DFL-700 with DI-804HV IPsec VPN Configuration Guide

This configuration shows how to connect a DFL-700 to a DI-804HV with an IPsec tunnel. Please check the D-Link AUS FTP Site at ftp://202.129.109.68 for updates on the firmware.



DFL-700 configuration

2)

1) Log into the DFL-700 using its IP address (https://192.168.1.1 in this example) and then enter the username and password.

orks for Peo	DFL-700 Network Security Firewall						
	System	Firewall	Servers	Tools	Status	Help	
Ľ	Administration S	ettings					
Ī	Management w HTTP Po HTTPS Po For security r ports. Also n baken the m	reb GUI ports ort: 80 ort: 443 reasons, it may be be ote that if web-based anagement web GU	tter to run the manag user authentication i has to use other por	ement web GUI o is enabled, ports (n non-standard 30 and 443 will be		
					🕥 🥴 Apply Cane	el Help	
	Select the interface Note that both the and read-only right to log on, but will re	e / user you wish to e user settings and the s logs on from a some ceive read-only acc	edit from the below list interface settings lim ewhere where only re ess only.	t. it what a user car ad-only access is	n do, so if a user wi allowed, the user v	th both admin vill be allowed	
	Administrative acc	ess via LAN interfac	e (Edit)				
irewall-	→ VPN. CI	ick on Ad	d New.				
II- J Pe	→ VPN. CI	ick on Ad	d New.	DFL-70	0 Firewall		
II- Pee	> VPN. CI	ick on Ad	d New.	DFL-70 Security Tools	0 Firewall Status	Help	
all-	VPN. Cl ople System VPN Tunnels	ick on Ad	d New.	DFL-70 Security Tools	0 Firewall Status	Help	
II- Pe	VPN. CI System VPN Tunnels Pick a VPN tunnel	ick on Ada Firewall	d New. Network Servers	DFL-70 Security Tools	0 Firewall Status	Help	
- Pe	VPN. CI System VPN Tunnels Pick a VPN tunnel	ick on Add Firewall	d New. Network Servers	DFL-70 Security Tools	0 Firewall Status	Help	
	VPN. CI Sople System VPN Tunnels Pick a VPN tunnel VPN Tunnels	ick on Ad Firewall to edit from the belo	d New. Network Servers	DFL-70 Security Tools	0 Firewall Status	Help	
Pe	VPN. Cl System VPN Tunnels Pick a VPN tunnel VPN Tunnels Name L [Add new]	ick on Ad Firewall to edit from the belo	d New. Network Servers wlist	DFL-70 Security Tools	0 Firewall Status	Help	
for Pe	VPN. Cl System VPN Tunnels Pick a VPN tunnel VPN Tunnels Name L [Add new]	ick on Add Firewall to edit from the belo	d New. Network Servers wlist	DFL-70 Security Tools	0 Firewall Status	Help	
Pe	VPN. Cl System VPN Tunnels Pick a VPN tunnel VPN Tunnels Name L Add new]	ick on Add	d New. Network Servers	DFL-70 Security Tools	0 Firewall Status	Help	

3) Enter the details for the Tunnel.

Name: DI-804HV Local Net: 192.168.1.0/24 Authentication: PSK Pre-shared key: dlinktest

LAN-to-LAN tunnel Remote net: 192.1	68.0.0/24					
Remote gateway:	195.74.119.	181				
	System	Firewall	Servers	loois	Status	нер
	VPN Tunnels					
	Add VPN tunnel :					
Policy			(
		Name. DF004HV	1.0/24			
Port Mapping		carnet. [152.100.	1.0724			_
Users	Authentication:					
	© PSK - F	Pre-Shared Key	3			
Schedules		PSK:				
	Retyp	be PSK: ********				
Services	O Certific	ate-based				
	Local	Identity: Admin - 0	CN=00900B025D59		*	
VPN	Cert	ificates:				
Certificates						
		Use ctrl/s To use ID	hift click to select mul lists below, you must	tiple certificates. select a CA certif	icate.	
Content Filtering	Iden	itity List: (no list)				
						- 1
	Tunnel type:					
	O Roamir	ng Users - single-ł	nost VPN clients			
	IKE	XAuth: 📕 Requ	ire user authenticatio	n via IKE XAuth ti	o open tunnel	
	⊙ LAN-to	-LAN tunnel				
	Remo	ote Net: 192.168.	D.0/24			
	Remote G	ateway: 195.74.1	19.181			
		The gatev range of II	vay can be a numeric P addresses for roamir	al IP address, DN ng / NATed gates	S name, or ways.	
	Pro	ky ARP: 🔲 Publi	sh remote network on	all interfaces via	Proxy ARP	

Click on Apply when done.

