GAJSHIELD INFOTECH PVT LTD

WAN Fail-Over for Internet Browsing

Administrative Guide

WAN Fail-Over for Internet Browsing

Administrative Guide

4, Peninsula Centre ▪ Parel ▪ Mumbai ▪ India 400010
Phone +91 22 66607450 • Fax +91 22 66607454

Configuring ISP Fail-Over for Internet Browsing

You will learn to configure ISP Fail-Over for Internet Browsing with GajShield UPTM in this guide.

This section is used to make settings for enabling the link failover function. We are assuming that you had already configured the ISP1 as a default gateway for GajShield UPTM and ISP2 as a secondary ISP. Now we will learn how to configure Internet Browsing Failover in Transparent as well as in Proxy mode.

For this click on **NETWORK - Advance - WAN Failover**

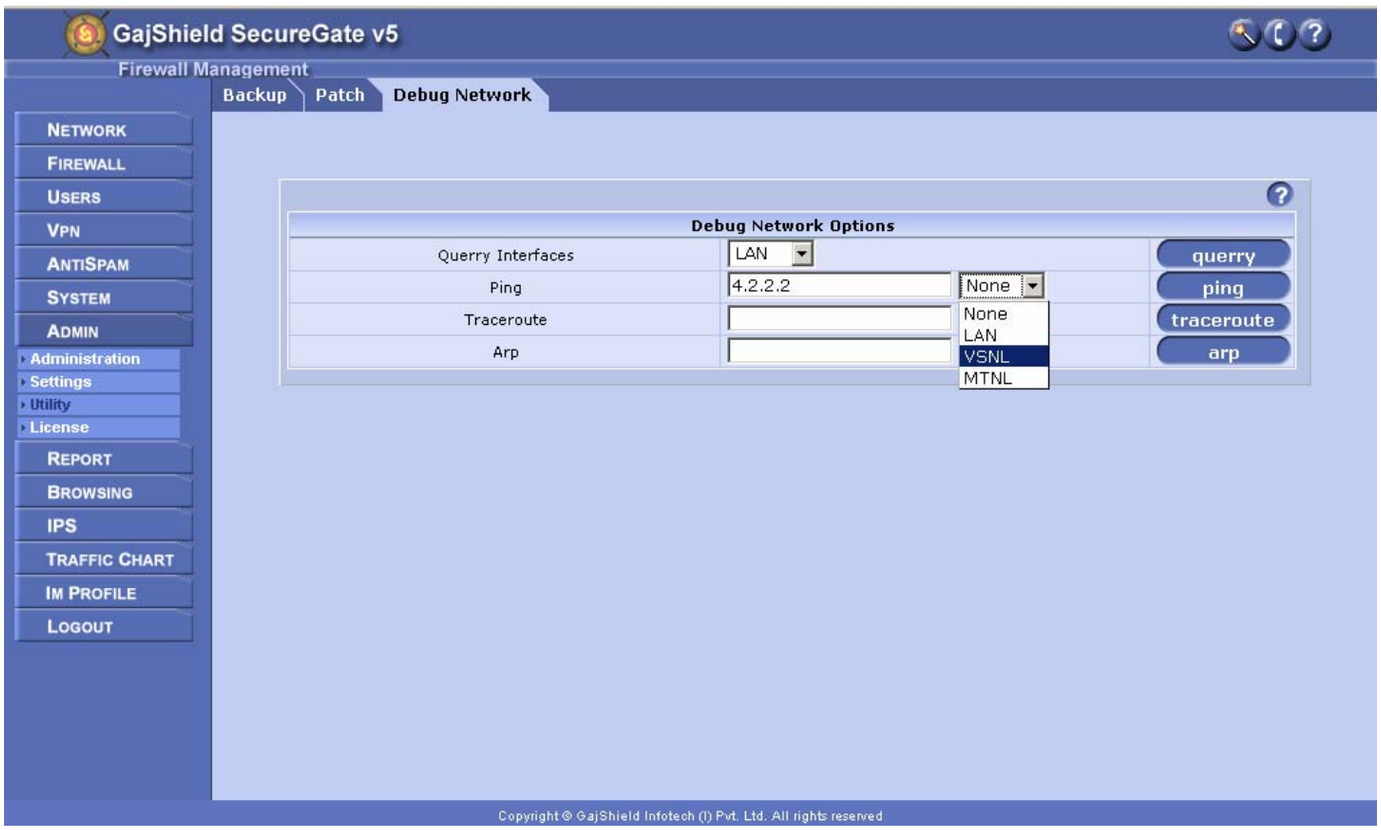
Here, we have to give target IP's to which firewall will send request (ping) continuously from both ISP's. When ISP1 down then it will wait for 2 sec and same request will pass to another ISP. Make sure that whatever target ip's you are configuring that should be ping from all the ISP's which you are configuring on GajShield UPTM.

