Setting up L2TP Over IPSec Server for remote access to LAN

Remote clients: Android 5.0, iOS v10.3, Mac OS v10.12.2 and Windows 7.

Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is "admin" and password is "admin".

Step 2. Set your firewall's WAN settings as per Internet provider requirements.

In our example WAN is set to PPPoE.

Step 3. Add a new object into the Address Book: "L2TP_Over_IPSec_Pool".

Specify the range of IP addresses which will be assigned to the clients connecting via L2TP. These addresses should be from the IP subnet used on your LAN. Make sure this range does not conflict with the range used by the DHCP Server on your LAN.

	Status S	System	Objects	Network	Policies	
▼ General Address Book Services	Objects » Gene L2TP_O Use an IP4 Ado	ral » Address Ver_IPS dress item to	Book » Interface ec_Pool define a name fo	Addresses » L2TP_O or a specific IP4 host	ver_IPSec_Pool , network or range.	
Key Ring Address Pool Pools NAT Pools	General	User A	Name: L2 Address: 192	P_Over_IPSec_Pool 2.168.10.150-192.168.10.	160	
VPN Objects LDAP IKE Config Mode Pool IKE ID Lists		(Comments:			ОК

Step 4. Add a new object into the Address Book: "L2TP_Over_IPSec_Server". This address should be unique and from the IP subnet used on your LAN.

	Status	System	Objects	Network	Policies	
▼ General	Objects » Ge	neral » Addres	s Book » Interfa	aceAddresses » L2TP_O	Dver_IPSec_Server	
Address Book	L2TP C	Over IPS	Sec Serv	/er		
Services	Use an IP4 A	Address item to	o define a name	e for a specific IP4 host	t. network or range.	
ALG						
Key Ring	Gener	ral User	Authenticatior	1		
▼ Address Pool			News	1075 0 150 0		
IP Pools			Name:	L2TP_Over_IPSec_Server		
NAT Pools			Address:	192.168.10.200		
▼ VPN Objects			Comments:			
LDAP						
IKE Config Mode Pool						_
IKE ID Lists					ок	

Step 5. Go to Object->Key Ring.
Add a Pre-Shared Key.
Enter a name e.g. "L2TP_PSK".
Shared Secret Type – set as Passphrase then enter the shared secret.

	Status	System Object	ts Network	Policies	
' General	Due Oh				
Address Book	Pre-Sha	ared Key			
Services	PSK (Pre-Sh	ared Key) authentication is	s based on a shared secret t	nat is known only by the parties invol	ved.
ALG	ļ	Name:	L2TP_PSK		
Key Ring	1				
Address Pool	Shared Secu	ret			
IP Pools	Shared Sect				
NAT Pools		Туре:	Passphrase 💌		
VPN Objects		Charad Coarat			
LDAP		Confirm Secret			
IKE Config Mode Pool		Commissecret.	A PSK containing non-	ASCII characters might be encoded (differently on other systems
IKE ID LISTS			and cause a mismatch, e.g	y. Windows uses UTF-16 while this O d phrases are vulnerable to dictionar	S uses UTF-8.
IPsec Algorithms			shared secrets.	d phrases are vallerable to dictional	y attacks, do not use them as
CRI Distribution Point Lists		Comments			
		oonnonto.			
D-Link					
D-Link	Status	System	Objects Netw	rork Policies	
D-Link	Status	System	Objects Netw	rork Policies	-
D-Link	Status	System	Objects Netw	vork Policies	
D-Link General Address Book	Status Objects	System	Objects Netw	vork Policies	
D-Link General Address Book Services	Status Objects Key	System » General » Key Ring Ring	Objects Netw	vork Policies	
D-Link General Address Book Services ALG	Status Objects Key	System » General » Key Ring Ring	Objects Netw	vork Policies	
D-Link General Address Book Services ALG Key Ring	Status Objects Key + Add	System » General » Key Ring Ring •	Objects Netw	vork Policies	
Ceneral Address Book Services ALG Key Ring Address Pool	Status Objects Key + Add # •	System » General » Key Ring Ring •	Objects Netw	rork Policies	Туре
Ceneral Address Book Services ALG Key Ring Address Pool IP Pools	Status Objects Key + Add # •	System » General » Key Ring Ring Name Auth_agent_psk	Objects Netw	rork Policies Type Pre-Shared Key	Type Hexadecin
Ceneral Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools NAT Pools	Status Objects Key + Add # •	System System General » Key Ring Ring Name auth_agent_psk HTTPSAdminCert	Objects Netw	rork Policies Type Pre-Shared Key Certificate	Type Hexadecim
D-Lintk General Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects	Status Objects Key + Add # 1 2	System » General » Key Ring Ring Name auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netw	rork Policies	Type Hexadecim Local
D-Link General Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects LDAP	Status Objects Key + Add # 1 2 3	System Seneral » Key Ring Ring Name auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netw	Vork Policies	Type Hexadecim Local Passphrase
Ceneral Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects LDAP IKE Config Mode Pool	Status Objects Key + Add # 1 1 2 3	System Seneral » Key Ring Ring Name auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netwo	Vork Policies	Type Hexadecim Local Passphrase
 D-Lintk General Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects LDAP IKE Config Mode Pool IKE ID Lists 	Status Objects Key + Add # 1 2 3	System Seneral » Key Ring Ring Name Auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netwo	Vork Policies	Type Hexadecim Local Passphrase
 D-Link General Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects LDAP IKE Config Mode Pool IKE ID Lists IKE Algorithms 	Status Objects Key + Add # • 1 2 3	System Seneral » Key Ring Ring Name auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netwo	rork Policies	Type Hexadecim Local Passphrase
 D-Link General Address Book Services ALG Key Ring Address Pool IP Pools NAT Pools VPN Objects LDAP IKE Config Mode Pool IKE Config Mode Pool IKE Algorithms IPsec Algorithms 	Status Objects Key + Add #• 1 2 3	System Seneral » Key Ring Ring Name auth_agent_psk HTTPSAdminCert L2TP_PSK	Objects Netwo	rork Policies	Type Hexadecirr Local Passphrase

