GAJSHIELD
Data Security Firewall

How to configure L2TP over IPSec on your firewall

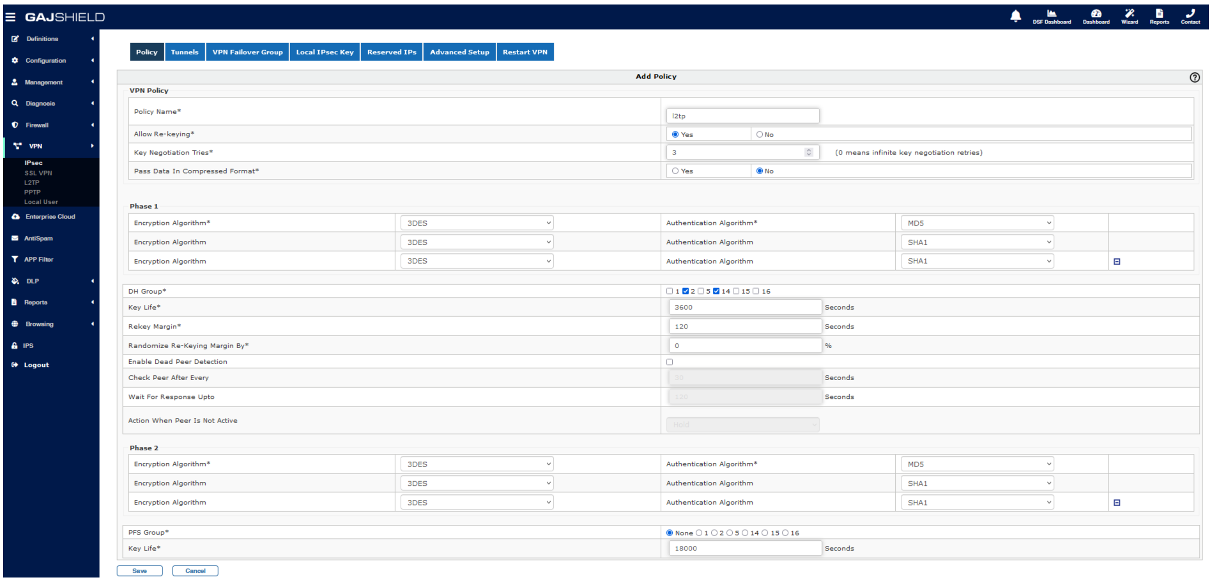
How to configure L2TP over IPSec on your firewall

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



Add Policy

VPN Policy

Policy Name*	l2tp
Allow Re-keying*	● Yes ○ No
Key Negotiation Tries*	3 (0 means infinite key negotiation retries)
Pass Data In Compressed Format*	○ Yes ● No

Phase 1

Encryption Algorithm*	3DES	Authentication Algorithm*	MD5
Encryption Algorithm	3DES	Authentication Algorithm	SHA1
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	□
Check Peer After Every	30 Seconds
Wait For Response Upto	120 Seconds
Action When Peer Is Not Active	Hold

Phase 2

Encryption Algorithm*	3DES	Authentication Algorithm*	MD5
Encryption Algorithm	3DES	Authentication Algorithm	SHA1
Encryption Algorithm	3DES	Authentication Algorithm	SHA1