(**Note:** Third Target IP is optional)

Admin->Utility->Debug Network

The Debug Network option provides a rudimentary set of network tools that can be used from the web interface which includes ping, traceroute and ARP. The results displayed helps checking network connectivity For ping DNS hostname or IP address and click Start. If you simply click on ARP it shows the ARP cache and for getting ARP of a specific system provides the IP address of that machine.

To check the target ip's which we had configured in NETWORK - Advance - WAN Failover are pinging or not from both the IPS's i.e. in our e.g. first we will check the ping to 4.2.2.2 ip from the ISP VSNL



And then check the ping to 4.2.2.2 ip from the ISP MTNL

Other target ip ping you can check by following the above procedure.

Admin->Settings->Email

Now we will configure the email alerts for WAN Failover i.e. whenever any ISP goes down GajShield UPTM will sends the email alerts to the email id's which you had configured in Email Settings

Configure Email Settings:

Default Admin Email ID: In this option configure Email addresses where the alerts should be send

SMTP Server IP: to which server these alerts should be sent. SMTP server i.e. mail server can be local or hosted on internet (recommended mail server is Local Mail server).

Email ID For Service Alerts: From which email id alerts will come

SMTP Server Login: If your outgoing mails requires authentication then you have to provide login name and password information.

SMTP Server Password: Password of the user which created on the mail server for GajShield UPTM.

Proxy authentication with local users [with Wan Fail-over] :

In this section we will learn how to configure your proxy authentication on GajShield UPTM. For same you need to select local in Proxy Authentication Scheme.

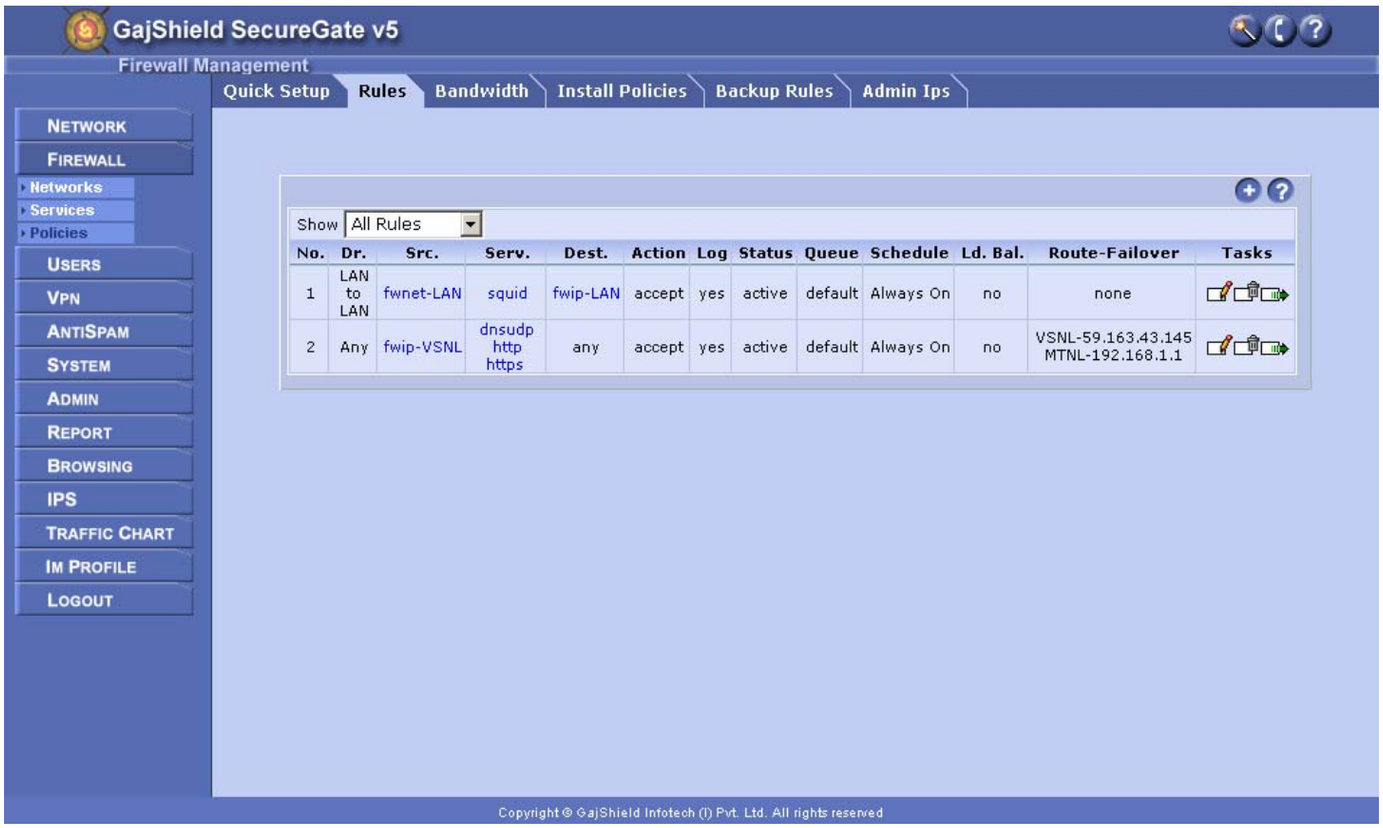
Click on local authentication Proxy Authentication Scheme as you can see in below screenshot:

