## How to setup L2TP Over IPSec VPN Service in DSR-250V2



Access to LAN via L2TP VPN tunnel



# **Configuration Steps:**

- Create IPSec VPN Profile Policy.
- Enable L2TP Server.
- Add user database.
- Configure Windows as L2TP client.

### Step 1. Go to VPN > IPsec profiles.

Create a new IPSec Policy. Use the below example as a guide.

Enter a Profile name, select the settings below and enter your desired Pre-shared Key.

<b>D-Littk</b> Building Networks for People	DSR-250v2	
	Edit new IKE	
System and status		
음 Administration	Profile name	L2TP
Authentication	IKE version	● IKEv1 ◯ IKEv2
昰 Interface	IKE phase-1 settings	
୍ଦ୍ୟ Network		
招 Firewall	Exchange mode	Main
🛈 Security	Local identifier type	Local WAN IP
🖭 VPN	Remote identifier type	Remote WAN IP +
IPsec profiles	DH group	
	0	Group 2 (1024 bit) -
IPsec site to site	5	Group 2 (1024 bit)
IPsec site to site	Encryption	3DES x AES-128 x
IPsec site to site IPsec client to site IPsec 1 to 1 mapping	Encryption Authentication algorithm	3DES X AES-128 X • SHA-1 X •
IPsec site to site IPsec client to site IPsec 1 to 1 mapping PPTP	Encryption Authentication algorithm	3DES x     AES-128 x       SHA-1 x
IPsec site to site IPsec client to site IPsec 1 to 1 mapping PPTP L2TP	Encryption Authentication algorithm SA lifetime	Group 2 (1024 bit)     •       3DES x AES-128 x     •       SHA-1 x     •       28800     seconds
IPsec site to site IPsec client to site IPsec 1 to 1 mapping PPTP L2TP OpenVPN	Encryption Authentication algorithm SA lifetime Authentication method	Group 2 (1024 bit)     3DES x AES-128 x     SHA-1 x   28800   seconds   Pre-shared Key
IPsec site to site IPsec client to site IPsec 1 to 1 mapping PPTP L2TP OpenVPN GRE	Encryption Authentication algorithm SA lifetime Authentication method Pre-shared Key	Group 2 (1024 bit) • 3DES x AES-128 x • SHA-1 x • 28800 seconds Pre-shared Key •

	Encryption	3DES X AES-128 X	*
System and status	Authentication algorithm	SHA-1 x	•
Administration			
<b>.</b>	SA lifetime	28800	seconds
	Authentication method	Pre-shared Key	•
류, Interface			
ഹി Network	Pre-shared Key	•••••	Þ
	Dead peer detection		
器 Firewall			
<ol> <li>Security</li> </ol>	Extended authentication		
🖳 VPN	IKE phase-2 settings		
VPN IPsec profiles	IKE phase-2 settings		
VPN IPsec profiles IPsec site to site	IKE phase-2 settings Protocol selection	ESP	•
VPN IPsec profiles IPsec site to site IPsec client to site	IKE phase-2 settings Protocol selection Encryption algorithm	ESP	•
VPN  IPsec profiles  IPsec site to site  IPsec client to site  IPsec 1 to 4 managing	IKE phase-2 settings Protocol selection Encryption algorithm	ESP 3DES X AES-128 X	•
VPN         IPsec profiles         IPsec site to site         IPsec client to site         IPsec 1 to 1 mapping	IKE phase-2 settings Protocol selection Encryption algorithm Authentication algorithm	ESP 3DES X AES-128 X SHA-1 X	•
<ul> <li>VPN</li> <li>IPsec profiles</li> <li>IPsec site to site</li> <li>IPsec client to site</li> <li>IPsec 1 to 1 mapping</li> <li>PPTP</li> </ul>	IKE phase-2 settings Protocol selection Encryption algorithm Authentication algorithm	ESP 3DES x AES-128 x SHA-1 x	•
VPN         IPsec profiles         IPsec site to site         IPsec client to site         IPsec 1 to 1 mapping         PPTP         L2TP	IKE phase-2 settings Protocol selection Encryption algorithm Authentication algorithm SA lifetime	ESP 3DES x AES-128 x SHA-1 x 3600	•     •     •     •     •     •     •     seconds
VPN         IPsec profiles         IPsec site to site         IPsec client to site         IPsec 1 to 1 mapping         PPTP         L2TP         OpenVPN	IKE phase-2 settings Protocol selection Encryption algorithm Authentication algorithm SA lifetime Perfect forward secrecy	ESP 3DES X AES-128 X SHA-1 X 3600	seconds



DSR-250v2

**IPsec profiles** 

# System and status Administration Authentication Interface Interface Network Firewall Security Image: VPN Image: Network <t

IPsec pr	ofiles		
+ 🖉	1		
	Name	î↓	IKE Version
-	L2TP		IKEV1
	IKE_profile_default		IKEV1

Step 2. Go to VPN > L2TP > L2TP Server.

Enable L2TP Server.

Specify the range of IP addresses you want to assign to the connecting clients (this range should be different from your LAN subnet).

Select "default\_user" in Local user group.

Enable L2TP over IPSec.

Select the IPSec Profile you created in Step 1 from the IKE profile.

