Configuration Guide



Overview

The IPSec gateway-to-gateway VPN tunnel using pre-shared keys (PSK) is the most secure method to ensure end-to-end data security across the Internet.



Scope

This document describes the configuration of D-Link DSR Series routers to implement an IPSec VPN tunnel secured with pre-shared keys. This use case will cover IPSec VPN tunnel configuration between a D-Link DSR-250N router and DFL-860E firewall.



Configuring the DFL-860E

Step 1. Go to Object>>InterfaceAddresses

😚 Home 🗏 🔣 Configuration 🗸 🕴 🎢 T	Fools 🗸 📔 🚳 Status 🖲	🖌 🔌 Maintenance 🗸			😚 Logout 🔞
IP Settings	Add -	eAddresses bider can be used to group related address obj dit this object	acts for better overview.		
Conn. Timeout Settings	#	Name	Address	User Auth Groups	Comments
Sength Limit Settings	1	🦁 wan1_ip	0.0.0		IPAddress of interface wan1
Fragmentation Settings	2	🦁 waninet	0.0.0/0		The network on interface wan1
Local Reassembly Settings	3	🍹 lan_ip	192.168.10.1		IPAddress of interface lan
SSL Settings	4	💡 lannet	192.168.10.0/24		The network on interface lan
Misc. Settings	5	🤤 dmz_ip	172.17.100.254 💥 Dele	te	IPAddress of interface dmz
🖻 🔛 Objects	6	🐺 dmznet	172.17.100.0/24	ble	The network on interface dmz
🖻 🙀 Address Book	7	🤤 wan2_ip	192.168.120.254 == New	Group	IPAddress of interface wan2
- DHCPAddresses	8	🤤 wan2net	192.168.120.0/24 A Move	e to Top	The network on interface wan2
	9	🤤 wan1_gw	0.0.0.0	eUp	Default gateway for interface wan1
- DALG with AV/WCF	10	🗟 wan1_dns1	0.0.0.0 🔬 Move	e to Index	Primary DNS server for interface wan1
- Services	11	🤤 wan1_dns2	0.0.0.0 🐺 Move	e Down	Secondary DNS server for interface
NAT Pools			🚸 Move	e to Bottom	Wall
Schedules					 Right-click on a row for additional options.
🖻 🙀 VPN Objects					

Edit lan-ip 192.168.10.1 to 192.168.1.1; Click **OK** to save the setting.

Use an IP4 Address item to define a name for a specific IP4 host, network or range.	
General User Authentication	
1 General	
Name: Ian_jp Address: 192.168.1.1 ① Comments 192.168.1.1	
Comments: IPAddress of Interface Ian	
	OK Cancel

Edit lannet 192.168.10.0/24 to 192.168.1.0/24; Click **OK** to save the setting.

Use an IP4 Address Item to define a name for a specific IP4 host, network or range	
General User Authentication	
🕑 General	
Name: lannet	
Address: 192.168.1.0/24	
Omments	
Comments: The network on Interface Ian	
	OK Cancel

After editing, the following page will display:

An address f	eAddresses older can be used to group related address objec	ts for better overview.		
🎦 Add 👻 🛃 E	dit this object			
#	Name	Address	User Auth Groups	Comments
1	🤤 wan1_ip	0.0.0.0		IPAddress of interface wan1
2	🦁 wan1net	0.0.0/0		The network on interface wan1
3	🗟 lan_ip	192.168.1.1		IPAddress of interface lan
4	🤤 lannet	192.168.1.0/24		The network on interface lan
5	😽 dmz_ip	172.17.100.254		IPAddress of interface dmz
6	😼 dmznet	172.17.100.0/24		The network on interface dmz
7	🤤 wan2_ip	192.168.120.254		IPAddress of interface wan2
8	🤤 wan2net	192.168.120.0/24		The network on interface wan2
9	🦁 wan1_gw	0.0.0.0		Default gateway for interface wan1
10	🤤 wan1_dns1	0.0.0.0		Primary DNS server for interface wan1
11	🗟 wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1
				Bight-click on a row for additional option

Step 2. Go to Object>>DHCPAddresses

Edit lan_dhcpserver_range 192.168.10.100-192.168.10.200 to 192.168.1.100-192.168.1.200;

Edit lan_dhcpserver_gw 192.168.10.1 to 192.168.1.1;

