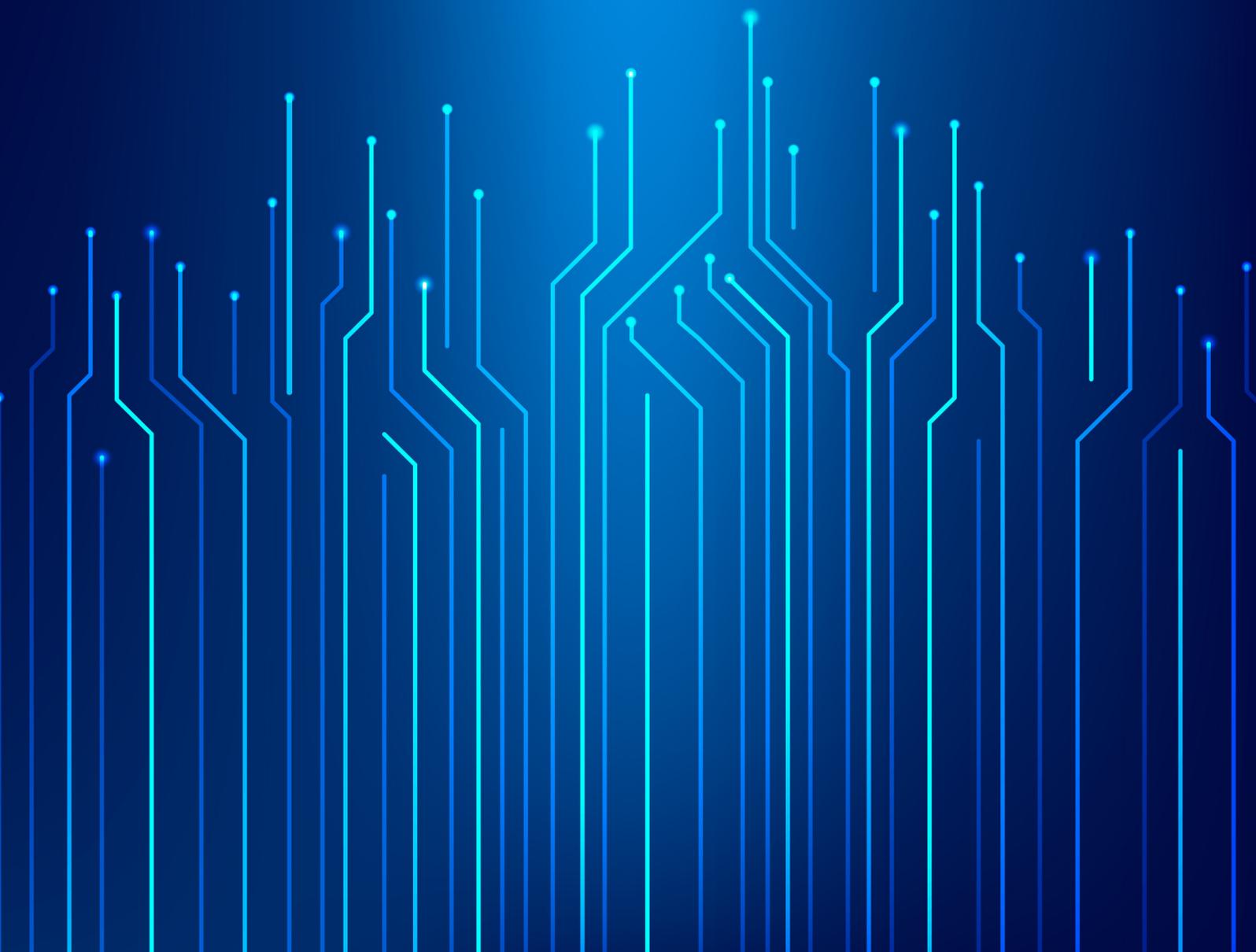


How to configure L2TP over IPSec on your firewall



How to configure L2TP over IPSec on your firewall

This section contains information about the parameters required to define the VPN tunnel. Default Policy will by default be pre-configured with factory settings. You'll have to create a new policy for L2TP.

