed options		
	2	Exch. <u>m</u> ode :	Aggressive Mode	-
	\mathcal{V}	PFS group :	None	•
			☐ Use IP compressio ☐ Disable <u>D</u> PD (Dea	n (LZS) d Peer Detection
		<u>H</u> elp	<u>о</u> к	<u>C</u> ancel

T IKE Policy	Configure
™ 3 ∏ IPSec Policy	New Entry
	Duplicate
	Delete
	Close

Setup7

Click **IKE Policy->New Entry**, enter DES+MD5+DH2 as the IKE policy name.

Select Encryption as DES, Hash as MD5, DH group as DH2 and click OK button.

Policy name :	DES+MD5+DH2			
Authentication	Encryption	Hash	DH Group	
Preshared Key	DES	MD5	DH-Group	2 (1024 Bit)
al and a constant				4.11
Authentication :	Preshared	Кеу	Y	Add
Authentication :	Preshared DES	Кеу	•	Add Remove
Authentication : Encryption : Hash :	Preshared DES MD5	Кеу	•	Add Remove

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

Protocol	Transform	None	
ESP	DES	MD5	
	Fop		(
protocol :	ESP	×	Add
rotocol : ransform :	ESP DES	× •	Add

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

Setup9

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

Select IKE policy as DES+MD5+DH2, IPSec policy as DES+MD5, Exch. mode as Main

Mode,	PFS	group	as DH-1
-------	-----	-------	---------

General	-IPSec Ge	neral Settings		
IPSec General Settings Identities IP Address Assignment	Paliaiaa	<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	licy <u>e</u> ditor
	Advanc	ed options		
	\sim	Exch. <u>m</u> ode :	Main Mode	-
		PFS group :	DH-Group 1 (768 Bit)	-
			Use IP compression Disable DPD (Dead	(LZS) Peer Detectio
		Help	ОК	Cancel

Setup **Remote Networks**, enter **Network address** as 192.168.1.0 and **Subnet masks** as 255.255.255.0

General IPSec General Settings Identities IP Address Assignment	Remote N Enter th Without	Networks le IP networks the tunnel s t entries tunneling will alwa	should be used for. ays be used.	
Remote Networks		Network addresses :	<u>S</u> ubnet masks :	
irewali Settings		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	
		E Apply tunneling sec	urity for local networks	
		Help	<u>O</u> K <u>C</u> ancel	

Setup11

Setup Firewall settings, select Enable Stateful Inspection as off and click OK button.

General	Firewall Settings
IPSec General Settings Identities IP Address Assignment Remote Networks	With firewall settings activated packets from other hosts will be discarded.
Firewall Settings	Enable Stateful Inspection : Off

Click Connect button to establish IPSec tunnel



2. LAN to LAN

2-1 Objective:

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

2-2 Environment:

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



2-3 Setups:

Remote_Firewall settings	Local_Firewall settings
01- Enable PPTP Client	01- Enable PPTP Server
02- Server IP address: 61.219.68.13	02- Local IP address: 10.10.99.254
03- Username: firewall	03- IP pool: 10.10.99.200-205
04- Password: firewall	04- Username: firewall
	05- Password: firewall

2-3-1 PPTP Server & PPTP Client

DFL-1500

01- Enable	PPTP Server	(Advanced se	ettings -> \	PN settin	igs -> PPTP)	
<u>IPSec</u>	<u>VPN Hub</u>	<u>VPN Spoke</u>	РРТР	<u>L2TP</u>	<u>Pass</u> <u>Through</u>		
	🗹 Enable PP	TP Server					
[Server] <mark>[Cli</mark>	<u>ent]</u>						
			Local	IP: 10.10.9	9.254		
				Assigned If	⊃ Range		
		Start:	10.10.99.20)O E	End: 10.10.99.	205	
		Username	firewall		Password: ••		
				Appl	у		

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

<u>IPSec</u>	VPN Hub	VPN Spoke	РРТР	L2TP	Pass Through		
	🗹 Enable PF	PTP Client					
[<u>Server</u>][Clie	ent]		12		20.40		
2			Serve	er IP: [61.219.6	8.13		
		Usernam	ne: firewall	Pasianad ID: 10	assword: ••••••	•	
			A	Apply	10.99.201		