You need to create user on GajShield UPTM, as user authenticate we had selected as **Local** while configuring proxy settings.

To do this follow below procedure to create user please follow the screenshots below and after then you need to restart your proxy service.

To restart the proxy service on GajShield UPTM click on BROWSING - Setup – Start Proxy and click on restart button.

Below are the policies which will require for configuring GajShield UPTM in Proxy Mode with the WAN Failover.



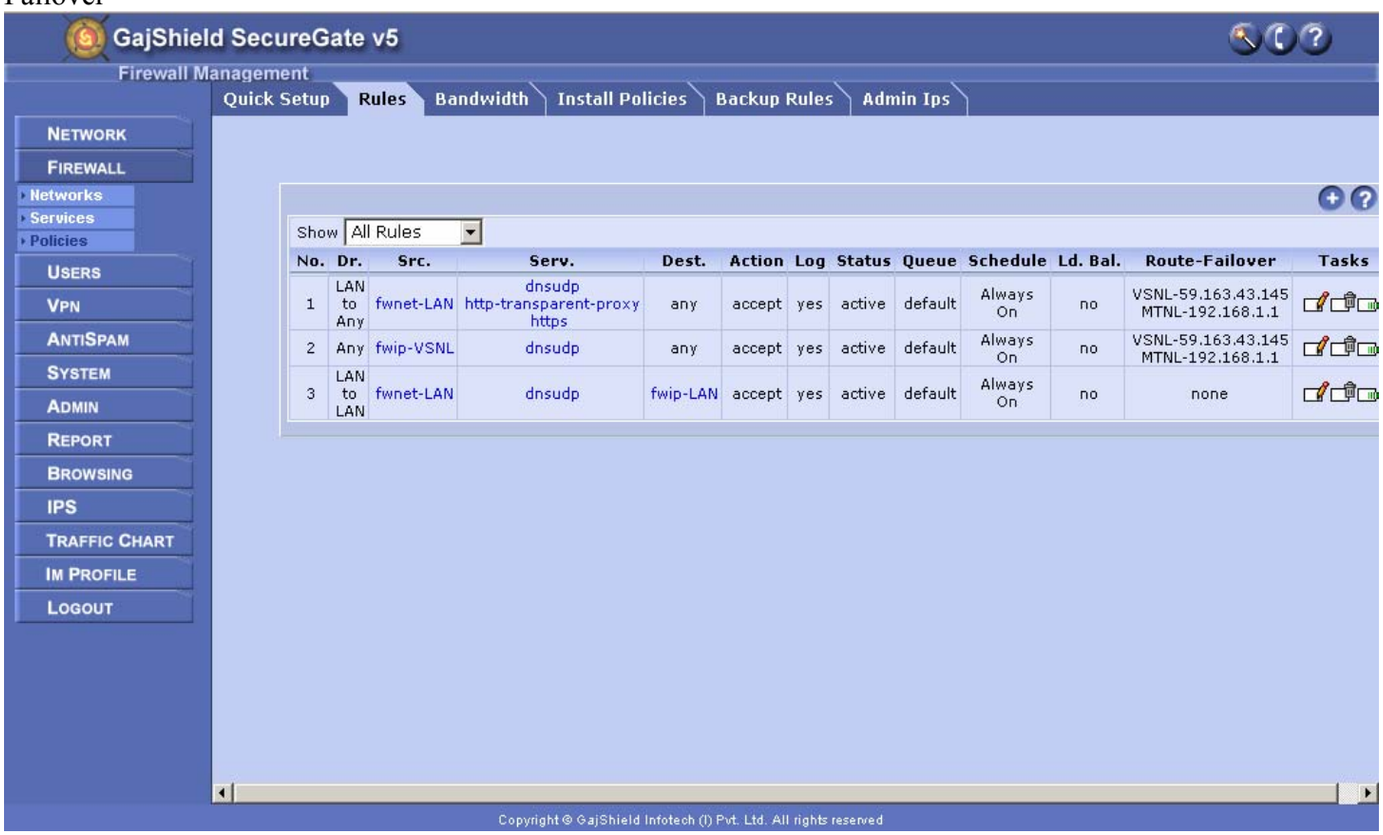
No.	Dr.	Src.	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	LAN to LAN	fwnet-LAN	squid	fwip-LAN	accept	yes	active	default	Always On	no	none	
2	Any	fwip-VSNL	dnsudp http https	any	accept	yes	active	default	Always On	no	VSNL-59.163.43.145 MTNL-192.168.1.1	