1. L2TP VPN Policy Settings

Go to VPN --> IPSec --> Policy

The screenshot shows the GAJSHIELD firewall configuration interface. The left sidebar contains a navigation menu with options: Definitions, Configuration, Management, Diagnosis, Firewall, VPN, IPsec, L2TP, PPTP, Local User, Enterprise Cloud, AntiSpam, APP Filter, DLP, Reports, Browsing, IPS, and Logout. The main content area is titled 'Policy' and includes tabs for Tunnels, VPN Failover Group, Local IPsec Key, Reserved IPs, Advanced Setup, and Restart VPN. The configuration form is for a policy named 'l2tp'. It includes fields for 'Allow Re-keying*' (Yes/No), 'Key Negotiation Tries*' (3), and 'Pass Data In Compressed Format*' (Yes/No). The form is divided into 'Phase 1' and 'Phase 2' sections. Phase 1 includes 'Encryption Algorithm*' (3DES), 'Authentication Algorithm*' (MD5), 'Encryption Algorithm' (3DES), 'Authentication Algorithm' (SHA1), 'DH Group*' (1, 2, 5, 14, 15, 16), 'Key Life*' (3600 Seconds), 'Rekey Margin*' (120 Seconds), 'Randomize Re-Keying Margin By*' (0 %), 'Enable Dead Peer Detection' (checkbox), 'Check Peer After Every' (Seconds), 'Wait For Response Upto' (Seconds), and 'Action When Peer Is Not Active' (Hold). Phase 2 includes 'Encryption Algorithm*' (3DES), 'Authentication Algorithm*' (MD5), 'Encryption Algorithm' (3DES), 'Authentication Algorithm' (SHA1), 'PFS Group*' (None, 1, 2, 5, 14, 15, 16), and 'Key Life*' (18000 Seconds). An 'Edit' button is located at the bottom of the form.

Note – Policy configuration is required to setup a L2TP tunnel. You can configure L2TP with both ISPs

2. L2TP VPN Tunnel Configuration

Go to VPN --> IPSec --> Tunnels

Policy **Tunnels** VPN Failover Group Local IPsec Key Reserved IPs Advanced Setup Restart VPN

Add Tunnel

Tunnel Name *	L2TPTunnel
Automatic Firewall Rules	<input checked="" type="checkbox"/>
VPN Details	
Policy	L2TTPolicyRev
VPN Type	L2TP
Action on Restart	Passive
IKE Version	IKEv1
Local Network Details	
Local Server	fwip-ShivFiberWAN  firewall WAN IP
Gateway of Local Server	shivfiberwanGW  Gateway of WAN interface
Local ID	X.509 DN
Remote Network Details	
Remote Host	Any
Remote ID	X.509 DN
Authentication Details	
Authentication Type	Preshared Key
Preshared Key	*****
Remote Certificate	UserTest
Add	

Note- You'll have to select L2TP in VPN type option since the configuration is L2TP over IPsec.

3. L2TP Configuration

Go to VPN -> L2TP -> L2TP Options

GAJSHIELD Dashboard Wizard Reports Contact Help

Definitions Configuration Management Diagnosis Firewall VPN IPsec **L2TP** PPTP Local User Enterprise Cloud AntiSpam APP Filter DLP Reports Browsing IPS Logout

