Volume

1

GAJSHIELD INFOTECH PVT LTD

Wan Failover & Load Balancing

Administrative Guide

WAN FAILOVER & LOAD BALANCING

Administrative Guide

© GajShield Infotech Pvt. Ltd.
4, Peninsula Centre ▪ Parel ▪ Mumbai ▪ India 400010
Phone +91 22 66607450 • Fax +91 22 66607454

Configuring WAN Failover & Load-Balancing

You will learn to configure Wan Failover and Load Balancing of WAN traffic in this guide.

GajShield is the only security device which supports policy based failovers. You can designate one or more interface on the GajShield appliance to work as primary or backups for each provided services. Each port can be used as a simple 'active/passive' setup, where traffic is routed through the other secondary interfaces of each policy, when the primary link fails i.e. is down or unavailable. You can also configure these ports in 'active/active' mode, where the user can load balance the traffic through each of the interfaces or ports. This would be referred to as 'load balancing'.

CAVEAT

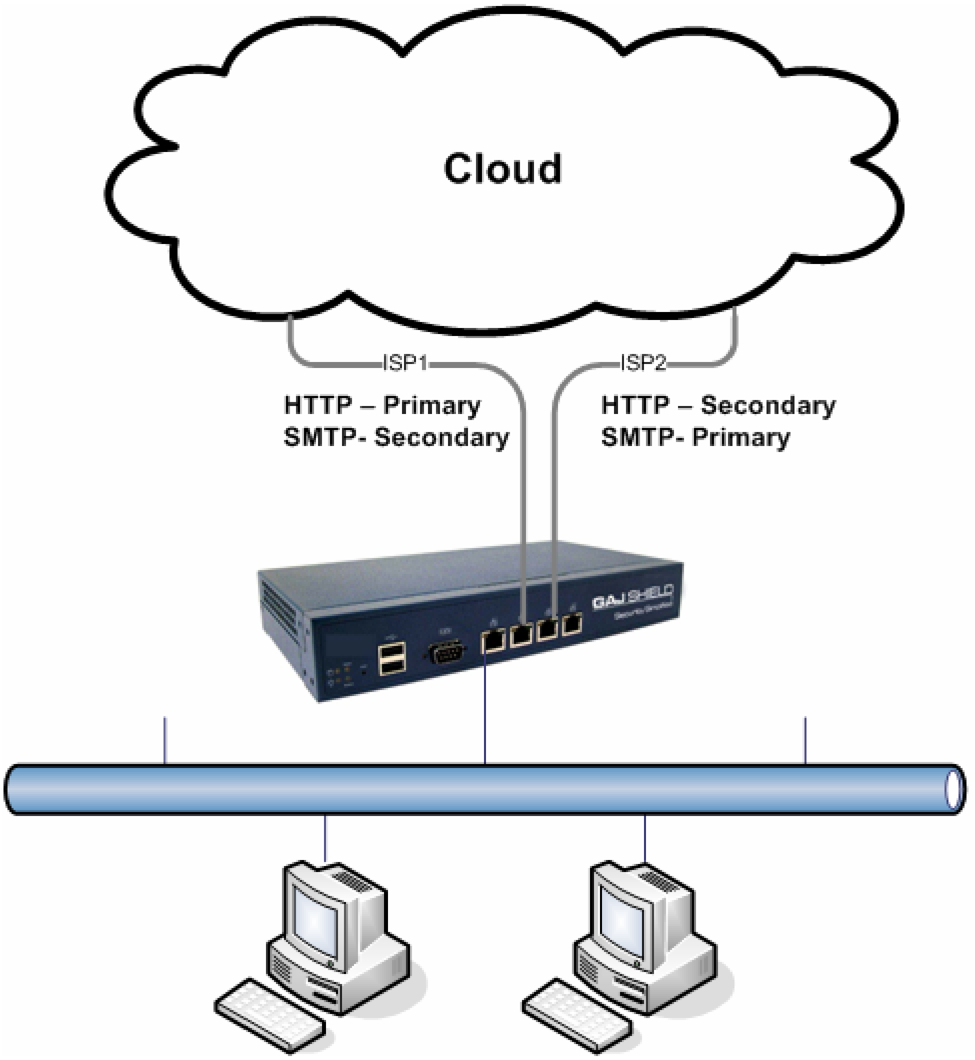
- These concepts and methods apply to all models of GajShield Soft and Hardware appliances.
- WAN Failover & Load-Balancing applies outbound-initiated traffic only; it cannot be used to perform inbound load-balancing functions such as what a content switch or load-balancing appliance provides.
- WAN Failover & Load-Balancing will only work in 'Routing' mode and will not work in 'Transparent' or 'Bridge' mode.
- These concepts and methods apply to all models of GajShield Soft and Hardware appliances.
- Failover and Load Balancing is supported in GajShield SecureGate 5.4 and above.