03- Add a static routing table (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	-	÷.	-
	4	2	-	·.	-
	5	2		2	120
	6	2	-	2	120

DFL-1100/700/200

01- Add User (Firewall -> Users)

User Management

Add new user:

User name:	firewall	
roup membership:		
Password	******	
i doomold.	· · · · · · · · · · · · · · · · · · ·	

L2TP/PPTP settings:

	In empty, the IP address will be taken nom	the servers in p
Networks behind user:	192.168.1.0/24	

02- Enable PPTP Server (Firewall -> VPN)

L2TP/PPTP Servers

Edit PPTP tunnel pptp-server:

Name:	pptp-server	
Outer IP:		Blank = WAN IP
	Must be WAN IP	if IPsec encryption is required
Inner IP:		Blank = LAN IP

IP Pool and settings:

Client IP Pool:	10.10.99.200 - 10.10.99.205		
	Proxy ARP dynamically added routes		
Primary DNS:	(Optional)		
Secondary DNS:	(Optional)		
	🗹 Use unit's own DNS relayer addresses		
Primary WINS:	(Optional)		
Secondary WINS:	(Optional)		

03- Enable PPTP Client (Firewall -> VPN)

L2TP/PPTP Clients

Add PPTP Client :

sic settinas:		
3		
Username:	firewall	
Password:	*****	
Retype Password	*****	
Interface IP:		Blank = get IP from serve
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 L2TP Server & L2TP Client

Remote_Firewall settings	Local_Firewall settings

2-3-3 IPSec

Remote_Firewall settings	Local_Firewall settings
01- Enable IPSec	01- Enable IPSec
02- Local IP address: 192.168.1.0/24	02- Local IP address: 10.10.99.0/24
03- Remote IP address: 10.10.99.0/24	03- Remote IP address: 192.168.1.0/24
04- Negotiation Mode: Main mode	04- Negotiation Mode: Main mode
05- Encapsulation Mode: Tunnel mode	05- Encapsulation Mode: Tunnel mode
06- Peer's IP address: 61.219.68.13	06- Peer's IP address: 61.219.68.14
07- PSK: 1234567890	07- PSK: 1234567890
08- IKE policy: DES+MD5	08- IKE policy: DES+MD5
09- IKE key group: DH2	09- IKE key group: DH2
10- IPSec policy: DES+MD5 (ESP)	10- IPSec policy: DES+MD5 (ESP)
11- IPSec key group: DH1	11- IPSec key group: DH1

DFL-1500

Remote_Firewall:

01- Add books (Basic -> Books)

Address	Service	Schedule				
Objects][Gro	oups]					
Address	s-> Objects ->	Edit				
			Edi	t Address o	bject num	ber 1
Name						24316 - 5U
		Address n	ame: WAI	N1-VPNA		
Value Address	Type:					
• St	ibnet	IP: 10.10.99.	.0	Mask: 25	5.255.255.0)
OR	inge St	art IP: 0.0.0.0		End IP: 25	5 255 255 2	255
OHe	ist	IP:0.0.0.0				
¢ ni	, st					
				Back	Appl	y)
]]	
Address	Service	<u>Schedule</u>				
bjects][Gro	oupsj					
Addres	s-> Objects ->	> Edit				
Marrie			Ed	lit Address	object nun	nber 1
Name		Addross	name: LAI			
Valuo		Address	lame. LA			
Address	Туре:					
⊙ Si	ubnet	IP: 192.168.	1.0	Mask: 2	255.255.255	.0
OR	ange St	tart IP: 0.0.0.0		End IP: 2	255.255.255	.255
Он	ost	IP: 0.0.0.0				
				Back	App	aly

