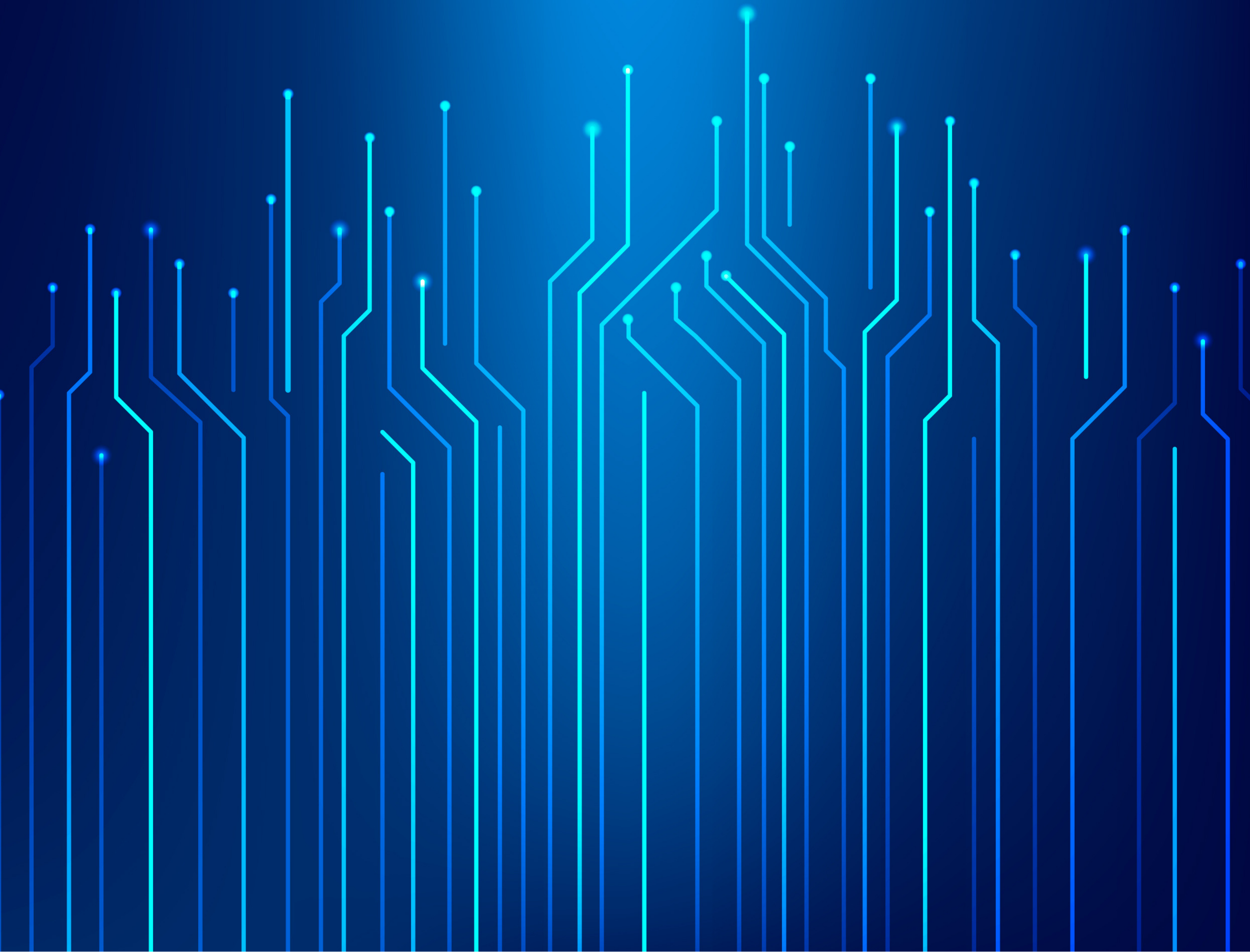
GAJSHIELD

Progressive Security

How to configure L2TP over IPSec on your firewall

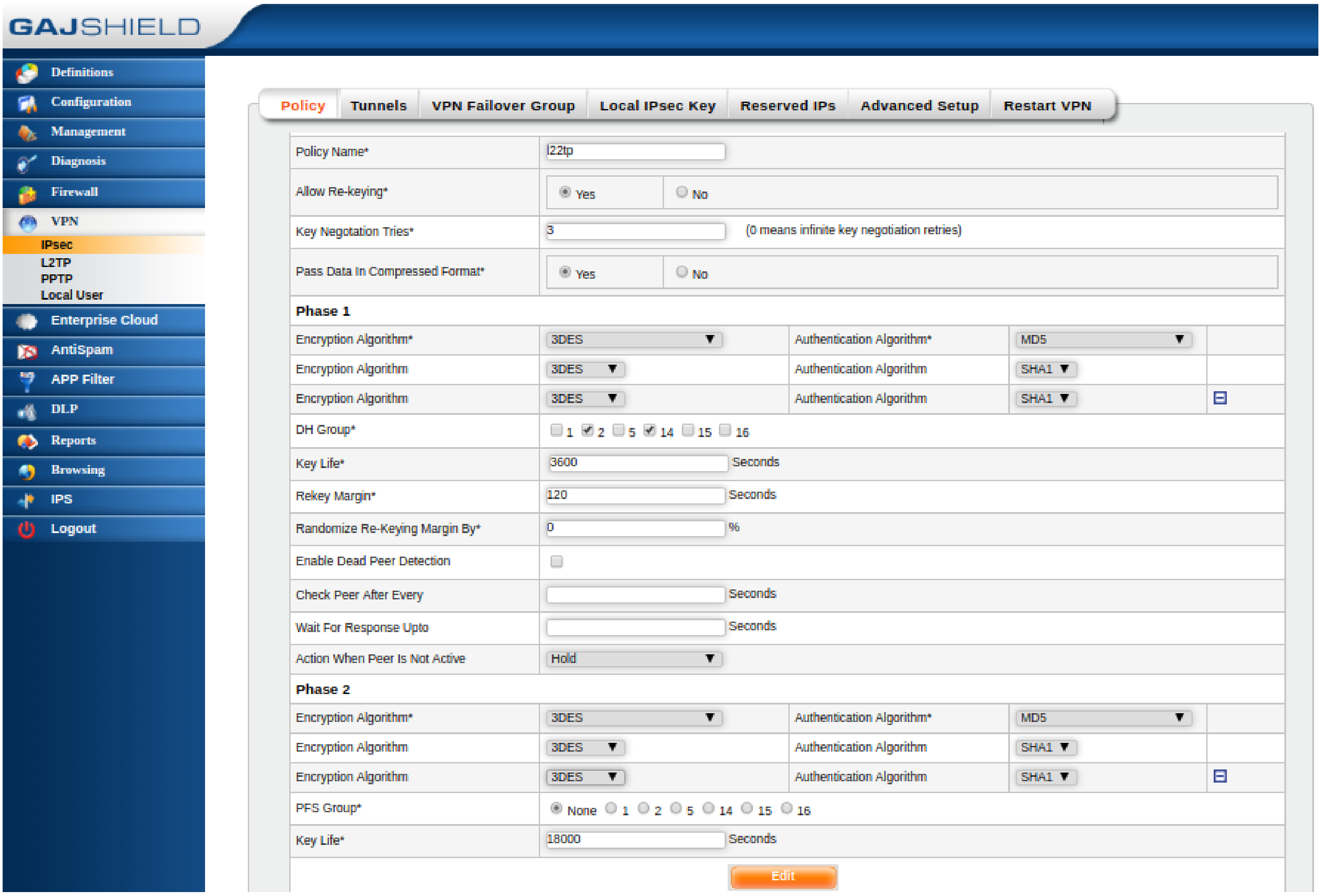


How to configure L2TP over IPSec on your firewall

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



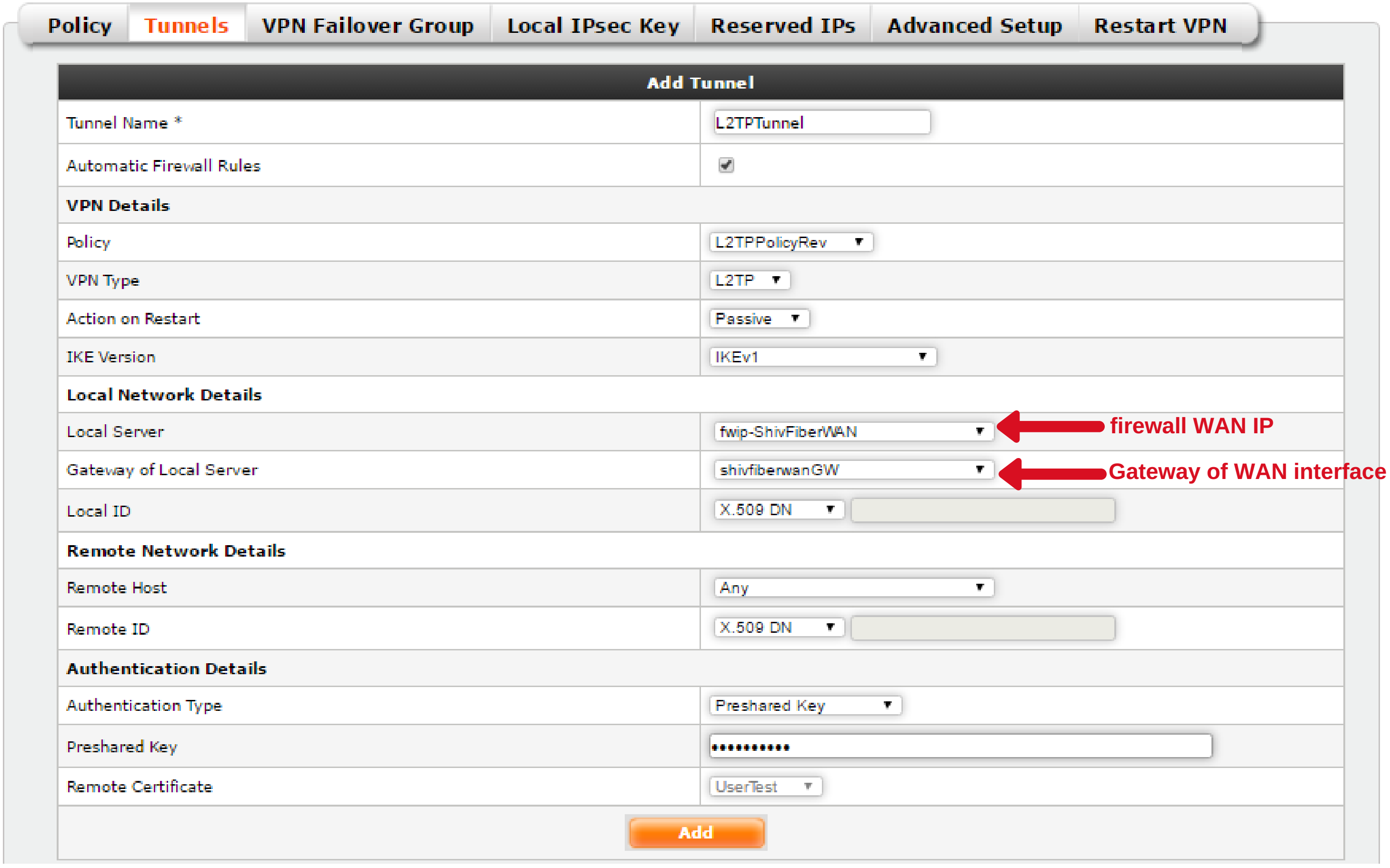
Policy Name*	l22tp			
Allow Re-keying*	● Yes ○ No			
Key Negotation Tries*	3 (0 means infinite key negotiation retries)			
Pass Data In Compressed Format*	● Yes ○ No			
Phase 1				
Encryption Algorithm*	3DES ▼	Authentication Algorithm*	MD5 ▼	
Encryption Algorithm	3DES ▼	Authentication Algorithm	SHA1 ▼	
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	Seconds			
Wait For Response Upto	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			

Edit

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



Add Tunnel

Tunnel Name *	L2TPTunnel
Automatic Firewall Rules	☑
VPN Details	
Policy	L2TPPolicyRev ▼
VPN Type	L2TP ▼
Action on Restart	Passive ▼
IKE Version	IKEv1 ▼
Local Network Details	
Local Server	fwip-ShivFiberWAN ▼
Gateway of Local Server	shivfiberwanGW ▼
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 ▼