Step 6. Go to Network->Interfaces and VPN->VPN and Tunnels->IPSec then add an IPSec Tunnel.

Name – Enter a name e.g. "L2TP_IPSec_Interface".

IKE Version – set as IKEv1.

Encapsulation Mode – set as Transport.

	Status System Objects Network Policies
	Interfaces and VPN Routing Network Services
▼ Link Layer	Network » Interfaces and VPN » VPN and Tunnels » IPsec » L2TP_IPSec_Interface
Ethernet	L2TP IPSec Interface
Link Aggregation	An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.
VLAN	
PPPoE	General Authentication IKE (Phase-1) IPsec (Phase-2) Virtual Routing Advanced
ARP/Neighbor Discovery	
▼ VPN and Tunnels	Name: L2TP_IPSec_Interface
IPsec	IKE Version: IKEv1
SSL	Encapsulation Mode: Transport
PPTP/L2TP Servers	
L2TPv3 Servers	IVE Deer
PPTP/L2TP Clients	IKE Peer
L2TPv3 Clients	Remote Endpoint: (None)
GRE	
6in4	
 Miscellaneous 	Comments:
Loopback	
Switch Management	OK Cancel

Step 6.1. Under Authentication Tab, select Pre-Shared Key in the Authentication Method and L2TP_PSK that you add in **Step 5.**

	Status S	System Objec	ts Network	Policies		
	Interfaces and VF	PN Routing	Network Services			
▼ Link Layer Ethernet Link Aggregation	Network » Interfa	aces and VPN » VPN and Sec_Interface I item is used to define IF	Tunnels » IPsec » L2Ti Psec endpoint and will a	P_IPSec_Interface	erface in the system.	
PPPoE	General	Authentication	IKE (Phase-1)	IPsec (Phase-2)	Virtual Routing	Advanced
▼ VPN and Tunnels		Authentication Method:	Pre-shared Key 💌			
SSL PPTP/L2TP Servers	Pre-Shared Ke	еу				
L2TPv3 Servers PPTP/L2TP Clients		Pre-shared key:	P L2TP_PSK *			
L2TPv3 Clients GRE	Authenticated	Identities				
6in4 ▼ Miscellaneous		Local ID:				
Loopback Switch Management		Enforce local ID:				

Step 6.2. Under IKE (Phase-1) and IPSec (Phase-2) tabs, select Deprecated Medium as Algorithm.