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

Status Edit	Rules Show Rules	Attack Alert Sun	nmary			
Firewall->Edi	t Rules					
Edit WAN1	Y to LAN1 Y ru	les				
Default actio	n for this packet direc	tion: Block V	Log Apply			
Packets are top-d	own matched by the	rules.				
Item	Status		Cond	ition		Action
# Nam	e Schedule	Source IP	Dest. IP	Service	Action	Log
1 Defai	ult ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y
						Page 1/1
	-	Prev. Page Ne	at Page Mow	e Page 1		
	Insert	Edit	Delete	Move Before: 1		
			A		5	
Firewall->Edit F	Rules->Insert					
	1240000	Insert a new	WAN1-to-LAN1	Firewall rule		
St	atus					
	Rule name:	Rule1				
-	Schedule:	Always 🐱				
Co	ondition					
	Source IP:	WAN1-VPNA	~	Dest. IP: LAN1-VE	PNA	~
	Service:	ANY 💌				
A	tion	· · · · · · · · · · · · · · · · · · ·				
	Forward 🗸	and log 🗸	the matched s	ession.		
	E	orward bandwidt	h class: def cla	ss 🗸		
	R	everse bandwidt	h class: def cla	ee 🗙		
	R.	everse bandwidt	li ciuss. dei_cia	<u>33 (*)</u>		
		Bac				
				PP-0		
3- Enable IP	Sec and edit IP	Sec rule (Adv a	nced Setting	IS -> VPN Setting	(2)	
					10)	
IDSoc	VDN Hub	VDN Spoko	DDTD		ass	

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

IPSec->IKE->Edit Rule			
	Status		
Active			
IKE Rule Name ipsec			
Condition			
	Local Address Type Subnet Address V		
	IP Address 192.168.1.0		
	PrefixLen / Subnet Mask 255.255.255.0		
	Remote Address Type Subnet Address 🗸		
	IP Address 10.10.99.0		
	PrefixLen / Subnet Mask 255.255.255.0		
	Action		
	Negotiation Mode Main		
Outgoing I	nterface WAN1		
Peer's IP /	Address Static IP V 61.219.68.13		
My Identifier	IP Address Auto_Assigned		
Peer's Identifie	IP Address Value Auto Assigned		
O ESD AL	the Encount and Authoriticate (DES_MD5)		
	Authentierte (MDE)		
O AR Algo	ithm Addrenticate (MD5)		
Pre-Sha	ared Key 1234567890		
	Advanced		
	Phase 1		
Negotiation Mode	ain		
Pre-Shared Key 12	rod Kov 1224567890		

Encrypt and Authenticate (DES, MD5)

Encrypt and Authenticate (DES, SHA1)

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

Y

Encryption Algorithm Encrypt and Authenticate (DES, MD5)

SA Life Time

Key Group

	F	Phase	1
Negotiation Mode	Main		
Pre-Shared Key	1234567890		
Encryption Algorithm	Encrypt and Authenticate (DES, MD5)		uthenticate (DES, MD5)
SA Life Time	28800		⊙sec ○min ○hour
Key Group	DH2 🗸		
	DH1		
	DH2	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)
Back	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 ar	nd Authenticate (DES, MD5) 🛛 👻
SA Life Time	28800	⊙ sec
Perfect Forward Secrecy(PFS)	DH1 🛩	
	None	
Back	DH1 DH2 DH5	Apply

Local_Firewall:

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

Address <u>Servi</u>	<u>ce</u> <u>Schedule</u>	
bjects] <u>[Groups]</u>		
Address-> Objec	cts -> Edit	
		Edit Address object number 1
Name		
Malua	Address name:	WANT-VPND
Address Type:		
Subnet	IP: 192.168.1.0	Mask: 255.255.255.0
○ Range	Start IP: 0.0.0.0	End IP: 255.255.255.255
○ Host	IP:0.0.0.0	
	[Back Apply
	Ļ	
Address Servi	ice Schedule	
bjects] [Groups]	<u>oonouno</u>	
· · · · · · · · · · · · · · · · · · ·		
Address-> Obje	cts -> Edit	
		Edit Address object number 1
Name		Eure Address object humber 1
	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
⊖ Host	IP: 0.0.0.0	
	(Back Apply