<b>D-Link</b> Building Networks for People	DSR-250v2		
	L2TP		
System and status			
Administration	L2TP server L2TP clier	11	
Authentication			
류. Interface	Enable L2TP server		
ංදි Network	Routing mode	NAT     Route	
器 Firewall	Starting IP address	192.168.33.10	
(†) Security	Ending IP address	192.168.33.50	
🖭 VPN	Authentication server	Local user database	•
IPsec profiles		Local user group	default_user •
IPsec site to site			
IPsec client to site		Authentication protocol	PAP x CHAP x MSCHAP x
IPsec client to site IPsec 1 to 1 mapping		Authentication protocol	PAP x CHAP x MSCHAP x MSCHAPV2 x
IPsec client to site IPsec 1 to 1 mapping PPTP		Authentication protocol Enable secret key	PAP x CHAP x MSCHAP x MSCHAPV2 x
IPsec client to site IPsec 1 to 1 mapping PPTP L2TP		Authentication protocol	PAP x CHAP x MSCHAP x MSCHAPV2 x
IPsec client to site IPsec 1 to 1 mapping PPTP L2TP OpenVPN	Idle timeout	Authentication protocol Enable secret key 450	PAP x CHAP x MSCHAP x MSCHAPV2 x
IPsec client to site IPsec 1 to 1 mapping PPTP L2TP OpenVPN GRE	Idle timeout L2TP over IPsec	Authentication protocol Enable secret key 450	PAP x CHAP x MSCHAP x MSCHAPV2 x seconds

# Step 3. Go to Authentication > User Database > User account > Local users.

Ř	System and status										
ĉ	Administration		User a	ccount Exte	rnal auth	server					
5	Authentication		Local gro	oup							
	User authentication										
	User database		+ 🖉	Ū							
	Captive portal			Group Name	îĻ	Membe	er	Associated	Servi	ces	î↓ I
_				default_user		2		OpenVPN,L2	2TP,P	PTP	I
쌺	Interface			ADMIN		1					1
ಷ್	Network			GUEST		1					(
田	Firewall										Total:3 iten
$\widehat{\mathbf{v}}$	Security	1	Local us	ers							
÷	VPN		+ 🖉								
				User name		↑↓	Groups		î↓	Descriptio	on
				admin			default_use	r		DEFAULT	NETWORK

# Add new username, select "default\_user" from the Group and enter passwords.

	Add local user							Cancel Apply
😫 System and status								
음 Administration	User name	test						
Authentication	Group	default_user x	-					
User authentication	New password		đ					
User database			72-					
Captive portal	Confirm password	8-64 Characters	Þ					
昂 Interface	Description (Optional)	1-64 Characters						
් Network	Email (Optional)	adc@example						
器 Firewall	Mobile (Optional)	eg.0987654321						
<ul> <li>Gecurity</li> </ul>								
System and status								
Administration	User account	External auth server						
Authentication	Local group							
User authentication	Loon group							
User database	+ 🖉 🗇							
Captive portal	Group Nan	ne îl	Member		Associated Services		↑↓	Description
	default_use	r	3		PPTP,L2TP			DEFAULT NETWORK GROUP
	ADMIN		1					ADMINISTRATION GROUP
୍ଦ୍ତ Network	00201							Total:3 ite
器 Firewall								10141.0 10
(†) Security	Local users							
🔛 VPN	+ 🖉 🗇							
	User name		ţ†	Groups		↑↓ Description		
	admin			default_user		DEFAULT NETWORK US	BER	
	user			default_user				
	test			default_user				
	admin			ADMIN		ADMINISTRATION ACCO	DUNT	
	guest			GUEST		GUEST ACCOUNT		

D-Link Building Networks for People	DSR-250v2			Q Sear
	User database			
🕅 System and status				
음 Administration	User account External at	ith server		
Authentication	Local group			
User authentication	Loon group			
User database	+ 🖉 ū	You h	ave selected 1 items for delete or edit	
Captive portal	Group Name	11 Member	Associated Services	↑↓ Description
	default_user	3	PPTP,L2TP	DEFAULT NETWORK GROUP
品 Interface	ADMIN	1		ADMINISTRATION GROUP
	GUEST	1		GUEST GROUP
ංගී Network				





# Select "Use my Internet connection (VPN)".



Enter the DSR-250V2 WAN IP address and Destination name below.

			-		×
←	Connect to a Workplace	e			
	Type the Internet ad	dress to connect to			
	Your network administrate	r can give you this address.			
	Internet address:	Example:Contoso.com or 157.54.0.1 or 3ffe:1234	4::11		
	Destination name:	VPN Connection			
	Use a smart card Remember my cree Allow other people This option allows a	tentials : to use this connection nyone with access to this computer to use this co	nnectic	on.	
		Cre	eate	Can	cel

Right-click on the VPN icon (in this example DSR250NV2\_L2TP\_o\_IPSec) and click on Properties.



Go to Security tab and select the following settings below.



Under Security tab, click on Advanced settings and enter the same Pre-shared key you type in Step1 then press OK to exit.



Select the L2TP VPN you created from the Connection window to connect and enter the username and password.

C2TP_over_IPSec_DFL	
Cover_IPSec-DWM-312	
SR250NV2_L2TPoIPSec	l
VPN Connection	
Windows Security ×	
Sign in	
User name	
Password	
The user name or password is incorrect.	
OK Cancel	