

# L2TP Configuration

The screenshot shows the GajShield SecureGate v5 web-based administration tool. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.190/cgi-bin/mainmenu.cgi". The page has a blue header with the GajShield logo and the text "GajShield SecureGate v5". Below the header is a "Firewall Management" section with two tabs: "L2TP Options" (selected) and "Restart L2TP". On the left is a navigation menu with categories: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, IPS, and LOGOUT. Under the VPN category, sub-items include IPsec, Certificates, L2TP (selected), PPTP, and Local User. The main content area displays the "Add L2TP Settings" form. The form fields are as follows:

Add L2TP Settings			
Server Name	L2TP-Server		
Server IP	219.2.3.2		
IP Range	Start IP	192.168.2.200	
	End IP	192.168.2.250	
Local Lan IP	192.168.2.190		
Authentication Type	local		
<input type="button" value="Add"/>			

At the bottom of the page, there is a copyright notice: "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved." and a status bar showing "Done" and the IP address "192.168.2.190".

In above example in 1<sup>st</sup> tab you have to specify L2TP server name and next tab public IP address [one which provided by ISP] of your ISP which is configured in firewall . Next tab is for range of ip-ddress from which whenever user will connect through VPN at that time users will get the ip-address from above define range. Next tab is for local lan ip address of firewall . Authentication type supported are local (VPN users created on firewall), Radius, Ldap, Tacacs Plus. If you want to select local authentication then vpn users are need to create.

Gajshield: Web based Administration and Management Tool - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.2.190/cgi-bin/mainmenuus.ggi

Google

Getting Started Latest Headlines

**GajShield SecureGate v5**

Firewall Management

L2TP Options

Restart L2TP

NETWORK

FIREWALL

USERS

VPN

IPsec

Certificates

L2TP

PPTP

Local User

SYSTEM

ADMIN

REPORT

BROWSING

IPS

LOGOUT

Server Name	Server IP	IP Range	Local IP	Authentication	Tasks
L2TP-Server	219.2.3.2	192.168.2.200 192.168.2.250	192.168.2.190	Local	

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done192.168.2.190

# VPN User Configuration

The screenshot shows the GajShield SecureGate v5 web interface in a Mozilla Firefox browser. The browser's address bar displays the URL `https://192.168.2.190/cgi-bin/mainmenu.cgi`. The interface has a blue header with the title "GajShield SecureGate v5" and a left sidebar with navigation menus. The "VPN" menu is expanded, showing sub-items: "IPsec", "Certificates", "L2TP", "PPTP", and "Local User". The "L2TP" sub-item is selected. The main content area is titled "VPN Users" and contains a form titled "Add VPN User Settings". The form has four input fields: "User Name" (containing "test2"), "Password" (containing "\*\*\*\*\*"), "Confirm Password" (containing "\*\*\*\*\*"), and "Local Network IP" (containing "192.168.2.201"). An "Add" button is located below the form. The footer of the interface shows the copyright notice "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.190".

Add VPN User Settings	
User Name	test2
Password	*****
Confirm Password	*****
Local Network IP	192.168.2.201

**Add**

In above example we are creating vpnuser. Provide vpn username and password for the client trying to connect L2TP server. If you are giving ip address then it must be within range of defined in L2TP server configuration or you can leave it blank; ip will get from the defined range as shown below.

# VPN Users

Gajshield: Web based Administration and Management Tool - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.2.190/cgi-bin/mainmenuus.cgi