▼ Link Layer	Network » Interfaces a	nd VPN » VPN and 1	Tunnels » IPsec » L2T	P IPSec Interface			
Ethernet	12TP IPSec	Interface					
Link Aggregation	An IPsec tunnel item	is used to define IPs	sec endpoint and will a	appear as a logical inte	erface in the system.		
VLAN			·				
PPPoE	General	Authentication	IKE (Phase-1)	IPsec (Phase-2)	Virtual Routing	Advanced	
ARP/Neighbor Discovery							
 VPN and Tunnels 							
IPsec	Proposal						
SSL	Diff	ie-Hellman group:					
PPTP/L2TP Servers			Available		Selected		
DETE/LICE Clients			01 (768-bit) 05 (1536-bit)		<pre> 02 (1024-bit) </pre>		•
12TPv3 Clients			14 (2048-bit) 15 (3072-bit)				
GRE			16 (4096-bit)				
6in4			18 (8192-bit)		-		-
 Miscellaneous 							
Loopback			Tincidde		× Remove	<u> </u>	
Switch Management		Algorithms	Depres ated Med				
Interface Groups		Lifetime:	28800			seconds	
		Endanie.	20000			3000103	
		Mode:	Main mode 💌				
	IKE Peers Settings						
	Outgo	ing Routing Table:	😸 main 💌				
		Local Endpoint:	(None) *				
Copyright © D-Link	Incomi	ng Interface Filter:	🌉 any 👻				
Link Layer	Network » Interface:	s and VPN » VPN a	and Tunnels » IPsec »	L2TP_IPSec_Interfac	е		
Ethernet	L2TP_IPSe	ec_Interfac	e				
Link Aggregation	An IPsec tunnel ite	m is used to define	e IPsec endpoint and	will appear as a logi	cal interface in the sy	stem.	
VLAN							
PPPoE	General	Authentication	IKE (Phase-1	IPsec (Phase	-2) Virtual Rou	ting Advanced	kk
ARP/Neighbor Discovery							
VPN and Tunnels							
IPsec	Proposal						
SSL	Derfe						
PPTP/L2TP Servers	Репе	ect Forward Secred	Available		Selected		
L2TPv3 Servers			14 (2048-bit)		 None (No 	PFS)	
PPTP/L2TP Clients			15 (3072-bit) 16 (4096-bit)		01 (768-6 02 (1024-	bit)	
L2TPv3 Clients			17 (6144-bit) 18 (8192-bit)		05 (1536-	bit)	
GRE							
6in4					-		-
Miscellaneous			+ Include		× Remov	e	~
Loopback						_	
Switch Management		Algorithm	IS: Deprecated-Me	5 -			
Interface Groups		Lifetim	ie: 3	600		seconds	
		Lifetim	e:	0		kilobytes	
						-	
	Drotastad Not	rko Catting -					
	Protected NetWO	rks Settings					
		Setup SA pe	EF: Network	*			
		Config Mode Po	OI: (None)	*			

Tink Lawa							
Link Layer	Network » Interfac	es and VPN » VPN and	Tunnels » IPsec » L2	TP_IPSec_Interface			
Ethernet	L2TP_IPS	ec_Interface					
Link Aggregation	An IPsec tunnel it	em is used to define IF	osec endpoint and wi	ll appear as a logical in	terface in the system.		
VLAN	_						
PPPoE	General	Authentication	IKE (Phase-1)	IPsec (Phase-2)	Virtual Routing	Advanced	
ARP/Neighbor Discovery							
 VPN and Tunnels 							
IPsec	Routing						
SSL			_				
PPTP/L2TP Servers	A	dd route dynamically:					
L2TPv3 Servers		Add route statically:		_			
PPTP/L2TP Clients		Plaintext MTU:	1420	0			
L2TPv3 Clients							
GRE	Tunnel Monitor						
6in4							
▼ Missellancous		Tunnel Monitoring:					
 Inscendence 							
Ecopback Switch Management	IP Addresses						
Switch Management							
Interface Groups			 Automatically p 	ick the address of a loc	al interface that corres	ponds to the local net.	
			 Specify address 	s manually:			
						OK Cancel	
	Status System	Objects Ne	etwork Policie	S			
	Interfaces and VPN	Routing Network Se	rvices				
							_
▼ Link Layer	Network » Interfaces and VF	PN » VPN and Tunnels » IPs	sec				
Link Aggregation	IPsec						
	Manage the IPsec tunnel in	nterfaces used for establish	ning IPsec VPN connection	ons to and from this system	1.		
PPPoE	+ Δdd -	Advanced Settings					Fil
ARP/Neighbor Discovery		, rataneou oounigo					
▼ VPN and Tunnels	# Name	Local Net	Remote Net	Remote Er	ndpoint Local En	dpoint Auth	
IPsec	1 IL2TP_IPSec_Inte	erface				Pre-shared Ke	У
SSL							
PPTP/L2TP Servers							A
L2TPv3 Servers							

Step 6.3. Under Advanced tab, tick Add route dynamically. Then Press the OK button.

Step 7. Go to Network->Interfaces and VPN->VPN and Tunnels->PPTP/L2TP Servers. Add a new PPTP/L2TP Server.

Inner IP Address – set as "L2TP_Over_IPSec_Server" you added in **Step 4**. Tunnel Protocol – L2TP.