Edit lan_dhcpserver_dns1 192.168.10.1 to 192.168.1.1;

Dipects	An address	Addresses folder can be used to group related address objects for bet	ter overview.	
DHCPAddresses	🎦 Add 👻 🛃	Edit this object		
ALG with AV/WCF	#	Name	Address	User Auth Groups
- Contraction -	1	😽 lan_dhcpserver_range	192.168.1.100-192.168.1.200	
- IP Pools	2	🤤 lan_dhcpserver_netmask	255.255.255.0	
	3	😽 lan_dhcpserver_gw	192.168.1.1	
Schedules	4	😽 lan_dhcpserver_dns1	192.168.1.1	

Step 3. Go to Configuration>>Save and Activate; click OK to save the settings.



Step 4. Go to Objects > Address Book > Interface Addresses. Click on Add and select IP4 address.

D-Link Building Networks for People			
🛭 😚 Home 🛛 🔣 Configuration 🚽 🛛 👖 Too	ls 🗸 🔰 🚳 Status 🗸 🛛 🔩 M	laintenance 🗸	
DFL-860E B System D Dects D Dects D Dects	An address folder can b An address folder can b Add Add Add Add Add Add Add Add	ESSES e used to group related address ob ct	jects for better overview.
DHCPAddresses	Ethernet Address	Name	Address
InterfaceAddresses	Ethernet Address Group	wan1_ip	0.0.0/0
ALG WITH AV/WCF	🗟 IP4 Address	🖓 lan ip	192.168.1.1
	4	lannet	192.168.1.0/24
NAT Pools	5	😓 dmz_ip	172.17.100.254
	6	🗟 dmznet	172.17.100.0/24
Authentication Objects	7	🗟 wan2_ip	192.168.120.254
E VPN Objects	8	🤤 wan2net	192.168.120.0/24
HTTP Banner Files	9	🤤 wan1_gw	0.0.0.0
E Rules	10	🤤 wan1_dns1	0.0.0.0
Interfaces Routing	11	🗟 wan1_dns2	0.0.0.0

Specify the settings of the remote network at the other end of the VPN tunnel.

In the Name field enter VPN-Remote-LAN.

In the Address field enter the Subnet ID and Mask Bits for the remote network: in our example it is 192.168.10.0/24.

Click the **OK** button.



Step 5. Add another IP Address. Enter the settings of the VPN endpoint-this is the public IP address of DSR-250N.

In the Name field enter **VPN-Remote-IP**.

In the Address field specify the public IP address of the remote network.

Use an IP4	dciress *4 Address item to define a name for a specific IP4 host, network or range.	
General	User Authentication	
射 General		
Name: VP	PN-Remote-IP	
Address: 17	72.17.2.17	
射 Commen	nts	
Comments:		
		OK Cancel
		UK Carce

Step 6. Go to Object > Authentication Objects. Click on Add and select Pre-Shared Key.

D-Link Building Networks for People					Logged in as administrator admin - 192.168.1.100
🥎 Home 🛛 🔣 Configuration 🗸 🕴 👔 1	Tools 🗸 📔 🚳 Status 🗸 🛛 🔩 I	Maintenance 🗸			😚 Logout 🕴 🔞 He
PFI-800E Optets Opte	Act thentication Act remove and most Act • Constant Set Chent Key Stat Chent Key	n Objects Pre-Sharec Kays and Cetificates Name Int TPSAdminCert	Type Certificate	Type Local	Comments

Enter the Pre-Shared Key settings for your VPN tunnel.

In the Name field, type Pre-Shared-Key.

In the Shared Secret field, select the type of key you want to use and type in the key. In our example we are using ASCII key (passphrase). Note that you will need to use exactly the same key when setting up the firewall on the other end of the tunnel.

Click **OK** when done.

😨 DFL-860E	Pre-Shared Key Post Che-shared Key authentication is based on a shared secret that is known only by the parties involved.
E - 6 System	Control
- Chierts	General
Address Book	🕑 General
Constant .	Name: pre_Shared_Key
Services	
Pools	
	Shared Secret
Schedules	
Concurrent and Chilester	Passphrase
Authentication Objects	Shared Secret:
E 🙀 VPN Objects	
HTTP Banner Files	Confirm Secret:
🗈 🕞 Rules	A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.
Interfaces	
E- 👸 Routing	Hexadecimal key
😟 🥁 IDP / IPS	Passphrase:
User Authentication	Generate Pandom Key
🗊 🔞 Traffic Management	
Tel- ConeDefense	

Step 7. Go to Interfaces > IPSec. Click on **Add** and select **IPSec Tunnel**.