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

<u>Sta</u>	<u>atus</u>	Edit Rul	es <u>Show Rules</u>	Attack Alert Sur	nmary		
	Firew	all->Edit Rul	es				
Packe	Edit Defa ets ar	WAN1 🛩 1 ult action for e top-down	to LAN1 🖍 rule this packet direct matched by the	es ion: Block 💌 🗸 rules.	Log Apply		
lte	m	5	Status		Cond	ition	
	#	Name	Schedule	Source IP	Dest. IP	Service	Actio
	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block
			P Insert	rev. Page Ne Edit	xt Page Mov Delete	e Page 1 🗸 Move Before: 1 🗸	
<u>Sta</u>	Status Edit Rules Show Rules Attack Alert Summary						
	Firew	all->Edit Rule	s->Edit				
				Edit WAN1-to-LAN1	Firewall rule num	ıber 1	
	Status						
	Rule name: Rule1						

~

🝸 the matched session.

Apply

~

Forward bandwidth class: def_class v Reverse bandwidth class: def_class v

Back

Dest. IP: LAN1-VPNB

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

Schedule: Always 🛩

Source IP: WAN1-VPNB

Service: ANY

Forward 🎽 and log

Condition

Action

IPSec	<u>VPN Hub</u>	<u>VPN Spoke</u>	<u> PPTP</u>	<u>L2TP</u>	<u>Pass</u> <u>Through</u>
	🗹 Enable IP	Sec 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 255.255.2				
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)				
OAH 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 A	Authenticate (DES, MD5) 🛛 💊
SA Life Time	28800	● sec ○ min ○ hour
Key Group	DH2 💌	
	DH1	
	DH2	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)
Badi	Encrypt only (DES)
to <u>Save Running Configur</u>	Encrypt only (3DES) Encrypt only (AES) Authenticate only (MD5) Authenticate only (SHA1)

	Phase	2	
Encapsulation	Tunnel		
Active Protocol	ESP		
Encryption Algorithm	Encrypt a	nd Authenticate (DES, MD5)	*
SA Life Time	28800	⊙sec ⊙min Ohour	
Perfect Forward Secrecy(PFS)	DH1 💌		
	None		
Bacl	DH1 DH2 DH5	Apply	

DFL-1100/700/200

Remote_Firewall:

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

Firewall Policy

Edit global policy parameters:

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

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

VPN Tunnels

Edit IPsec tunnel ipsec:

Name:	ipsec	
Local Net:	192.168.1.0/24	

Authentication:

PSK:	****	1024562000
Retype PSK:	*****	1234507890
Certificate-ba	sed	
Local Identity:	Admin - CN=000F	3D6937BC
Certificates:		
	1	
	1	
	Use ctrl/shift click To use ID lists belo	to select multiple certificates. w. vou must select a CA certificate.

Tunnel type:

C 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, I range of IP addresses for roaming / NATed ga	DNS name, or ateways.
Route:	Automatically add a route for the remote r	network.
Proxy ARP:	\Box Publish remote network on all interfaces v	via Proxy ARP.
IKE XAuth client:	Pass username and password to peer via requires it.	IKE XAuth, if the remote gateway
XAuth Username:		
XAuth Password:		

VPN Tunnels

Edit advanced settings of IPsec tunnel ipsec:

IKE Mode:	Main mode IKE
	C 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
	O Manually configured keepalives:
	Source IP:

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1	DES	MD5 💽	0	28800
#2	DES	MD5 -	0	28800
#3:	CAST-128	SHA-1 🗸	0	28800
#4:	Blowfish-40 Allowed: 40-448 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 + DES . MD5 -0 3600 #2: 3DES CAST-128 0 #3: SHA-1 💌 3600 Blowfish-40 Allowed: 40-448 0 #4: MD5 . 3600 Blowfish-128 Allowed: 40-448 Blowfish-256 Allowed: 40-448 #5: SHA-1 👻 0 3600 Blowfish-128 Allowed: 128-448 Blowfish-256 Allowed:128-448 #6: MD5 • 0 3600 Blowfish-256 Allowed: 256-448 Blowfish-448 Allowed: 256-448 0 O #7: MD5 ٠ 0 O #8: -+ MD5 -