Outer Interface Filter – set as "L2TP_IPSec_Interface" you added in **Step 6**.

Server IP – set as iinet_ip (the PPPoE interface ip in this example).

	Status System Objects Network Policies	
	Interfaces and VPN Routing Network Services	
▼ Link Layer Ethernet Link Aggregation	Network » Interfaces and VPN » VPN and Tunnels » PPTP/L2TP Servers » L2TP_Interface L2TP_Interface	
VLAN	A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.	
PPPoE	General PPP Parameters Add Route Virtual Routing	
ARP/Neighbor Discovery		
▼ VPN and Tunnels	Name: L2TP_Interface	
IPsec		
SSL		
PPTP/L2TP Servers	Outer Interface Filter:	
L2TPv3 Servers	Server IP: 4 iinet_ip	
PPTP/L2TP Clients	Comments:	
L2TPv3 Clients		
GRE		
6in4	ОК С	ancel

Step 7.1. Under PPP Parameters.

IP Pool – set as "L2TP_Over_IPSec_Pool" you added in **Step 3** and set the Primary and Secondary DNS.

	Status Sys	stem Object	s Network	Policies
	Interfaces and VPN	Routing	Network Services	
▼ Link Layer	Network » Interface	s and VPN » VPN and	Tunnels » PPTP/I 2TF	2 Servers » 12TP Interface
Ethernet		rface		
Link Aggregation		ver interface terminate	e PPP (Point to Poin	t Protocol) tunnals sat un over existing ID networks
VLAN	AFFIF/LZIF SCI	ver interface terminate		it Protocol) tunnels set up over existing iP networks.
PPPoE	General	PPP Parameters	Add Route	Virtual Routing
ARP/Neighbor Discovery				
▼ VPN and Tunnels	Specify if User Aut the DNS/WINS ser	hentication Rules are to ver information to hand	o be used, and the e I out to connected cl	ncryption strengths allowed. Also specify the IP address assignment and ients.
IPsec				_
SSL				Use User Authentication Rules
PPTP/L2TP Servers				
L2TPv3 Servers	Microsoft Point-	To-Point Encryption	(MPPE)	
PPTP/L2TP Clients				
L2TPv3 Clients				✓ None
GRE				✓ RC4 40 bit
6in4				RC4 56 bit
▼ Miscellaneous				RC4 128 bit
Loopback				Stateful MPPE (less secure, use only for compatibility)
Switch Management				
Interface Groups	IP Pool			
		IP Pool:	4 L2TP_Over_IPSe 💌	
			Primary	Secondary
		DNS:	🔄 iinet_dns1 💌	8.8.8.
		NBNS/WINS:	(None) 👻	(None)
Copyright © D-Link				OK Cancel

Step 7.2. Under Add Route tab. Filter – set as "all-nets" Proxy ARP – include "lan" Then press OK button.

	Status System Obje	ects Networ	k Policies		
	Interfaces and VPN Routing	Network Services			
▼ Link Layer Ethernet	Network » Interfaces and VPN » VPN a	nd Tunnels » PPTP/L21	TP Servers » L2TP_In	terface	
Link Aggregation	A PPTP/L2TP server interface termin	ates PPP (Point to Po	pint Protocol) tunnels	set up over existing I	P networks.
PPPoE	General PPP Parameter	s Add Route	Virtual Routing		
VPN and Tunnels					
IPsec	Filter				
SSL PPTP/L2TP Servers	Allowed Network	S: 4 all-nets	•		
L2TPv3 Servers PPTP/L2TP Clients	Proxy ARP				
L2TPv3 Clients GRE 6in4	Proxy ARP interface	S: Available		Selected	
Miscellaneous Loopback		dmz L2TP_IPSec_LAN_ wan1 wan2	<u>G</u> roup	▲ Ian	
Switch Management		+ Include		▼ Kemove]
Sta	tus System Objects Network	Policies			
Link Layer Ne Ethernet P Link Aggregation Ad	twork. » Interfaces and VPN. » VPN and Tunnels. » PPTP/L2TP S PTP/L2TP Servers Id, remove and configure PPTP/L2TP (Point-to-Point Tunneli	ervers ng Protocol / Layer 2 Tunneli	ng Protocol) servers used f	or terminating PPTP/L2TP-t	pased VPN tunne
PPPoE +	Add				I
VPN and Tunnels	Name Tunnel protocol Jords server PPTP	Inner IP address	Outer interface	IP pool	Outer server II
IPsec SSL	2 KL2TP_Interface L2TP	L2TP_Over_IPSec_Server	L2TP_IPSec_Interface	L2TP_Over_IPSec_Pool	iinet_ip
PPTP/LZTP Servers L2TPv3 Servers PPTP/L2TP Clients					6