Getting Started Latest Headlines

## GajShield SecureGate v5

Firewall Management

VPN Users

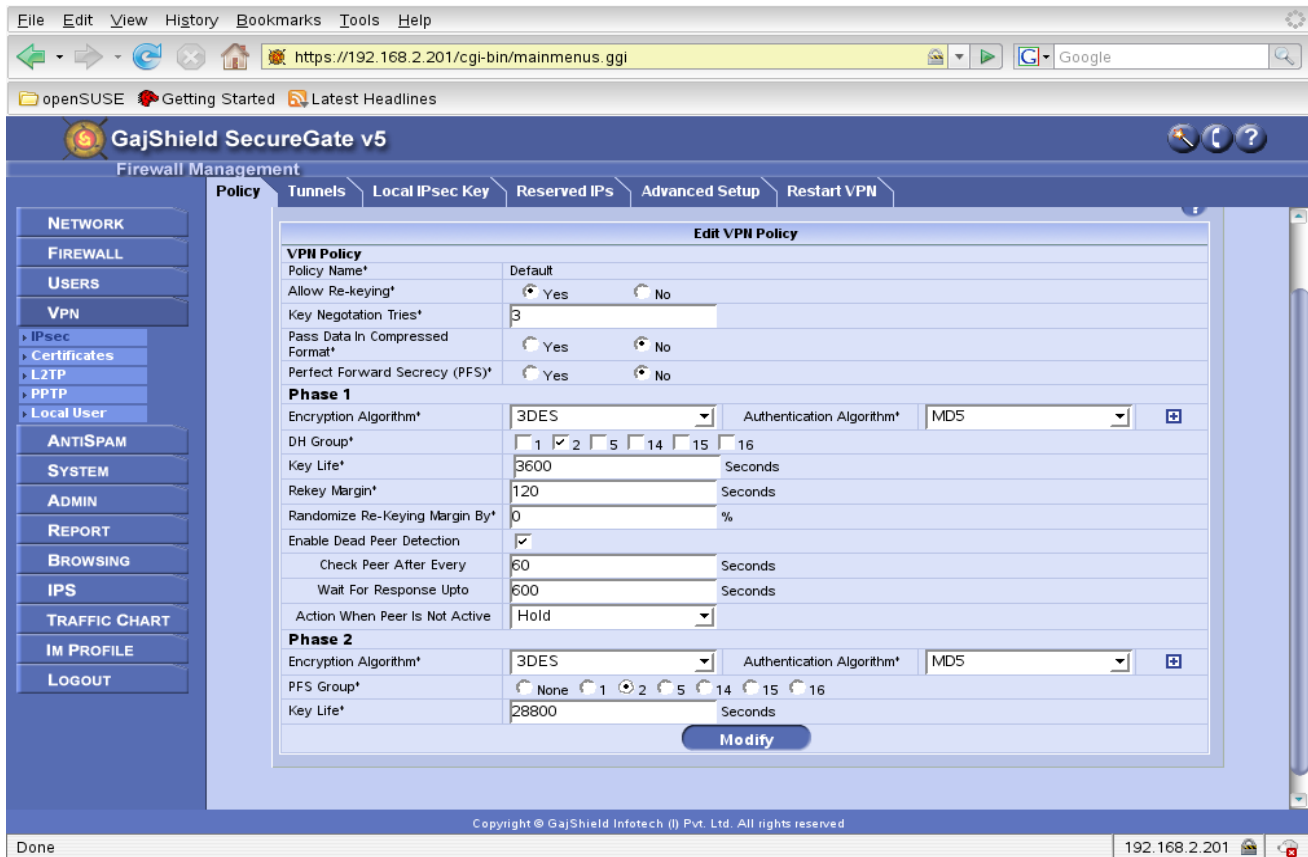
- NETWORK
- FIREWALL
- USERS
- VPN
  - IPsec
  - Certificates
  - L2TP
  - PPTP
  - Local User
- SYSTEM
  - ADMIN
  - REPORT
  - BROWSING
  - IPS
  - LOGOUT

Username	Local N/w IP	Tasks
test1	192.168.2.200	<input type="checkbox"/>
test2	192.168.2.201	<input type="checkbox"/>
test3		<input type="checkbox"/>

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.190

# L2tp policy settings



In above example we can create one separate policy or you can use default policy for L2tp tunnel. For L2TP in default policy you need change DH Group from 5 to 2 in Phase 1 and in Phase 2 PFS Group from 5 to 2 a part from this do not need to change any thing kept every thing as it is.