Local_Firewall:

01-Enable allow all VPN traffic (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.	
	🍼	83	0
	Apply	Cancel	Help

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

VPN Tunnels

Edit IPsec tunnel ipsec:

Name:	ipsec	
Local Net:	10.10.99.0/24	

Authentication:

PSK:		
Retype PSK:	1234567890	
ertificate-ba	sed	-
Local Identity:	Admin - CN=000F3D59A5A4	
Certificates:	Use ctrl/shift click to select multi	ple certificates.
Certificates:	Use ctrl/shift click to select multi To use ID lists below, you must s	ple certificates. select a CA certificate.

Tunnel type:

O Roaming Users - single-host IPsec clients

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

IAN-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.
	On if supported and needed (NAT detected between gateways)
	◯ 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: <mark>,</mark>	DFS	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	MD5 💌	0	0
IPse	1 Worish-256 Allowed:256-256			
#1:	AES-128 Allowed:128-256 AES-256 Allowed:128-256 AES-256 Allowed:256-256	HMAC MD5 💌	Life KB	Life Sec 3600

IPsec Proposal List

	Cipher	HMAC
#1:	DES 💌	MD5
#2:	DES JDES	MD5
#3:	CAST-128 -	SHA-1
#4:	Blowfish-40 Allowed: 40-448 Blowfish-128 Allowed: 40-448	MD5
#5:	Blowfish-256 Allowed: 40-448 Blowfish-128 Allowed: 128-448	SHA-1
#6:	Blowfish-256 Allowed:128-448 Blowfish-256 Allowed:256-448	MD5
#7:	Blowfish-448 Allowed: 256-448 Blowfish-448 Allowed: 448-448	MD5
#8:	- Twofish-128 Allowed:128-256 Twofish-256 Allowed:128-256	MD5
"AES estab	Twofish-256 Allowed: 256-256 AES-128 Allowed: 128-256 (AES-256 Allowed: 128-256	is unit will pro ccept any cip
	AES-256 Allowed: 256-256	

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

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



DFL-600

Remote_Firewall:

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

Policy Rules / Global Policy Status / Policies			
Inbound Port Filter	Outbound Port Filter		
Enabled	🗹 Enabled		
 Allow all except policy settings 	Allow all except policy settings		
🔿 Deny all except policy settings	O Deny all except policy settings		
e avanterie			

02- Enable IPSec and edit IPSec rule (Advanced -> VPN-IPSec -> Tunnel Settings)

IPSec Settings / Status	<u>Manual Key</u> / Tun	nel Settings / <u>Tunnel Table</u> / <u>IPSec</u>
Add/New Tunnel		
Tunnel Name	ipsec	
Peer Tunnel Type	Static IP address	~
Termination IP	61.219.68.13	
DomainName		
Peer ID Type	Address(IPV4_Addr)	*
Peer ID	61.219.68.13	(optional)
Shared Key	1234567890	
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 💌	

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 ad	ld P1 proposal	
P1 Proposals	P1Param 🚩	NOT_SET 🔽
A.	NOT_SET	NOT_SET 🚩
Click here to ad	ld P2 proposal	
P2 Proposals	P2Param 💙	NOT_SET 💙
	NOT_SET 🔽	NOT_SET 🔽
Target Host Rar	ige	
Starting Target Host	10.10.99.0	
Subnet Mask	255.255.255.0	

Local_Firewall:

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

Policy Rules / Global Policy Status / Policies

Inbound Port Filter	Outbound Port Filter
🗹 Enabled	🗹 Enabled
 Allow all except policy settings 	Allow all except policy settings
O Deny all except policy settings	🔿 Deny all except policy settings

02- Enable IPSec and edit IPSec rule (Advanced -> VPN-IPSec -> Tunnel Settings)

IPSec Settings / Status	<u>Manual Key</u> / Tuni	nel Settings / <u>Tunnel Table</u> / <u>IPS</u>
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	O 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 🔽	

<u>Click here to add P1 proposal</u>

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 Rai	nge	
Starting Target Host	192.168.1.0	
Subnet Mask	255.255.255.0	