Step 8. Go to Network->Interfaces and VPN->Miscellaneous->Interface Groups. Add interface groups for "L2TP_Interface" (added in **Step 7**) and "lan"

	Status	System	Objec	ts Network	Policies	
1	Interfaces ar	Id VPN R	outing	Network Services		
▼ Link Layer	Interfa	ce Group				
Link Aggregation	Use an inte	erface group to c	ombine seve	ral interfaces for a simplifie	d security policy.	
VLAN						
PPPoE			Name:	L2TP_IPSec_LAN_Gro	wivalant	
ARP/Neighbor Discovery				Security/Transport Ed	uivalent	
▼ VPN and Tunnels						
IPsec	Interfaces					
SSL				Accellette		Colored
PPTP/L2TP Servers				Available		Selected
L2TPv3 Servers				dmz	<u> </u>	lan
PPTP/L2TP Clients				iinet L2TP_IPSec_Interface		
GRE				pptp_server wan1		
6in4				wan2	-	-
 Miscellaneous 				+ Include		× Remove
Loopback						
Switch Management			Comments:			
Interface Groups						
						OK Cancel
1	Status Interfaces an	System	Object	Network	Policies	
▼ Link Layer	Notwork » I	stafaaaa and VD	L » Misseller	aug y Interface Cround		
Ethernet	Interfa			eous » interiace Groups		
Link Aggregation	Use interfa	ce aroups to com	bine several	interfaces for simplified pol	icv management.	
VLAN		<u> </u>				
PPPoE	+ Add	-				
ARP/Neighbor Discovery	# • N	ame			Members	
▼ VPN and Tunnels	1 3	L2TP_IPSec_LAN	Group		L2TP_Interface	, lan
IPsec					_	
DDTD/I 2TD Servers						
12TPv3 Servers						
PPTP/L2TP Clients						
L2TPv3 Clients						
GRE						
6in4						
 Miscellaneous 						
Loopback						
Switch Management						
Interface Groups						

Step 9. Go to Policies->Firewalling->Rules->Main IP Rules. Create a new IP Rule to allow L2TP Tunnel communication with LAN:

Set Action as "Allow".

Set Source Interface/Network as "L2TP_IPSec_LAN_Group"/all-nets.

Set Destination Interface/Network as "L2TP_IPSec_LAN_Group"/all-nets.

Service: all_services.

Then press OK button.