# VPN Tunnel Details

File Edit View History Bookmarks Tools Help

https://192.168.2.201/cgi-bin/mainmenuus.cgi





openSUSE Getting Started Latest Headlines

## GajShield SecureGate v5

Firewall Management

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

- NETWORK
- FIREWALL
- USERS
- VPN
  - IPsec
  - Certificates
  - L2TP
  - PPTP
  - Local User
- ANTISPAM
- SYSTEM
- ADMIN
- REPORT
- BROWSING
- IPS
- TRAFFIC CHART
- IM PROFILE
- LOGOUT

Tunnel Name	Action on Restart	Policy	VPN Type	Local Network Details	Remote Network Details	Authentication	Task
merytunnel	passive	Default	ipsec	fwip-vsrl vsrl-gateway fwnet-LAN	Any testRemote	*****	 
TEST_2	passive	Default	l2tp	fwip-TA TA Gateway	Any	*****	 

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.201

# VPN Tunnel Configuration Using Preshared Key

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser address bar shows the URL `https://192.168.2.201/cgi-bin/mainmenuus.cgi`. The interface has a sidebar menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, ANTISPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The main content area is titled 'Firewall Management' and includes tabs for Policy, Tunnels, Local IPsec Key, Reserved IPs, Advanced Setup, and Restart VPN. The 'Tunnels' tab is active, showing a 'Modify VPN User Settings' form. The form contains the following fields:

Modify VPN User Settings	
Tunnel Name *	TEST_2
<b>VPN Details</b>	
Policy	Default
VPN Type	L2TP
Action on Restart	Passive
<b>Local Network Details</b>	
Local Server	fwip-TATA
Gateway of Local Server	Gateway
Local ID	X509 DN
<b>Remote Network Details</b>	
Remote Host	Any
Remote ID	X509 DN
<b>Authentication Details</b>	
Authentication Type	Preshared Key
Preshared Key	*****
Remote Certificate	

A 'Modify' button is located at the bottom right of the form. The footer of the interface shows 'Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved' and the IP address '192.168.2.201'.

In above example in 1<sup>st</sup> tab specify the name of tunnel then choose the policy which we created above, then select L2TP in type of vpn. If you can select passive or active in action on restart depends on whether your firewall going to dial for establishing tunnel. In Local server you have to select the fwip-isp's name which is the public ip address. You provide gateway of the ISP in next selected tab.( for that gateway ip you have to create host because by default it's not created in networks--->host ). In local id tab keep x509 DN , do not change it . In remote host select any because client end they can use different isp and in authentication type there are two options use Pre-shared key or Digital certificate if u are using certificate. At the client end you required this certificate to connect the L2TP server . In remote certificate tab you have to select the same certificate and if you have selected pre-shared key then you have to define key in below tab which will be use to client end.

# Rules of L2TP-IPsec VPN

The screenshot displays the GajShield SecureGate v5 web-based administration interface. The main menu on the left includes NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, IPS, and LOGOUT. The FIREWALL section is expanded, showing a list of rules. The 'Rules' tab is active, displaying a table of firewall rules. Below the table, a modal window is open, showing details for 'test-user-2'.

**Firewall Rules Table:**

No.	Dr.	Src.	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	Any	internet	L2TP-IPsec	fwip-TATA	accept	yes	active	default	Always On	no	none	[Icons]
2	Any	test-user-1	ping	fwnet-LAN	accept	yes	active	default	Always On	no	none	[Icons]
3	Any	test-user-2	smtp	fwnet-LAN	accept	yes	active	default	Always On	no	none	[Icons]