1st rule created is for your local network access GajShield UPTM local LAN ip on the proxy port (Port which you had configured in BROWSING – Setup – Browsing Options)
2nd rule created is for ports which normally require i.e. https, http and dnsudp ports to allow from GajShield UPTM to the Internet in this rule we had also configure Failover by selecting Link 1 as VSNL and if VSNL link goes down then all Internet browsing traffic shift to the ISP MTNL and once VSNL link comes up the Internet Browsing traffic shifts back to the VSNL ISP.
Click on Install Polices once you created above two rules to apply on GajShield UPTM.

NOTE:-- In local authenticate mode you need to do proxy setting in client's browser.

Transparent mode with proxy [with WAN Fail-over]:

In Transparent proxy mode all Internet traffic flow through the GajShield UPTM. In transparent proxy mode user authentication not possible, authentication is purely IP based. So in this mode you don't need to create local user or you don't need to do browsing setting on client's browser. Configure rules in policies and configure firewall ip address as a gateway in local system. On firewall in Browsing --- users setting --- users , you need to provide IP ' s in your network, so you can achieve ip based authentication and imposed the Site and MIME Blocking policies.
Below screenshot explains the policies which will require to configure Transparent mode proxy with WAN Failover



No.	Dr.	Src.	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	LAN to Any	fwnet-LAN	dnsudp http-transparent-proxy https	any	accept	yes	active	default	Always On	no	VSNL-59.163.43.145 MTNL-192.168.1.1	
2	Any	fwip-VSNL	dnsudp	any	accept	yes	active	default	Always On	no	VSNL-59.163.43.145 MTNL-192.168.1.1	
3	LAN to LAN	fwnet-LAN	dnsudp	fwip-LAN	accept	yes	active	default	Always On	no	none	

Here in first rule we had opened http-transparent-proxy, https and dnsudp ports from local network to the Internet with WAN Failover
And in second rule created is for to allow GajShield UPTM to resolve dns on the Internet with WAN failover.

Note: In Transparent mode Internet access users have to use GajShield UPTM Local LAN ip as the gateway and DNS server entries provided by the ISP. If you don't want to use ISP DNS then you can use GajShield UPTM Local LAN ip as a DNS server but for this you need to configure **third rule** (which is already configured on above screenshot).