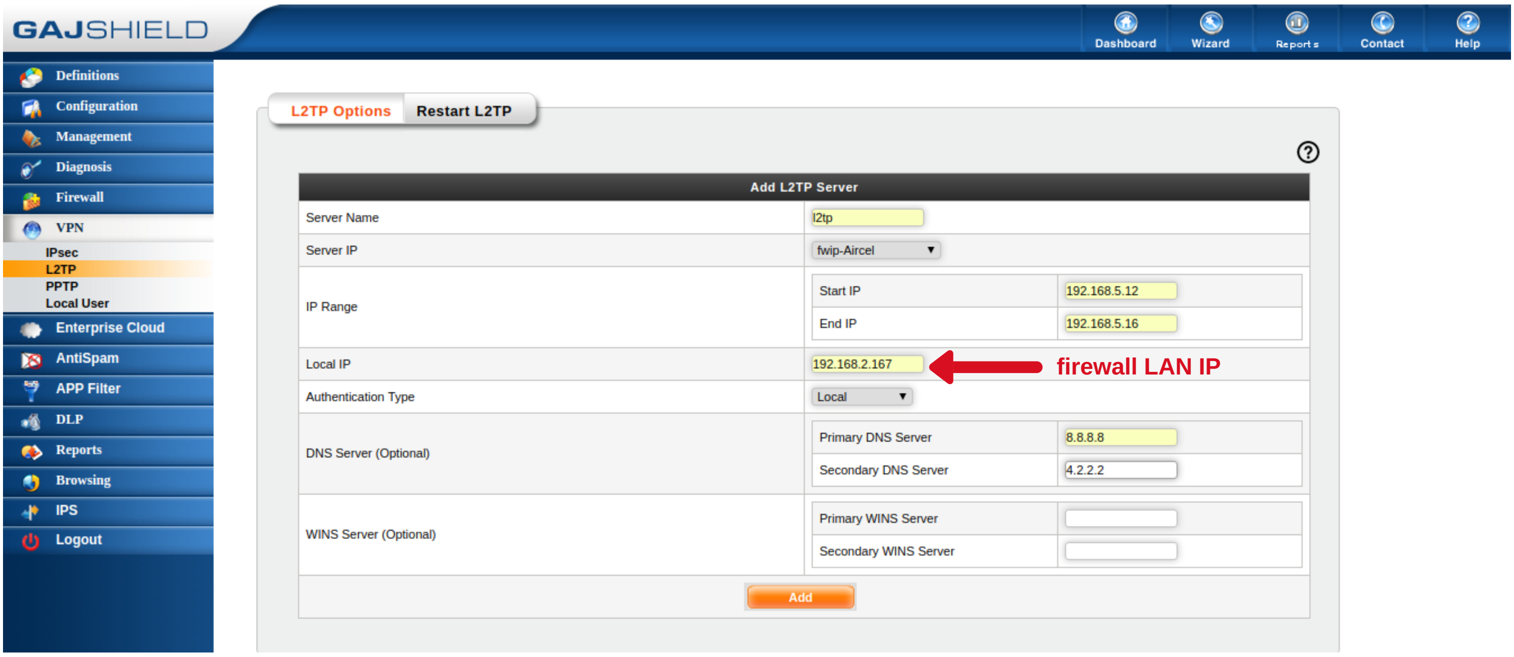
firewall WAN IP

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 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	
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	