			00,000	Network	Policies		
	Firewalling	User Auth	entication Intr	usion Prevent	ion Traffic M	Manageme	ent
Rules Main IP Rules Additional IP Rule Sets Application Rule Sets	Policies » Fire L2TP_IF An IP rule spe	walling » Ru PSec_A ecifies what a	les » Main IP Rules » Ilow action to perform on n	L2TP_IPSec_/	Allow that matches the s	pecified fi	lter criteria
▼ Profiles	Gener	al					
Anti-Virus					``````````````````````````````````````		
Email Control			Name: L2TP_	IPSec_Allow	ļ		
File Control			A stimu		1		
Geolocation Filter			Action: Allow	*	ļ		
Schedules							
VolD	Address Filte	er					
Web							
web			Interfa	ce	Network		
			Source: Source:	[P_IPSec_LA ▼	4 all-nets	-	
			Destination:	TP_IPSec_LA 🔻	4 all-nets	-	
			Ourier 💽 r		1		
			Service:	services 💌	ļ		
			Schedule: (None)	-	ļ		
	Application C	ontrol					
			ation Control:	DFF			
		Applica					
		Applica					
		Applica					
	Status Syste	Applica m Ob	jects Network	Policie	s		
	Status Syste	Applica m Ob	jects Network	Policie	s c Management		
	Status Syste	Applica m Ob Authentication	jects Network	Policie tion Traffi	s c Management		
▼ Rules	Status Syste Firewalling User Policies » Firewalling »	Applica m Ob Authentication	jects Network	Policie tion Traffi	s c Management		
▼ Rules Main IP Rules	Status Syste Firewalling User Policies » Firewalling » Main IP Rule	Applic: m Ob Authentication Rules » Main	jects Network	Policie tion Traffi	s c Management		
▼ Rules Main IP Rules Additional IP Rule Sets	Status Syste Firewalling User Policies » Firewalling » Main IP Rule IP rules are used to fi	Applica m Ob Authentication Rules » Main S Iter IP-based n	jects Network Intrusion Preven P Rules etwork traffic. In addition	Policie tion Traffi	s c Management	slation as we	ell as Server Lo
Rules Main IP Rules Additional IP Rule Sets Application Rule Sets	Status Syste Firewalling User Policies » Firewalling » Main IP Rule IP rules are used to fi	Applic: m Ob Authentication Rules » Main S Iter IP-based n	jects Network	Policie tion Traffi	c Management	slation as we	ell as Server Lo
▼ Rules Main IP Rules Additional IP Rule Sets Application Rule Sets ▼ Profiles	Status Syste Firewalling User Policies » Firewalling » Main IP Rule IP rules are used to fi + Add •	Applica m Ob Authentication Rules » Main S Iter IP-based n	jects Network Intrusion Preven P Rules etwork traffic. In addition	Policie tion Traffi	c Management	slation as we	ell as Server Lo.
 Rules Main IP Rules Additional IP Rule Sets Application Rule Sets Profiles Anti-Virus 	Status Syste Firewalling User Policies » Firewalling » Main IP Rule IP rules are used to fir + Add •	Applica m Ob Authentication Rules » Main S Iter IP-based n	jects Network Intrusion Preven P Rules etwork traffic. In addition	Policie tion Traffi , they provide me	c Management	Dest Net	ell as Server Lo.
 ▼ Rules Main IP Rules Additional IP Rule Sets Application Rule Sets ▼ Profiles Anti-Virus Email Control 	Status Syste Firewalling User Policies » Firewalling » Main IP Rule IP rules are used to fi + Add • # • Name 1 • 1072 IPS	Applica m Ob Authentication Rules » Main S Iter IP-based n	jects Network Intrusion Preven P Rules etwork traffic. In addition	Policie tion Traffi , they provide me Src Net Det	s c Management eans for address trans	Dest Net	ell as Server Lo. Service
 Rules Main IP Rules Additional IP Rule Sets Application Rule Sets Profiles Anti-Virus Email Control File Control 	Status System Firewalling User Policies > Firewalling > Main IP Rule IP rules are used to fire + Add # Name 1 L2TP_IPS	Application Authentication Rules » Main P Rules » Main Comparison Rules a Main Comparison Compa	jects Network Intrusion Preven P Rules etwork traffic. In addition Src If	Policie tion Traffi , they provide me Src Net Des all-nets at L	s c Management eans for address trans at If 2TP_IPSec_LAN_Group	Dest Net	ell as Server Lo Service
 Rules Main IP Rules Additional IP Rule Sets Application Rule Sets Profiles Anti-Virus Email Control File Control Geolocation Filter 	Status Syste Firewalling User Policies > Firewalling > Main IP Rule IP rules are used to fin + Add # • Name 1 • L2TP_IPSr 2 • ping_fw	Application Authentication Rules » Main P Rules » Main P Rules v Main P R	jects Network Intrusion Preven P Rules etwork traffic. In addition Src If I L2TP_IPSec_LAN_Group Ian	Policie tion Traff they provide me Src Net Des all-nets all L allanet all c	c Management c Management eans for address trans st If 2TP_IPSec_LAN_Group ore	Dest Net	ell as Server Lo Service al all_tcpudpicn aping-inbound
 Rules Main IP Rules Additional IP Rule Sets Application Rule Sets Profiles Anti-Virus Email Control File Control Geolocation Filter Schedules 	Status System Firewalling User Policies > Firewalling > Main IP Rule IP rules are used to fit + Add # Name 1 L2TP_IPSe 2 ping_fw 3 a lan_to_ward	Application Authentication Rules » Main P S Iter IP-based n Compared to the second Compared to t	jects Network Intrusion Preven P Rules etwork traffic. In addition Src If I L2TP_IPSec_LAN_Group	Policie tion Traff they provide me Src Net Des all-nets all L allanet all c	c Management c Management cans for address trans st If 2TP_IPSec_LAN_Group ore	Dest Net	ell as Server Lo Service 3 all_tcpudpicn 4 ping-inbounc

Step 10. Go to System->Device->Users->Local User Database.

Add Local User Database.

Enter a name e.g. L2TP_users.

	Status System Objects Network Policies
	Device Advanced Settings
▼ Device	System » Device » Users » Local User Databases » L2TP_Users
Date and Time	12TP Users
DNS	A local user database contains user accounts used for authentication purposes.
Remote Management	· · · · · · · · · · · · · · · · · · ·
Log and Event Receivers	General Users
▼ Monitoring	
Hardware Monitoring Setting:	Name: L2TP_Users
Link Monitors	Comments:
Real-Time Monitor Alerts	
▼ Users	
Local User Databases	ОК

Step 10.1. Go to Users tab then enter l2tp username and password. Then press OK button.