Steps To Configure WAN Failover

You can have any number of WAN interfaces for Failover and Load Balancing .

- Configure one or more WAN interfaces
- Configure ping monitoring to detect WAN failures
- Configure firewall policies for WAN failover
- Install policies

Sample Environment



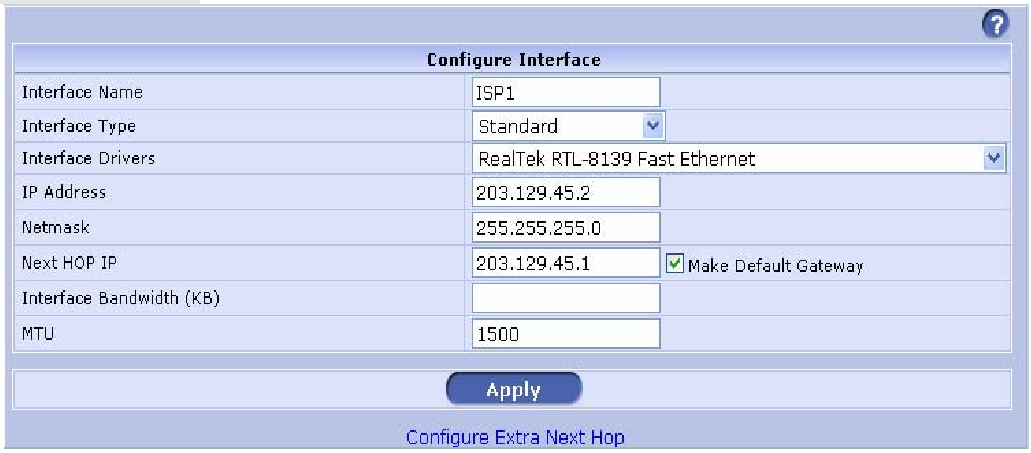
This is a sample environment where GajShield UPTM is connected to two ISPs (ISP1 & ISP2). HTTP traffic is routed through ISP1 and traffic flows through ISP2, when ISP1 fails. Similarly, SMTP traffic is routed through ISP2 and failed over to ISP1 when ISP2 fails.

In the above example, we have shown only two ISPs. But you can have more than two ISPs too. It is assumed that the UPTM used has GajShield SecureGate 5.4 firmware and the basic configuration has already been done on the firewall.

Steps to Configure Wan Failover

①

On Network -> Basic -> Interfaces page, configure the chosen port for WAN connectivity. Provide a name to this port and configure the IP addresses. To ensure, that this port is visible for failover/load balancing/and source routing, provide the Next HOP IP or the gateway provided to you by your service provider.

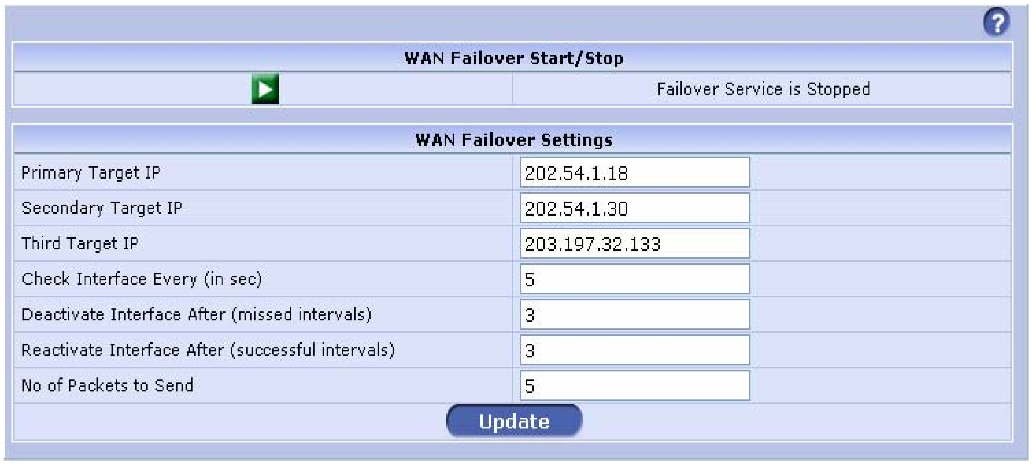


Configure Interface

Interface Name	ISP1
Interface Type	Standard
Interface Drivers	RealTek RTL-8139 Fast Ethernet
IP Address	203.129.45.2
Netmask	255.255.255.0
Next HOP IP	203.129.45.1 ☑ Make Default Gateway
Interface Bandwidth (KB)	
MTU	1500

②

Go to Network->Advanced->WAN Failover to configure the ping monitoring to detect WAN failures. Configure the Main and Alternate Target IPs, the firewall needs to monitor to detect failures. After configuring the given parameters, start the failover.