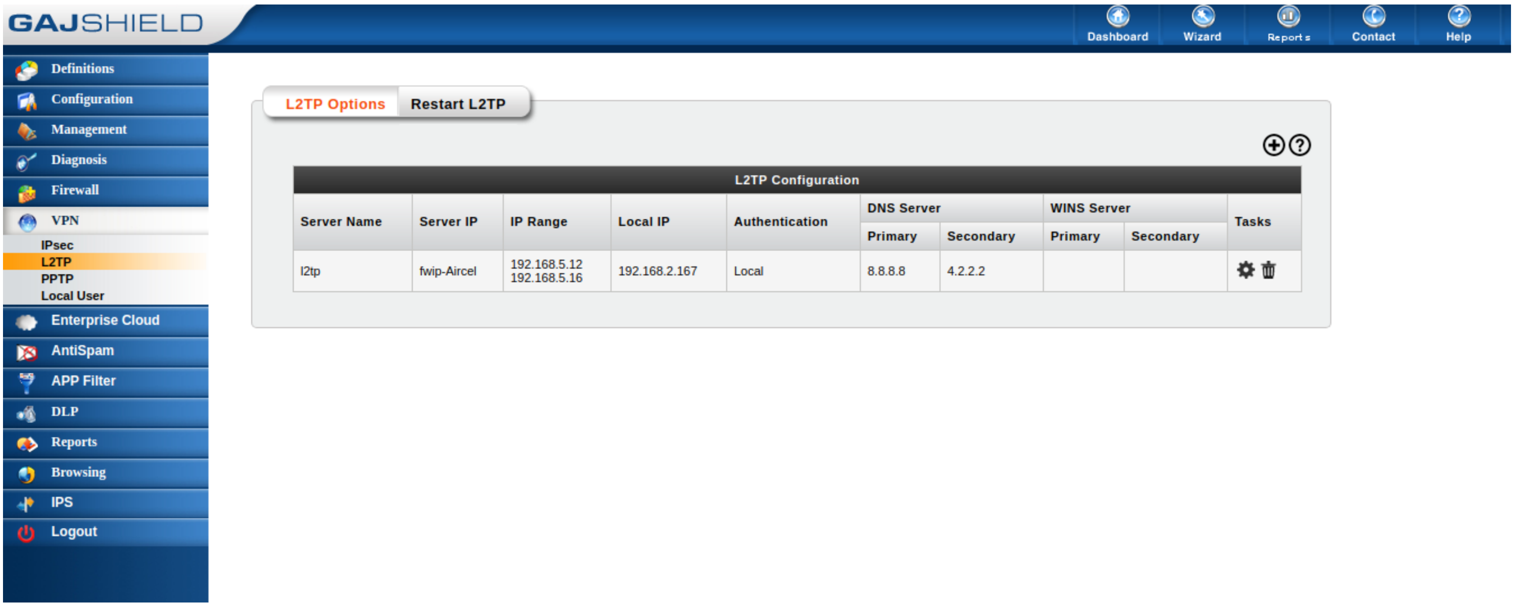
firewall LAN IP

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.

Local IP: Firewall local LAN IP.