L2TP Options Restart L2TP

Add L2TP Server

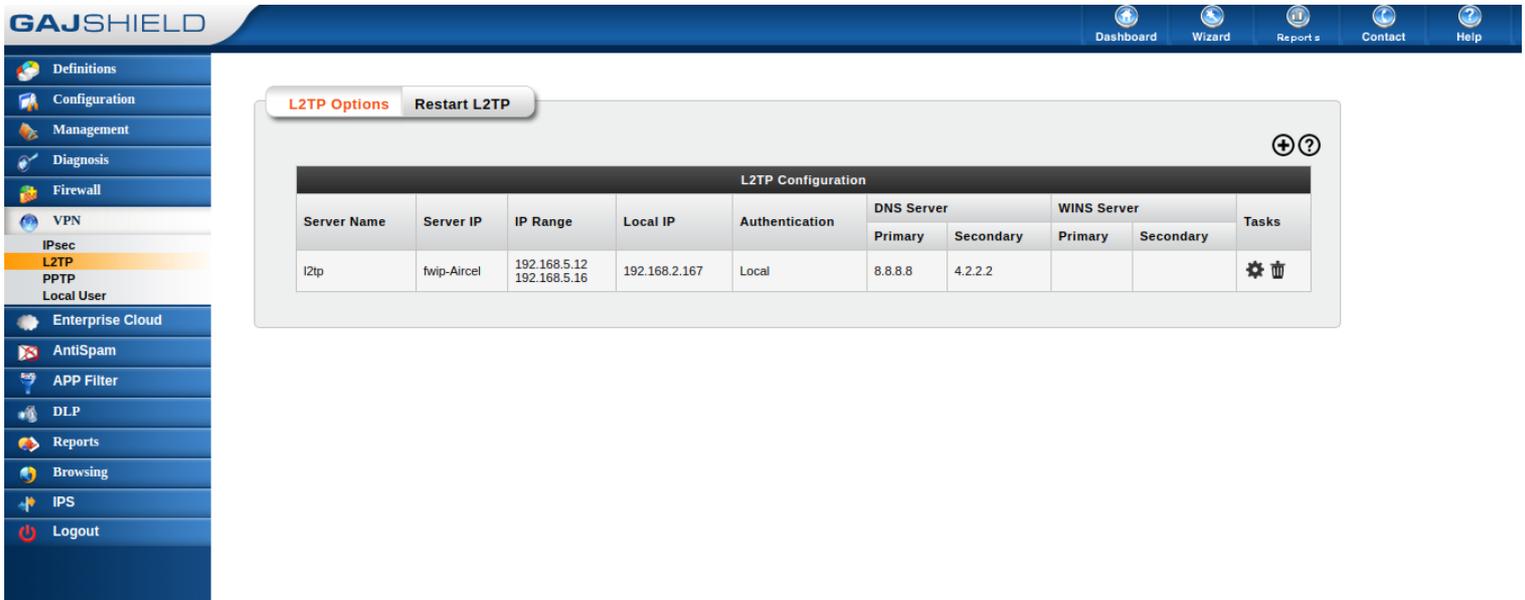
Server Name	l2tp		
Server IP	fwip-Aircel		
IP Range	Start IP	192.168.5.12	
	End IP	192.168.5.16	
Local IP	192.168.2.167  firewall LAN IP		
Authentication Type	Local		
DNS Server (Optional)	Primary DNS Server	8.8.8.8	
	Secondary DNS Server	4.2.2.2	
WINS Server (Optional)	Primary WINS Server		
	Secondary WINS Server		
Add			

Specify the following fields:

Server IP: Public IP of Firewall.

IP Range: When Users connect through VPN, that time users get the IP address from the above defined range.

Local IP: Firewall local LAN IP.