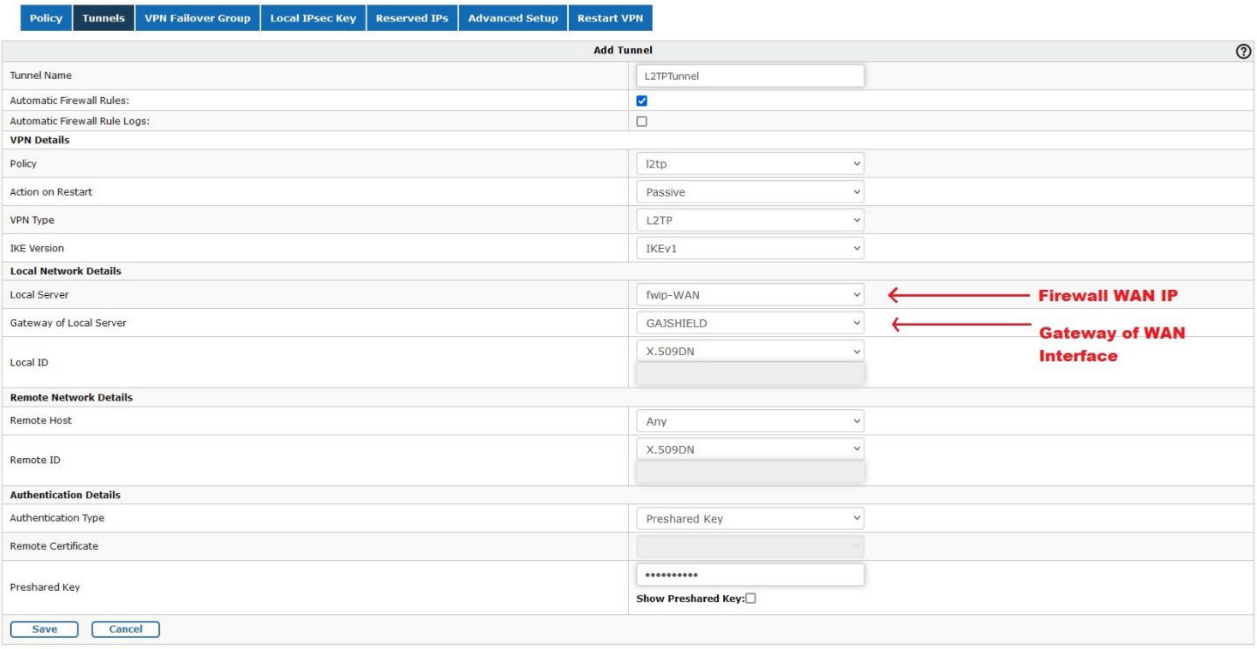
PFS Group*	● None ○ 1 ○ 2 ○ 5 ○ 14 ○ 15 ○ 16
Key Life*	18000 Seconds

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

Copyright © GajShield Infotech (I) Pvt. Ltd.



Add Tunnel

Tunnel Name	L2TPTunnel
Automatic Firewall Rules:	☑
Automatic Firewall Rule Logs:	☐
VPN Details	
Policy	l2tp
Action on Restart	Passive
VPN Type	L2TP
IKE Version	IKEv1
Local Network Details	
Local Server	fwip-WAN
Gateway of Local Server	GAJSHIELD
Local ID	X.509DN
Remote Network Details	
Remote Host	Any
Remote ID	X.509DN
Authentication Details	
Authentication Type	Preshared Key
Remote Certificate	
Preshared Key	•••••••••• Show Preshared Key:☐

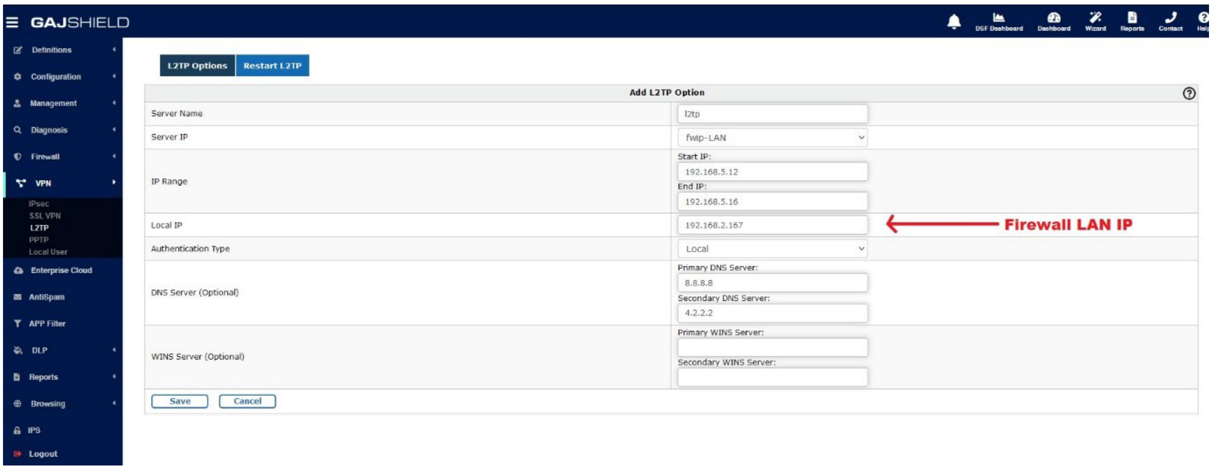
Firewall WAN IP

Gateway of WAN Interface

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



Add L2TP Option

Server Name	l2tp
Server IP	fwip-LAN
IP Range	Start IP: 192.168.5.12 End IP: 192.168.5.16
Local IP	192.168.2.167
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:

Firewall LAN IP

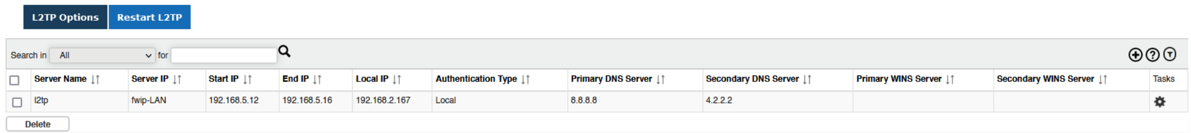
Specify the following fields:

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.

Copyright © GajShield Infotech (I) Pvt. Ltd.

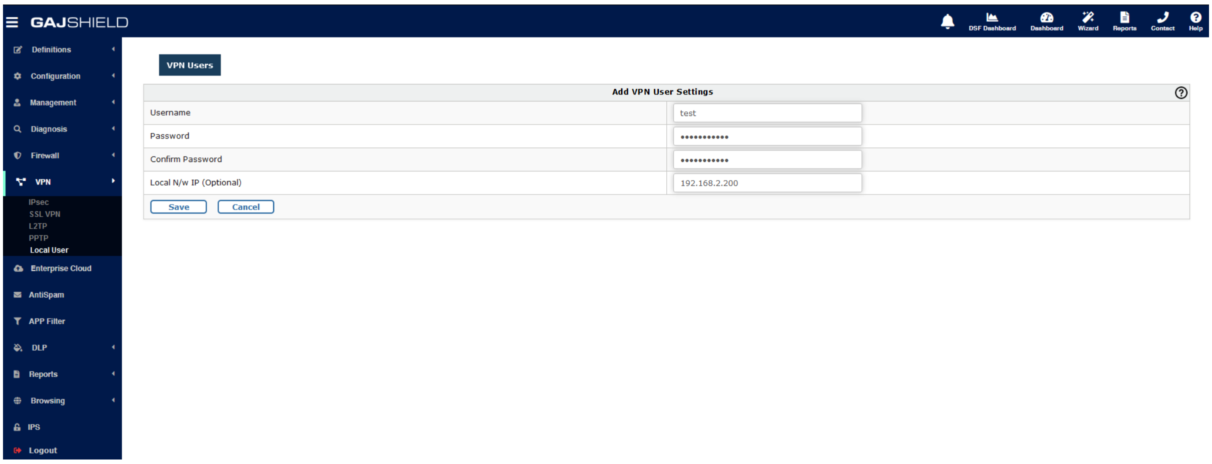
Local IP: Firewall local LAN IP.



☐	Server Name	Server IP	Start IP	End IP	Local IP	Authentication Type	Primary DNS Server	Secondary DNS Server	Primary WINS Server	Secondary WINS Server	Tasks
☐	l2tp	fwip-LAN	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