**Modal Window Details:**

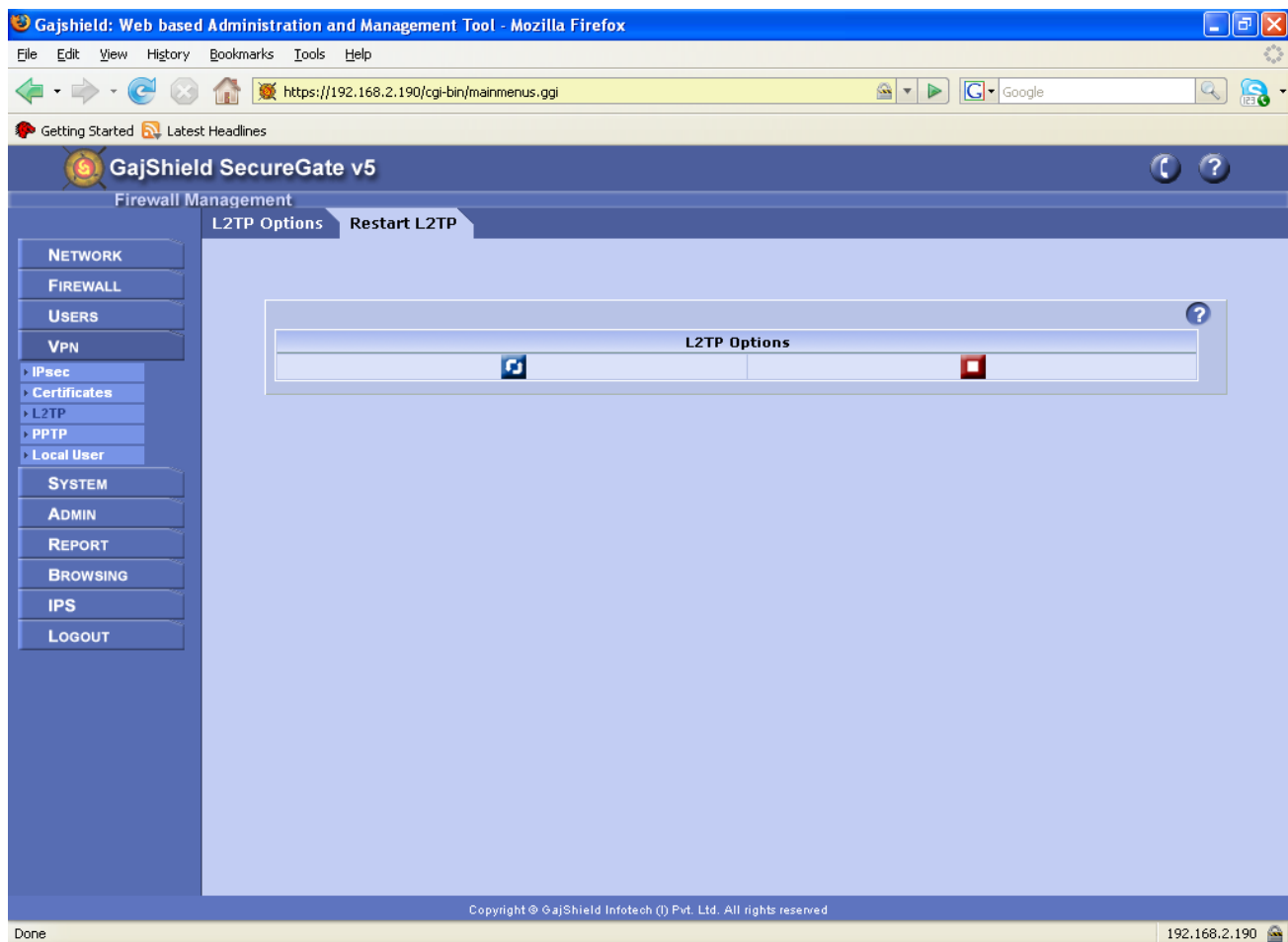
Host/Network ID	Host/Network IP	Netmask
test-user-2	192.168.2.201	255.255.255.255

Close

In above example 1<sup>st</sup> rule is created for VPN server access and the rest of rules are created for the access of internal LAN.