4) Click on Edit on the newly created DI-804V profile

D-Link Building Networks for Peop	S Dle		Netw	DFL-70 ork Security	0 Firewall	
	System VPN Tunnels VPN tunnel DI-1	Firewal	Serve	rs Tools	Status	Help
Policy Port Mapping	Pick a VPN tunnel	I to edit from the b	elow list:			C) Help
Users	VPN Tunnels Name I DI-804HV 1 [Add new]	Local Net 192.168.1.0/24	Remote Net 192.168.0.0/24	Remote Gateway 195.74.119.181	(<u>Edit</u>)	

 Click on Advanced. Set IKE mode to 'Main Mode' (default), IKE DH Group '2 – modp 1024-bit'(default). Leave PFS unchecked. Set NAT traversal to 'Disabled'. Click on 'Apply' when done

etworks for People		DFL-700 Network Security Firewall					
Syste	em <mark>Firewa</mark>	I Servers	Tools	Status	Help		
VPN Tu	nnels						
Edit adva	nced settings of VPN tun	nel DI-804HV :					
	Limit MTU: 1424						
apping	IKE Mode: 💿 Main n	ode IKF					
add the second se	O Aggres	sive mode IKE					
IKI	E DH Group: 2 - modp 1	024-bit 💌					
	PFS: 🗖 Enable	Perfect Forward Secrec	.y				
PE:	S DH Group: 2 - modp 1	024-bit 🗾					
NA NA	T Traversal: 💿 Disable	ed.					
	O On if s	upported and needed (N/	AT detected betw	veen gateways)			
	O On if s	upported					
	Keepalives: 💿 No kee	epalives.					
	C Autom	atic keepalives (works wi	ith other DFL-700.	/1100 units)			
	O Manua	lly configured keepalives	8:				
	So	urce IP:					
	Destin	ation IP:					
ing IKE Prov	nosal List						
	abar	Hach		ifa Caa			

6) Click on 'Activate' on the bottom left hand corner of the screen.



7) Click on the 'Activate Changes' button.

	System	Firewall	Servers	Tools	Status	Help					
	Activate Chang	es									
	Press "Activate Cł	nanges" below to sav	ve your changes and	have them take e	ffect.						
Administration	If an administrator accidentally locked	If an administrator does not log in within a set time, the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.									
Interfaces	Wait for admin logi	n for: 1 minute	before reverting.								
Routing	Activate Chan	ges									

DI-804HV configuration

 Log on to the DI-804V using its IP address (<u>http://192.168.0.1</u> in this example) and enter the username and password.



 Click on 'VPN' on the left hand side. Under VPN Settings, check the enable box for VPN. Set the Max. number of tunnels to 5 for example. In ID 1, enter the Tunnel Name, 'dfl-700'. Click on 'Apply' then 'Continue'. In ID 1, set the method to 'IKE' and then click on 'More'.

Building Networks for People			DI Broadb	-804HV and VPN Rout	er
1	Home	Advanced	Tools	Status	Help
	VPN Settings				
-		ltem		Setting	
	VPN		🗹 Enable		
	NetBIOS broad	cast	🗖 Enable		
ard	Max. number of	tunnels	5		
WAN	D	Tunnal Name		Mothed	
	1	dfl-700		IKE Mon	e
LAN	2				
	-			IKE Mon	-
	3			IKE Mon	
	4				
PN	5				e
	Previous page	Next page		0	
	Dynamic VP	N Settings	2TP Server Setting	PPTP Server Setti	ing
				-	2 0
				V	2 😡
				Apply Ca	ncel Hel

3) Enter the details for the tunnel.