	Status	System	Objects	Network	Policies
	Device	Advanced Setti	ings		
▼ Device					
Date and Time	User				
DNS	User cred etc	entials may be use	ed in User Auth	entication Rules, wh	ich in turn are used in e.g. PPP,
Remote Management	0.0				
Log and Event Receivers	Ge	eneral SSH P	ublic Key		
 Monitoring 					
Hardware Monitoring Settings			Name:	2tpuser	
Link Monitors			Password:		
Real-Time Monitor Alerts			_	Very Weak	
▼ Users		Confirm	Password:		
Local User Databases			Groups:		
	Comma Users that Users that Add admi	a separated list of g are members of th are members of th nistrators Ad	groups ne 'administrato ne 'auditors' gro d auditors	ors' group are allowe oup are only allowed	ed to change the firewall configur to view the firewall configuration
	Per-User	IP Configuration	n (For PPTP,	L2TP And SSL V	PN)
		Static Client I	P Address: (None) 🔻	
		Networks b	ehind user:	None) 🔻	
		Metric fo	r networks:]	
Copyright © D-Link			Comments:		

	Status	System	Objects	Network	Policies	
	Device	Advanced Setti	ngs			
Device	System	» Device » Users » L	.ocal User Databa	ses		
Date and Time	Loca	l User Data	bases			
DNS	Manage	the local user datab	ases and user a	counts used for au	thentication purposes	\$
Remote Management	manage				anonaoaaon parpooo	
Log and Event Receivers	+ Add	•				
 Monitoring 						
Hardware Monitoring Settings	# •	Name				C
Link Monitors	1	🔩 AdminUsers				
Real-Time Monitor Alerts	2	🚘 pptp_user				
▼ Users	3	Sector L2TP_User				
Local User Databases	,					

Step 11. Go to Policies->User Authentication->Rules->Authentication Rules.

Add User Authentication Rule.

Name: L2TP_Auth.

Authentication agent – set as L2TP/PPTP/SSL VPN.

Authentication Source – set as Local.

Interface – set as "L2TP_Interface" added in **Step 7**.

Originator IP – set as "all-nets".

Terminator IP – set as "iinet_ip" (PPPoE interface ip in this example).

	Status	System	Objects	s Networ	c I	Policies		
[Firewalling	User Authe	ntication	Intrusion Preve	ntion	Traffic Managem	ent	
▼ Rules Authentication Rules	Policies » Us	ser Authentication Auth	» Rules » Au	uthentication Rules ×	L2TP_Au	th		
Authentication Agents Vuser Directories	The User Au	uthentication Rul	eset specifies	from where users	are allow	ed to authenticate to	o the system, and ho	W.
LDAP RADIUS	Gene	eral Log S	Name	Authentication O	ptions	Accounting	Agent Options	Restrictions
▼ Accounting RADIUS		Authentica	ation agent:					
▼ Settings		Autoenticati	Interface:	L2TP_Interface				
Automotion Sectings		Ter	minator IP:	4 iinet_ip	•			
		(Comments:					
								OK Cancel

Step 11.1. Go to Authentication Options tab, select L2TP_user as Local User DB then press OK button.



Step 12. After the configuration is done, click "Configuration" in main bar and select "Save and Activate".

Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall's LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

	Setup Wizard 🚺 🔅 Configuration 🚺	Notifications 0 🎝 admin
Status System	The configuration has been changed.	
Run-time Information M	Save and Activate	
	View Changes	
Save Configurat	Discard changes	
Save and activate changes n		

Save and Activate

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Note: Due to configuration changes the currently active user admin (192.168.10.151) will no longer be automatically logged on after the activation of the new configuration. You will need to manually login with an administrator user account to verify the new configuration.

OK Cancel

Android 5.0 Settings.

1.0 Go to Settings->Connections->More Networks->VPN.



1.1 Add a new L2TP/IPSec PSK Profile and enter the L2TP server public IP address and Pre-Shared Key (entered in **Step 5**) then Save.

¢	Add VPN	-
D L2	Name DSR-1000AC	
D: L2	Type L2TP/IPSec PSK ▼	
	Server address 123.123.123.123	
	L2TP secret Not used	
	IPSec identifier Not used	
	IPSec pre-shared key	
	Show advanced options	
	CANCEL SAVE	

1.2 Press the L2TP/IPSec Profile you added to connect. Enter the L2TP username and password you added in **Step 10**.



You should see a Key icon on the top-left hand corner that indicates it is connected.



IOS v10.3 (iPhone 7 Plus running) Settings:

2.0 Go to Settings->VPN->Add VPN Configuration:

Description – set as DFL.