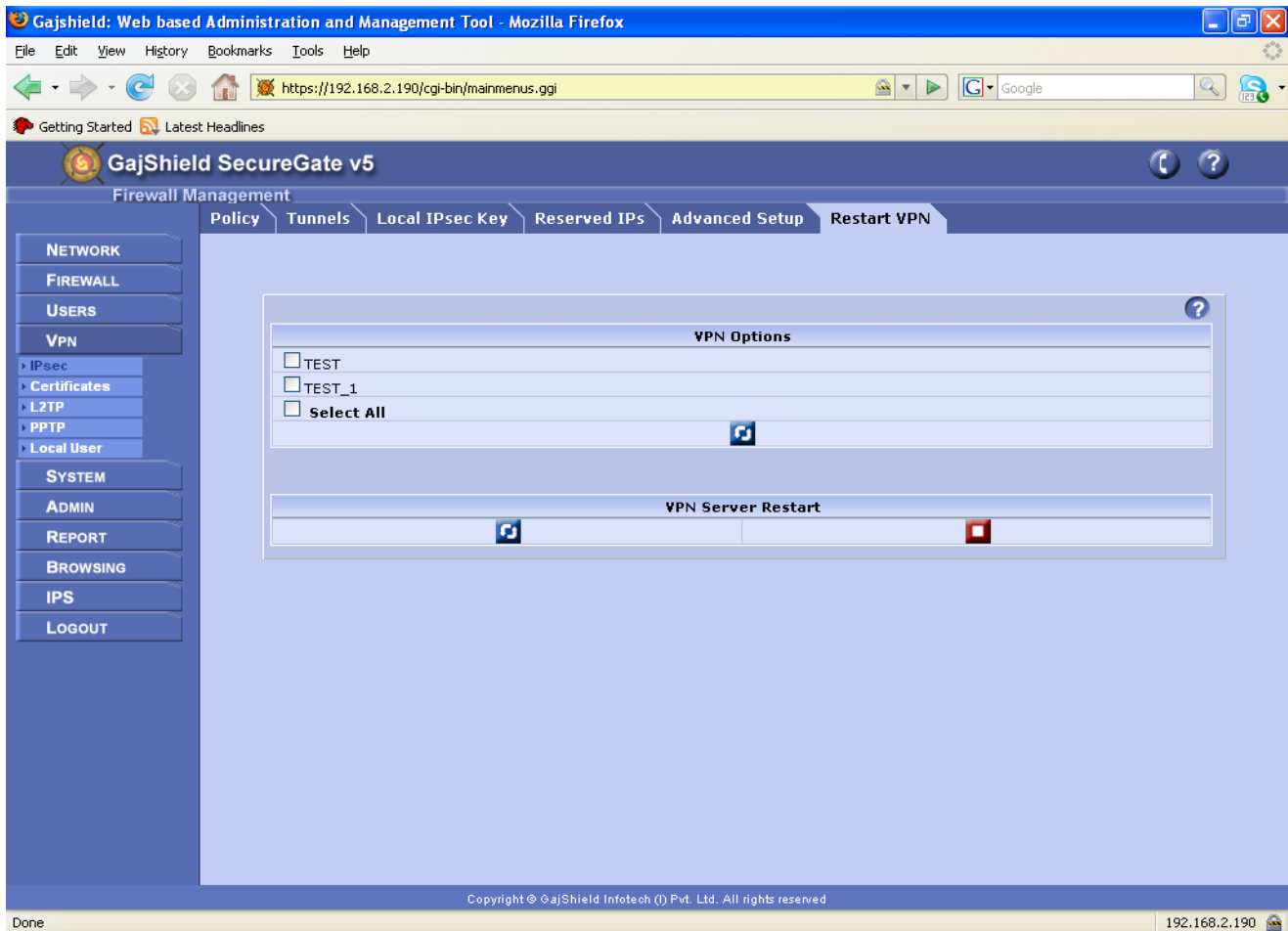


# Restart L2TP



To restart L2TP server select blue tab and to stop the server select red tab.

# Restart VPN



Here if you select the blue tab in vpn server restart then it will restart all the above listed tunnels and if you select red then it will stop the vpn server and if u want to restart select tunnel then mark your tunnel name and select the blue tab it will restart the tunnel which is only selected.

## L2TP-client configuration