Local Subnet : 192.168.0.0

Local netmask: 255.255.255.0 Remote Subnet: 192.168.1.0 Remote netmask: 255.255.255.0 Remote Gateway: 195.74.119.180 Preshare key: dlinktest

	Home	Advanced	Tools	Status	Help
	VPN Settings -	Tunnel 1			
Altin o		tem		Setting	
	Tunnel Name		dfl-700		
	Aggressive Mode		🗖 Enable		
Wizard	Local Subnet		192.168.0.0		
INVANI	Local Netmask		255.255.255.0		
WAIN	Remote Subnet		192.168.1.0		
LAN	Remote Netmas	ĸ	255.255.255.0		
	Remote Gateway	(195.74.119.180		
DHCP	Preshare Key		dlinktest		
	IKE Proposal ind	ex	Select IKE Propo	sal	
VPN	IPSec Proposal i	ndex	Select IPSec Pri	oposal	

4) In the Set IKE Proposal screen, set ID 1 to the following settings

Proposal Name: 3des-md5 DH-Group: Group2 Encrypt algorithm: 3DES Auth algorithm: MD5 Lifetime: 28800 Life Time Unit: Sec.

In 'Proposal ID', select 1 then click on 'Add to'. Click on 'Apply' then 'Continue'.

	Home	Advance	d Tools	Sta	tus	Help
-	VPN Sottings T	unnel 1 Set	IKE Pronosal			
	Vin Settings - 1	unner 1 - Jer	INC 1 TOPOSAI			
	Ite	em		Settir	g	
	IKE Proposal inde	X	3des-md5			
				Deserve		
Nizard				Remove		
WAN	ID Proposal Nam	e DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
	1 3des-md5	Group 2 💌	3DES -	MD5 -	28800	Sec. 💌
-	2	Group 1 🚽	3DES -	SHA1 -	0	Sec.
	3	Group 1 💌	3DES 👻	SHA1 -	0	Sec.
	4	Group 1 星	3DES -	SHA1 🔽	0	Sec. 💌
	5	Group 1 星	3DES 🔽	SHA1 -	0	Sec.
	6	Group 1 💌	3DES 💌	SHA1 🔽	0	Sec.
	7	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
	8	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
	9	Group 1 💌	3DES 💌	SHA1 💌	0	Sec.
				SHA1	0	Sec.

5) Click on 'Back'. Click on 'Select IPsec Proposal'.

Proposal Name: 3des-md5 DH-Group: None Encap protocol: ESP Encrypt algorithm: 3DES Auth algorithm: MD5 Lifetime: 3600 Life Time Unit: Sec.

In 'Proposal ID', select 1 then click on 'Add to'. Click on 'Apply' then 'Continue'.

D-Link Building Networks for People				DI- Broadbo	804H	V Route	r
1	Home	Advan	ced	Tools	Statu	s	Help
	VPN Settings	Tunnel 1 - S	et IPSEC P	roposal			
	_	Item			Setting		
	IPSec Proposal	index	3de:	s-md5			
zard				Rem	ove		
			1				
WAN	ID Proposal Name	DH Group	Encap	Encrypt	Auth	Life Time	Life Time Unit
	1 3des-md5	None 💌	ESP	3DES 💌	MD5 -	3600	Sec.
AN	2	None	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
нср	3	None	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
	4	None	ESP -	3DES 💌	None 💌	0	Sec. 💌
VPN	5	None	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
	6	None	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
	7	None	ESP -	3DES 💌	None 💌	0	Sec. 💌
	8	None	ESP -	3DES 💌	None 💌	0	Sec. 💌
	9	None	ESP -	3DES 💌	None 💌	0	Sec. 💌
	10	None	ESP 🗾	3DES 💌	None 💌	0	Sec. 💌
		Proposal I	D select or	ie 💌 Add to	Proposal inc	dex	
				_			
					3 🗸) 🕓) 🗘

Testing the connection

From the DFL-700 side, you can initiate a ping to a machine on the LAN side of the DI-804HV (i.e. 192.168.0.10). The tunnel should then be generated and then you should get a response as shown below.

🖾 Command Prompt - ping 192.168.0.10 -t	
Reply from 192.168.0.10: bytes=32 time=35ms TTL=128 Reply from 192.168.0.10: bytes=32 time=36ms TTL=128 Reply from 192.168.0.10: bytes=32 time=35ms TTL=128 Reply from 192.168.0.10: bytes=32 time=37ms TTL=128 Reply from 192.168.0.10: bytes=32 time=37ms TTL=128 Reply from 192.168.0.10: bytes=32 time=37ms TTL=128 Reply from 192.168.0.10: bytes=32 time=36ms TTL=128 Reply from 192.168.0.10: bytes=32 time=36ms TTL=128 Reply from 192.168.0.10: bytes=32 time=36ms TTL=128	