WAN Failover Start/Stop

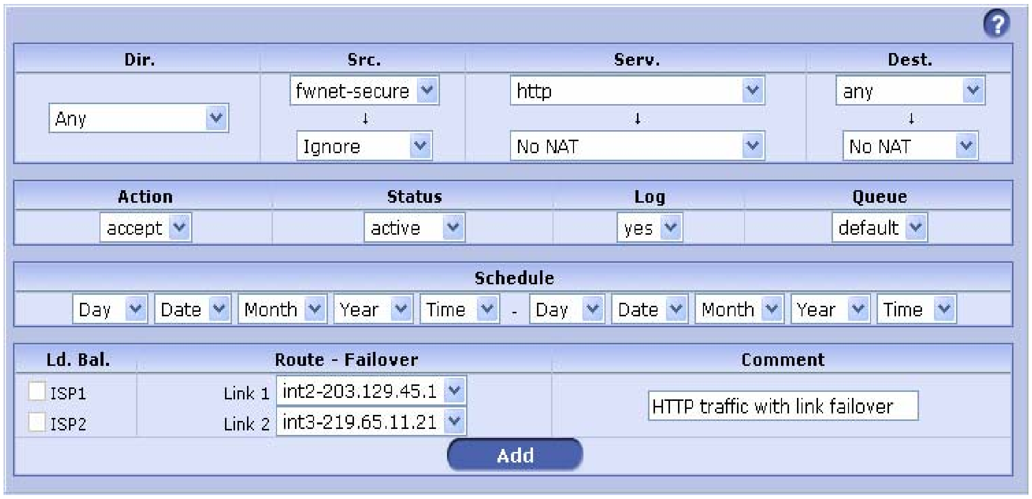
▶	Failover Service is Stopped

WAN Failover Settings

Primary Target IP	202.54.1.18
Secondary Target IP	202.54.1.30
Third Target IP	203.197.32.133
Check Interface Every (in sec)	5
Deactivate Interface After (missed intervals)	3
Reactivate Interface After (successful intervals)	3
No of Packets to Send	5

③

Go to the policy page to configure auto-failover. On Firewall->Policies->Rules, add a policy and configure the failover policy for it. Select the primary link as Link 1 in the Failover column. In our example, we have selected ISP1 on interface 2 as our primary link for the HTTP traffic. Similarly, select the other secondary links. The priority is taken from top to bottom, i.e. the traffic will flow through Link 1, if Link 1 fails, it is automatically routed through Link 2 and then to Link 3 and others. Also, ensure that you select 'Any' as the direction and do not NAT the rule.



Dir.	Src.	Serv.	Dest.
Any	fwnet-secure ↓ Ignore	http ↓ No NAT	any ↓ No NAT

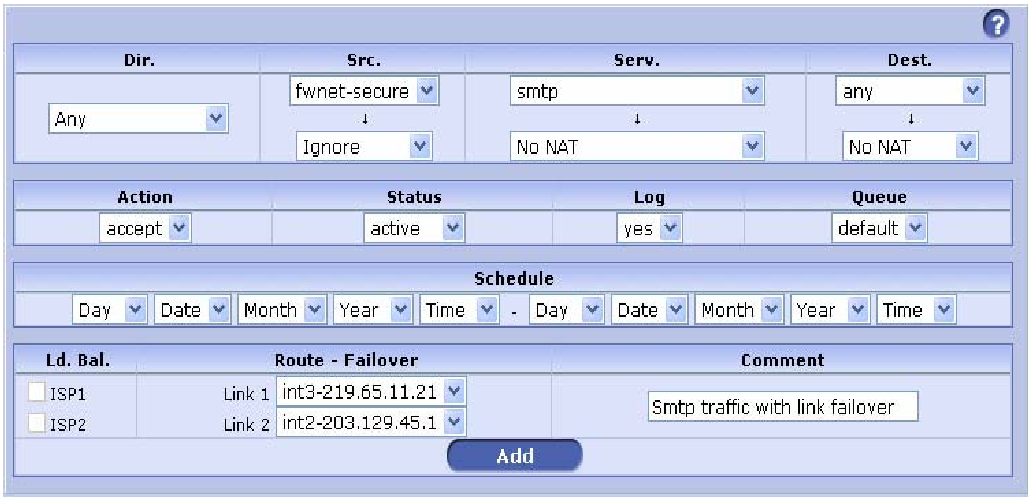
Action	Status	Log	Queue
accept	active	yes	default