🚯 Home 🗏 📉 Configuration 🗸 🗌 👬 1	Fools 🗸 🕴 🚳 Status 🗸 🗌 🗞 Maintenance	* .				👶 Logout 📔 🔋 Hel
PFL-860E	Manage the IPsec tunnel interfaces used	d for establishing IPsec VPN cor	nections to and from this system.			
E jo System E jo Objects E jo Rules	Add Add Advanced Settings					
E- Canterfaces	# Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
Ethernet						Right-click on a row for additional options.
PPPOE PFTP/L2TP Servers PPTP/L2TP Clients Switch Management interface Groups						

Enter your IPSec tunnel settings.

In the Name field, enter IPSec-tunnel.

In the Local Network field, select **lannet** (this is the private network on this side of the VPN tunnel).

In the Remote Network field, select **VPN-Remote-LAN** (this is the private network on the other side of the VPN tunnel, see **Step 4**).

In the Remote Endpoint field, select **VPN-Remote-IP** (this is the public IP address of the remote network, see **Step 5**).

Encapsulation Mode should be set to **Tunnel**.

Under Algorithms select the desired algorithms and IKE/IPSec Lifetime. In our example we are using Medium settings.

You can modify or add your own set of security algorithms under Objects > VPN Objects > IKE Algorithms and IPSec Algorithms.

- 🍣 Home 🛛 🔣 Configuration 🚽 🛛 👬	Tools 🗸 🛛 🕤 Status 🗸 🗌	Naintenance -								😚 Logou	it የ
PFL-560E Objects Control Co	Brec Lune I Annovember 2 Algorithms	IPSec-tunnel Innet VPN-Remote-LAN VPN-Remote-IP Tunnel (None)	ec endpoint and will h Routing	appear as a logical int	erface in the sys Keep-alive	tem.	 _	_	 		
B G Routing B G DP / IPS C Lese Authentication B G Lese Authentication B G Traffic Management B G ZoneDetense	IKE Algorithms: IKE Lifetime: IPsec Algorithms: IPsec Lifetime: IPsec Lifetime:	Medium 28800 Medium 3600 0	× ×		seconds seconds kilobytes						

Click on Authentication tab. Make sure the **Pre-Shared Key** option is enabled. Select the **Pre-Shared-Key** in the

dropdown menu (see **Step 6**).

Click on the **OK** button

General Authent	ication XAuth Ro	uting IKE Settings Ke	ep-alive Advance	d		
Authentication						
X.509 Certificate						
Root Certificate(s)						
HTTPSAdminCert	× ×	×				
Gateway certificate:	(Nono)					
Identification list						
identification list.	(None)					
Pre-shared Key						
Des also and loss of	a at 1.0					

Step 8. Go to Interfaces > Interface Groups. Click on **Add** and select **Interface Group**.

😚 Home 🛛 🔣 Configuration 🗸 🗌 👬	Tools 🗸 🛛 🚳 Status 🖌 👋 Mainte	nance 🗸		👶 Logout 👘 🦹 H
DFL-860E	Interface Groups	e several interfaces for simplified policy manager	nent.	
B Dijects B Rules	Add -			
E 🔒 Interfaces		Name	Members	Comments
- Wethernet - WVLAN - 😚 IPsec - 🐯 GRE				Right-click on a row for additional options.
PPPoE PTP/L2TP Servers PTP/L2TP Clients Switch Management Interface Groups ARP				

Create a group which has your IPSec tunnel and your LAN.

In the Name field, type *IPSec-LAN*.

Under Interfaces add **IPSec-tunnel** and **Ian** into the Selected field.

Click on the	OK button.
--------------	------------

Interface Group	
Use an interface group to combine several interfaces for a simplified security policy.	
General	
2) General	
Name: IPSec-LAN	
Security/Transport Equivalent	
*) Interfaces	
Available Selected IPSec-tunnel	
dmz lan lan	
wan1 wan2	
2 Comments	
Comments:	
	OK Cancel

Step 9. Go to Rules > IP Rules. Click on **Add** and select **IP Rule**.