Account – enter the L2TP username added **Step 10**. Password – enter the L2TP password added **Step 10**. Secret – enter the shared secret in **Step 5** then click **Done**.



2.1 Select DFL and enable the **Status** to connect.

•০০০ vodafone AU 🗢 🕅	1:08 PM	* 88% 💷)		
Settings	VPN			
VPN CONFIGURATION	NS			
Status	Conne	ected		
🗸 DFL		(i)		
Unknown			• vodafone AU 🗢 VPN 1:08 P	M 🕴 88% 🗖
Home Unknown		<u>(</u>)	VPN DFL	Edit
Hotspot Shiel	d VPN			
HotspotVPN		U	Туре	L2TP
PERSONAL VPN			Server	
Status	Not Conne	ected	Account	l2tpuser
			Assigned IP Address	192.168.10.154
Hotspot Shiel HotspotVPN	d VPN	<u>(</u>)	Connect Time	0:24
Add VPN Configu	iration		Delete \	/PN

MAC OS Sierra v10.12.2 Settings.



3.0 Go to System Preferences->Network then click on the (+) sign to add a new connection.

Interface – set as VPN. VPN type – set as L2TP Over IPSec.

Service name – enter a name you prefer e.g. DFL_L2TP then click Create.

	Network	Q Search
S	elect the interface and enter a name fo	or the new service.
• Wi-Fi	Interface: VPN	•
Bluetooth PAN Not Connected	Service Name: DFL_L2TP	connected.
• Ethernet Not Connected		Cancel Create
• 802.11n NIC Not Connected	IP Address:	
Thundet Bridge Not Connected	Router:	
	DNS Server:	
	Search Domains:	
(+)- ☆~		Advanced ?
\smile		Assist Me Revert Apply

	Network	Q Search
Locati	on: Automatic	`
• Wi-Fi Connected	Status: Not Connected	
Not Connected Mot Connected Not Connected	Configuration: DFL	○
• 802.11n NIC Not Connected	Server Address: 123.123.123.123 Account Name: I2tpuser	3
Thundet Bridge> Not Connected DFL_L2TP Not Connected	Authentication S Connect	Settings
+ - 8.	Show VPN status in menu bar	Advanced ?
1 W 1	Assist Me	Revert Apply

3.1 Enter a Configuration name, Server Address and the L2TP username added in **Step 10**.

3.2 Click on "Authentication Settings..." then enter the L2TP user password added in **Step 10** and "Shared Secret" added in **Step 5** then Press OK.

	Network	Q Search
Wi-Fi Connected DFL_L2TP Connected Bluetooth PAN Not Connected Ethernet Not Connected 802.11n NIC Not Connected Thundet Bridge Not Connected	User Authentication: Password: RSA SecurID Certificate Select Kerberos CryptoCard Machine Authentication: Shared Secret: Certificate Select Group Name: (Optional) Cancel OK	nt:
+ - *	Show VPN status in menu bar Assist Me	Advanced ? Revert Apply

3.3 Click **Connect** button to established a connection.

$\bullet \bullet \circ \checkmark $	Network	Q Search	8 ⊖ ○ < >		Network	Q Search
Loca	ation: Automatic			Location:	Automatic	•
• Wi-Fi Connected Image: Connected • Bluetooth PAN Image: Connected • Ethernet Not Connected Image: Connected • 802.11n NIC Image: Connected • Not Connected Image: Connected	Status: Not Connected Configuration: DFL Server Address: 123.123.123 Account Name: 12tpuser	8	Wi-Fi Connected DFL_L2TP Connected Bluetooth PAN Not Connected Ethernet Not Connected	 ? ?<	Status: Connected Connect Time: 0:04:35 IP Address: 192.168.10.151 Configuration: DFL L2TP Over IPS Server Address: 202.100, 106, 107 Account Name: I2tpuser	Sent: ####################################
Not Connected	Authentication Settin Connect	gs	BUZ-IIT NIC Not Connected Thundet Bridge Not Connected	<>	Authentication Se Disconnect	Advanced 2
+ - •	Assist Me	Revert Apply	+ - &-		Assist Me	Revert Apply

Windows L2TP Client Settings:

4.0 Go to Properties of the VPN connection, enter the WAN ip address of the DFL.



4.1 Go to Security tab:

Type of VPN – set as L2TP/IPSec.

Data Encryption – set as Optional encryption

Click on Advanced Settings then enter the L2TP Shared key added in Step 5.



4.2 Enter the L2TP username and password added in **Step 10** then click **Connect**.

User name:	12tpuser
Password:	•••••
2 N	
Domain:	