Schedule: Day Date Month Year Time - Day Date Month Year Time

Ld. Bal.	Route - Failover	Comment
□ ISP1 □ ISP2	Link 1 int2-203.129.45.1 Link 2 int3-219.65.11.21	HTTP traffic with link failover

④

Similarly, we will also create a rule for SMTP with ISP2 as primary and ISP1 as secondary. Once configured, install the policies. The GajShield UPTM will monitor each link and if any link fails, the traffic flowing through that link will be routed through the secondary links



Dir.	Src.	Serv.	Dest.
Any	fwnet-secure ↓ Ignore	smtp ↓ No NAT	any ↓ No NAT

Action	Status	Log	Queue
accept	active	yes	default

Schedule: Day Date Month Year Time - Day Date Month Year Time

Ld. Bal.	Route - Failover	Comment
□ ISP1 □ ISP2	Link 1 int3-219.65.11.21 Link 2 int2-203.129.45.1	Smtp traffic with link failover

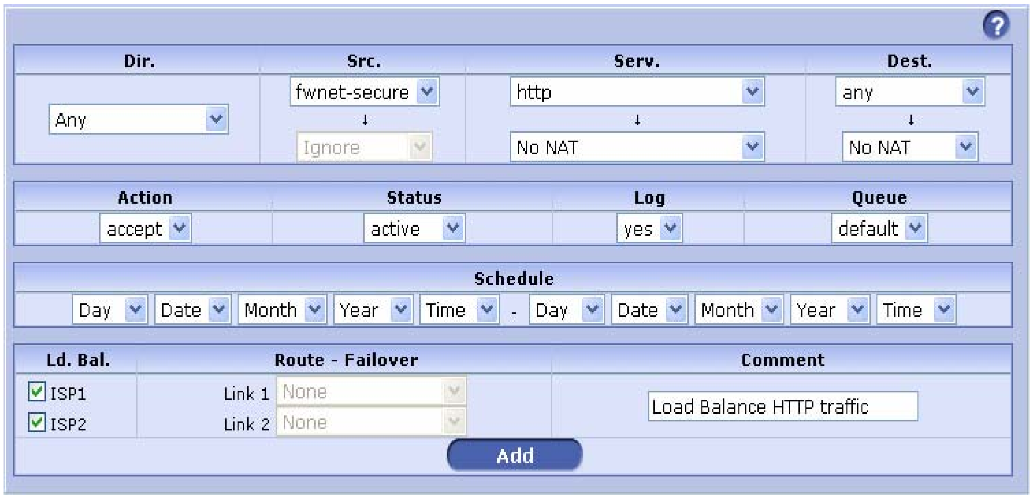
Load Balancing

GajShield UPTM can also be used to load balance the traffic through multiple links. It can be configured for each service or policy set. If any of the links in the chain fail, the traffic will be folder to the next link in the chain. For example, if there are three links i.e. ISP1, ISP2 and ISP3. If HTTP traffic is load balanced between these 3 links and if ISP2 fails, the traffic which was meant for ISP2 will not get folder to ISP3. If ISP3 fails, the traffic will fold over to ISP1 in round-robin.

GajShield UPTM has Auto-Failover on Load Balancing policies too.

In our example, we will configure HTTP traffic to be load balanced between ISP1 and ISP2. Configure the interfaces as discussed above, if you have not configured them. Configure WAN failover settings as shown above

After the above settings are done, go to Firewall->Policies->Rules and configure the rule as shown in the screen below



Dir.	Src.	Serv.	Dest.
Any	fwnet-secure ↓ Ignore	http ↓ No NAT	any ↓ No NAT

Action	Status	Log	Queue
accept	active	yes	default

Schedule: Day Date Month Year Time - Day Date Month Year Time

Ld. Bal.	Route - Failover	Comment
☑ ISP1 ☑ ISP2	Link 1 None Link 2 None	Load Balance HTTP traffic

HTTP traffic will now load balance between ISP1 and ISP2 with auto-failover, if any of the WAN link fails.

Conclusion

GajShield UPTMs support multiple WAN failover on each policy set. There are no restrictions in the number of ISPs you can use to failover the traffic. Similarly, Load balancing not only load balances the traffic, but also fails it over to the other link