🚳 Status 🗸 🛛 Naintenance 🚽						👶 Logout	🕐 Helj
IP Rules IP ries are used to fiter IP-based network Ads • IP Rule Folder IP Rule Folder I	k traffic. In addition, they provi Action Mallow	de means for address trar Src If	hslähon as well as Server Load Src Net ∳ lannet	balancing. Dest If	Dest Net Ģ lan_ip	Service	tions.
	Status Maintenance Pruse are used to fifter P-based networ Pruse are used to fifter P-based networ Pruse pruse	Status - Maintenance - IP Aule Status - Maintenance - IP Aule Status - Statu	Status - Maintenance - IP Rules IP rules IP rules an used to film IP Based network traffic. In addition, they provide means for address traffic Rule Factor P Rule Rule Rule Rule Rule Rule Rule Rule	Status - No P Rules IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Los Mol - P Rule Fouldr Nome Action Size Lf Size Fouldr P Rule Nome Action Size Lf Size Fouldr Size Net Imme Action Size Lg Imme Imme Action Imme Action Imme Imme Imme Imme </td <td>Status - No Maintenance - IP Rules IP rules IP rules are used to filter P-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing. Add - P Rule Fader Rule Fade</td> <td>Status - Maintennance - PRules Professes and to filter P-based retwork traffic in addition, they provide means for address fransistion as well as Server Load Balancing Also PRules PRULes PRULe</td> <td>Status - Autoreance - Control Contro Control Control Control Control Control Control Con</td>	Status - No Maintenance - IP Rules IP rules IP rules are used to filter P-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing. Add - P Rule Fader Rule Fade	Status - Maintennance - PRules Professes and to filter P-based retwork traffic in addition, they provide means for address fransistion as well as Server Load Balancing Also PRules PRULes PRULe	Status - Autoreance - Control Contro Control Control Control Control Control Control Con

This rule will allow communication between the LAN and the IPSec tunnel.

In the Name field, type *IPSec-Allow*.

Under Action select **Allow**.

Under Service select **all_services**.

Under Address Filter specify the following:

Source and Destination Interfaces: IPSec-LAN (this is the group you created in **Step 8**).

Source and Destination Network: select **all-nets**.

ID E	Dula		
8 IPP An IP	rule specifies what action to p	perform on network traffic that matches the specified filter criteria.	
Genera	Log Settings	NAT SAT Multiplex SAT SLB SAT SLB Monitors	
_			
射 Gener	ral		
Name:	IPSec-Allow		
Action:	Allow 🗸		
Service:	all_services 🗸		
Schedule:	(None) 🗸		
-			
Addre	ess Filter		
Specify sou	irce interface and source netw	vork, together with destination interface and destination network. All parameters have to match for the rule to match.	
	Interface	Network	
Source:	IPSec-LAN V	all-nets	
Destination:	IPSec-LAN 🗸	' all-nets	
🛃 Comm	nents		
Comments:			
		<i>N</i>	
			OK Cancel

Click on the Log Settings tab.

Select the **Enable Logging** option.

Click on the $\ensuremath{\text{OK}}$ button when done.

8 IP Rule An IP rule specifies what action to perform on network traffic that matches the specified fifter criteria.	
General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors	
General Select if logging should be enabled and what severity to use. Enable logging Log with severity: Default	
	OK Cancel

Step 10. To save the new configuration, click on Configuration, in the top menu bar and select Save and Activate.



Click **OK** to confirm the new settings.

Configuring the DSR-250N

Go to VPN>>IPsec VPN>>Policies to add an IPSec policy. Click Add New IPSec Policy and input the following:

nis page sh om this pa ote: Policy	ows ti ge. with	he list of co '*' represer	onfigu nts a (rred IPsec VPM Client Policy.	l polici	ies on the ro	uter	. A user c	an also	add, dele	te, ed	it, enable,	disable a	ind export I	Psec V	PN poli	icies
Show 10	• e	ntries [Righ	nt clici	on record to	get mor	re options]											٩
Status	¢	Name	÷	Backup Tunnel Name	÷	Туре	⇔	IPSec Mode	÷	Local	θ	Remote	÷	Auth	e	ncr	÷
						1	√o da	ta available	e in table	9							
howing 0 to	0 of 0	entries												I Previous	Next	Las	t 刘