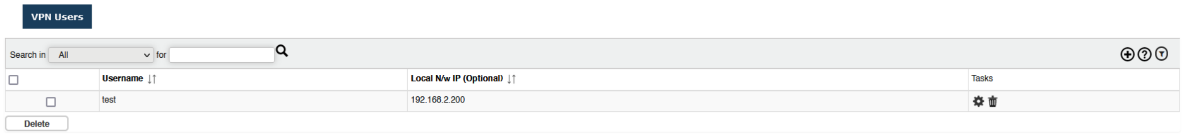
Go to VPN -> Local User -> VPN Users



Add VPN User Settings

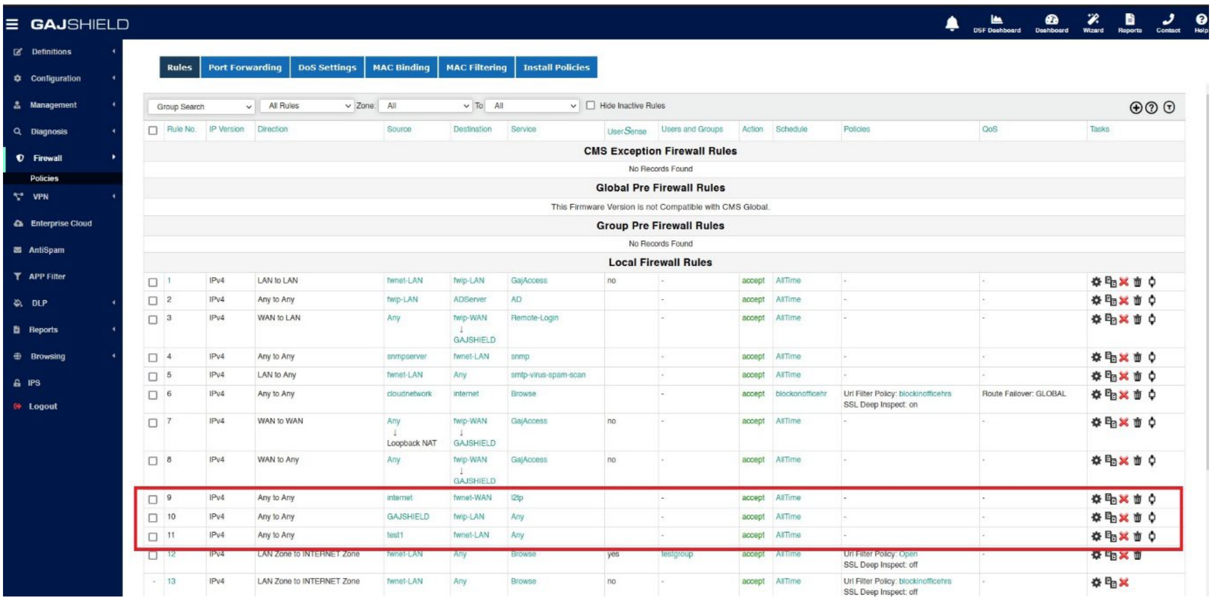
Username	test
Password	•••••••••••
Confirm Password	•••••••••••
Local N/w IP (Optional)	192.168.2.200

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



☐	Username	Local N/w IP (Optional)	Tasks
☐	test	192.168.2.200	⚙ 🗑

5. Rules for L2TP VPN
Go to Firewalls -> Policies -> Rules



Group Search | All Rules | Zone: All | To All | □ Hide Inactive Rules

□	Rule No.	IP Version	Direction	Source	Destination	Service	UserSense	Users and Groups	Action	Schedule	Policies	QoS	Tasks
CMS Exception Firewall Rules													
No Records Found													
Global Pre Firewall Rules													
This Firmware Version is not Compatible with CMS Global.													
Group Pre Firewall Rules													
No Records Found													
Local Firewall Rules													
□	1	IPv4	LAN to LAN	fwnet-LAN	fwip-LAN	GajAccess	no	-	accept	AllTime	-	-	
□	2	IPv4	Any to Any	fwip-LAN	ADServer	AD		-	accept	AllTime	-	-	
□	3	IPv4	WAN to LAN	Any	fwip-WAN ↓ GAJSHIELD	Remote-Login		-	accept	AllTime	-	-	
□	4	IPv4	Any to Any	snmpserver	fwnet-LAN	snmp		-	accept	AllTime	-	-	
□	5	IPv4	LAN to Any	fwnet-LAN	Any	smtp-virus-spam-scan		-	accept	AllTime	-	-	
□	6	IPv4	Any to Any	cloudnetwork	internet	Browse		-	accept	blockonofficehr	Url Filter Policy: blockinofficehrs SSL Deep Inspect: on	Route Failover: GLOBAL	
□	7	IPv4	WAN to WAN	Any ↓ Loopback NAT	fwip-WAN ↓ GAJSHIELD	GajAccess	no	-	accept	AllTime	-	-	
□	8	IPv4	WAN to Any	Any	fwip-WAN ↓ GAJSHIELD	GajAccess	no	-	accept	AllTime	-	-	
□	9	IPv4	Any to Any	internet	fwnet-WAN	l2tp		-	accept	AllTime	-	-	
□	10	IPv4	Any to Any	GAJSHIELD	fwip-LAN	Any		-	accept	AllTime	-	-	
□	11	IPv4	Any to Any	test1	fwnet-LAN	Any		-	accept	AllTime	-	-	
□	12	IPv4	LAN Zone to INTERNET Zone	fwnet-LAN	Any	Browse	yes	testgroup	accept	AllTime	Url Filter Policy: Open SSL Deep Inspect: off	-	
-	13	IPv4	LAN Zone to INTERNET Zone	fwnet-LAN	Any	Browse	no	-	accept	AllTime	Url Filter Policy: blockinofficehrs SSL Deep Inspect: off	-	

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)

Copyright © GajShield Infotech (I) Pvt. Ltd.