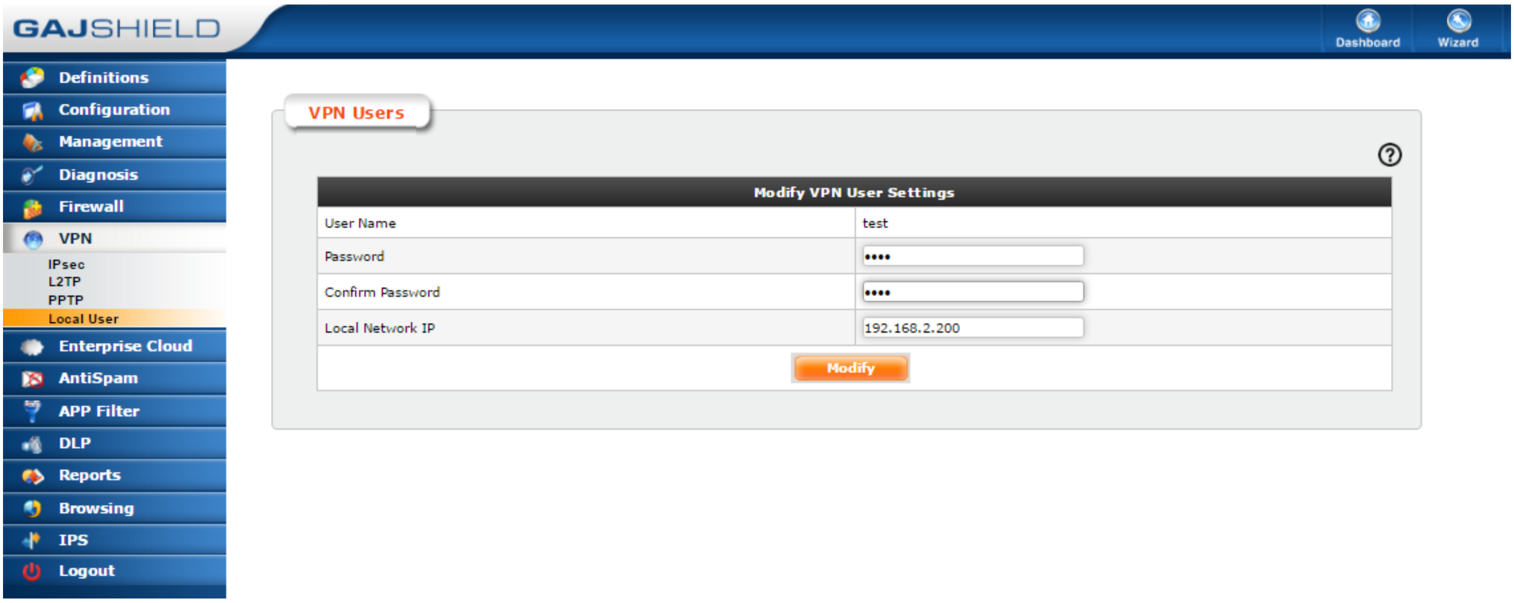


L2TP Configuration

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

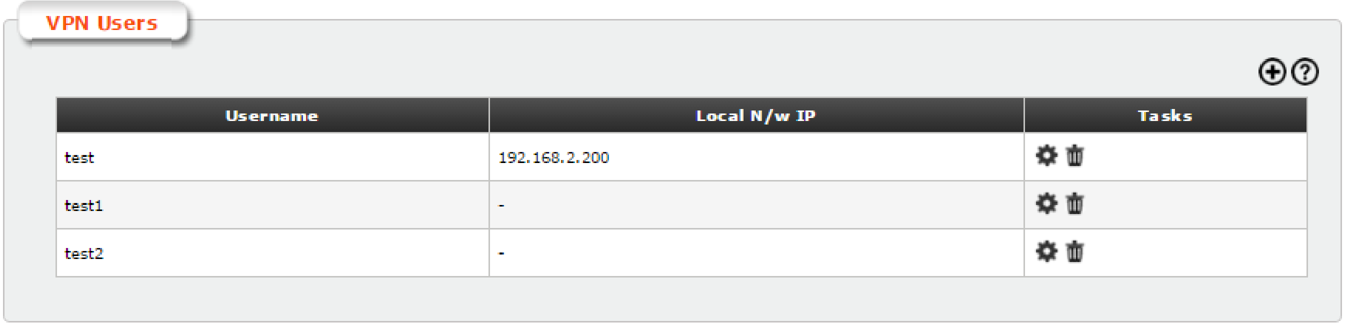


Modify VPN User Settings

User Name	test
Password	••••
Confirm Password	••••
Local Network IP	192.168.2.200

Modify

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



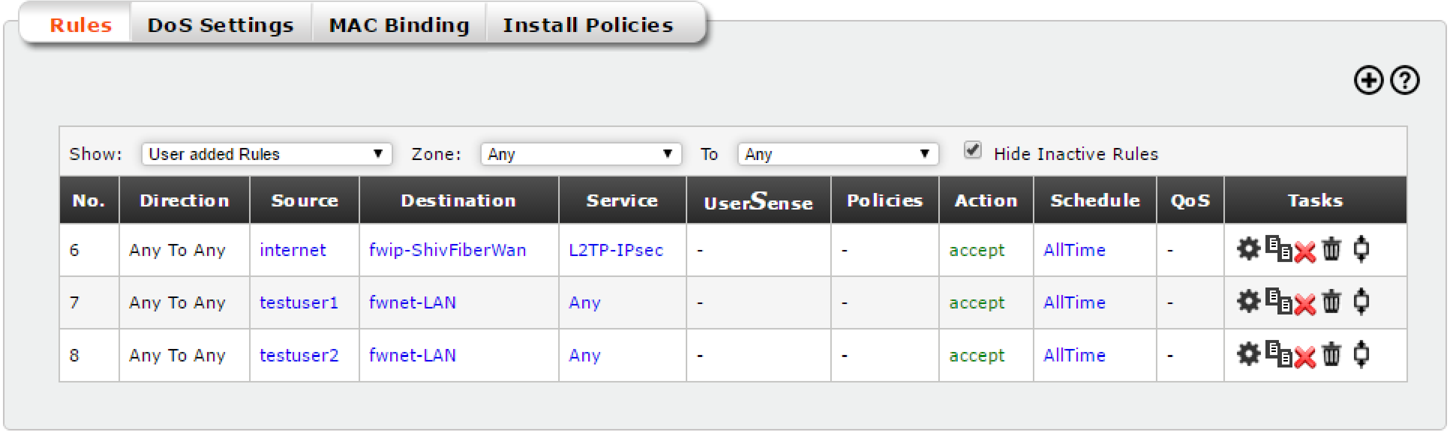
VPN Users

⊕ ?

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: User added Rules ▾ Zone: Any ▾ To Any ▾ ☑ 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)