Policy Name: IPSec

Policy Type: Auto Policy

IP Protocol Version: IPv4

IKE Version: IKEv1

Select Local Gateway: Dedicated WAN

Remote Endpoint: **IP Address**

IP Address / FQDN: The WAN IP address of your DFL-860E

Local IP: Subnet

Local Start IP Address: 192.168.10.0

Local Subnet Mask: 255.255.255.0

Remote IP: Subnet

Remote Start IP Address: 192.168.1.0

Remote Subnet Mask: 255.255.255.0

Pre share Key: Your DFL-860E Pre share key

IPSec Policy Configuration			×
General			^
Policy Name	IPSec		
Policy Type	Auto Policy	•	
IP Protocol Version	IPv4	•	
IKE Version	IKEv1	•	
L2TP Mode	None	•	
IPSec Mode	Tunnel Mode		
Select Local Gateway	Dedicated WAN	•	
Remote Endpoint	IP Address	•	
IP Address / FQDN	172.17.2.6	DFL-860E WAN IP	
Enable Mode Config	OFF		
5 11 N 10105			•
		Save	

Protocol	ESP 🔻
Enable DHCP	OFF
Local IP	Subnet 🔻
Local Start IP Address	192.168.10.0
Local Subnet Mask	255.255.255.0
Remote IP	Subnet 🔻
Remote Start IP Address	192.168.1.0
Remote Subnet Mask	255.255.255.0
Enable Keepalive	OFF
Phase1(IKE SA Parameters)	
Exchange Mode	Main 🔹
Direction / Type	Both

This section refers to the
local internal network of
the DSR-250N.
This section refers to the
remote internal network
of the DFL-860E.

	MD5	SHA-1	ON
	SHA2-256	OFF SHA2-384	OFF
	SHA2-512	OFF	
	Authentication Method	Pre-Shared Key	
	Pre-Shared Key	1234567890 [Length: 8 - 49	
	Diffie-Hellman (DH) Group	Group 2 (1024 bit) 🔻	
	SA-Lifetime	28800 [Range: 300 - 604800] Seconds	
	Enable Dead Peer Detection	OFF	
	Extended Authentication	None 🔻	
1	Phase2-(Auto Policy Parameters)		
	SA Lifetime	3600 Seconds T	

Authentication Method and Pre-Shared Key settings must be identical with remote Pre-Shared Key settings on the DFL-860E.

Verifying the connection:

Go to Status>>Network Information>>Active VPNs>>IPSec SAs

Right click on **IPSec**, then select **Connect**.

D-Link Unified Services Router -	DSR-250N		Logged in a Se	as: admin (ADMIN) erial: QBDT123456789	Language: English [US]) Firmware: 3.11_WW Wizard System Sea	togout
🗥 Status	🛜 Wireless	💻 Network	S VPN	Security	🗘 Maintenance	
Status » Network Information » IPsec SAs SSL VPN Conn This page lists current establis Active IPSec SAs List	Active VPNs IPsec SA nections PPTP VPN Co hed IPsec Security Assoc	nnections Open	VPN Connections	L2TP VPN Connec	stions GRE Tunnel Sta	2 O
Show 10 Tentries [Right	click on record to get more	e options]				٩
Policy Name	Endpoint	⊖ tx (KB)		s) 🕀	State	⇔
IPSec	172.17.2.6	0.00	0	Connect	IPsec SA Not Established	ext > Last >

Connection is established.

	🝘 Status	🛜 Wireless	💻 Network	A VPN	Security	🗘 Maintenance	
atus » Nei	twork Information »	Active VPNs » IPsec S	iAs				00
			Operat	tion Succeeded			
IPsec SA	AS SSL VPN Conne	ections PPTP VPN (Connections Open	n VPN Connections	L2TP VPN Connect	ions GRE Tunnel Status	ĺ
is page lis	ts current establish	ed IPsec Security Asso	ociations.				
ctive IPS	ec SAs List						
Show 10	• entries [Right cl	ick on record to get mo	ore options]				٩
Policy Na	me 🗘	Endpoint	⊖ tx (KB)	⊖ tx (Packet	s) 🕀 S	tate	⇔
IPSec		172.17.2.6	0.00	0	IF	^p sec SA Established	
Showing 1 to	1 of 1 entries				K	First Previous Next	Last 刘



Visit our website for more information www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries. All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2017 D-Link Corporation. All Rights Reserved.