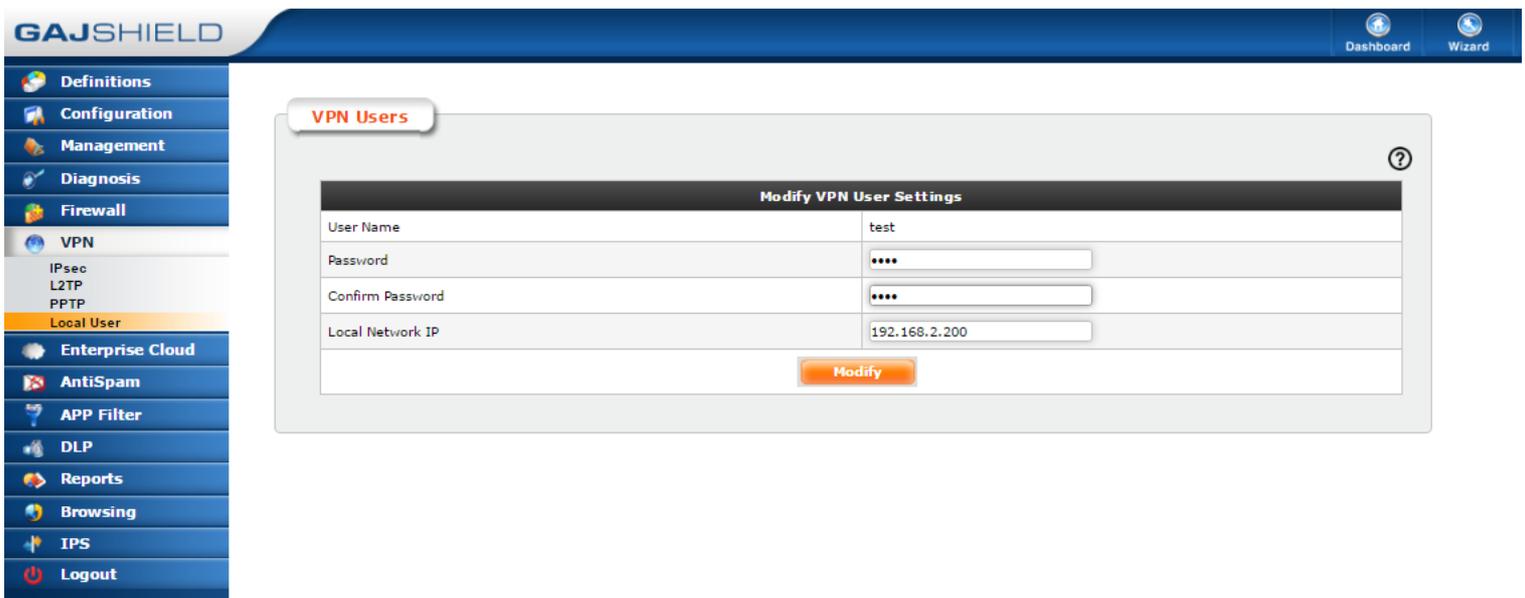


The screenshot shows the GAJSHIELD web interface. The left sidebar contains a navigation menu with items: Definitions, Configuration, Management, Diagnosis, Firewall, VPN, IPsec, L2TP (highlighted), PPTP, Local User, Enterprise Cloud, AntiSpam, APP Filter, DLP, Reports, Browsing, IPS, and Logout. The main content area is titled 'L2TP Options' and 'Restart L2TP'. It features a table for 'L2TP Configuration' with the following data:

Server Name	Server IP	IP Range	Local IP	Authentication	DNS Server		WINS Server		Tasks
					Primary	Secondary	Primary	Secondary	
l2tp	fwip-Aircel	192.168.5.12 192.168.5.16	192.168.2.167	Local	8.8.8.8	4.2.2.2			 

4. Create a VPN User

Go to VPN -> Local User -> VPN Users



The screenshot shows the GAJSHIELD web interface for 'Modify VPN User Settings'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'VPN Users' and contains a form with the following fields:

User Name	test
Password
Confirm Password
Local Network IP	192.168.2.200

Below the form is an orange 'Modify' button.

You can create a new user or modify an existing VPN user

VPN Users



Username	Local N/w IP	Tasks
test	192.168.2.200	
test1	-	
test2	-	

5. Rules for L2TP VPN

Go to Firewalls -> Policies -> Rules

Rules DoS Settings MAC Binding Install Policies



Show: Zone: To: Hide Inactive Rules

No.	Direction	Source	Destination	Service	UserSense	Policies	Action	Schedule	QoS	Tasks
6	Any To Any	internet	fwip-ShivFiberWan	L2TP-IPsec	-	-	accept	AllTime	-	
7	Any To Any	testuser1	fwnet-LAN	Any	-	-	accept	AllTime	-	
8	Any To Any	testuser2	fwnet-LAN	Any	-	-	accept	AllTime	-	

Configure the 3 rules as specified above.

NOTE: If a user has 2 ISPs, he'll have to configure 2 tunnels, second time with the second ISP as the destination. (If user wants to configure L2TP with both the ISPs)