



An Introduction to Load balancing and Failover: What to look for when going for Multiple Gateways?

Conventional wisdom holds that the Internet was made to withstand nuclear attack. In reality, outages caused by both bad network design and failures of critical equipment are becoming more commonplace, experts say.

"If you have one single point of failure, you are in trouble."

Most of the Organizations now utilize Internet as a critical part of their business and use Internet for delivering mission-critical content and applications. Organizations running mission critical applications over the Internet understand the importance of having stable, redundant and fast connections for their business needs.

If the physical connection or the ISP goes down, Organization's vital link to Internet also goes down.

By maintaining only one link to the public network, they are faced with a single point of failure and serious network vulnerability. When link fails, the organization and its customers are left with significant downtime and financial loss.

Revenue, customer satisfaction, partner relationships and employee productivity, all are at stake when link goes down. Internet outages impact an organization's email, web sites, applications or VPN traffic.

This has forced Organizations to think of an alternative to provide constant and secure availability/connection to Internet for business continuance.

This awareness of the need for a reliable and continuous connection has resulted in the realization of the importance of having multiple ISPs.

"Multi-home" means provisioning multiple ISP connections over different providers. If a link should fail, traffic may be shifted to an alternate provider. While this solves the immediate problem, it effectively leaves one provider "dark" until a failure occurs. And it is often found that the provisioned resources are not being used in the optimal way.

Although the solution of multiple links is effective in achieving constant and secured Internet connection and reducing the traffic volume on each link, it also requires additional hardware and increases management overhead, including repeated reconfigurations to balance the traffic.

If your organization is planning for multiple links, look for the solution which supports the following features:

1. Easy implementation
2. Load balancing

- Minimum reconfiguration
- Prevent links from overloading
- Continuous availability of Internet/ Internet available all times
- Speed up the User response time
- Provide redundancy and Failover

3. Optimal use of redundant hardware

Load balancing

Industry observers say Organizations who continue to use Internet links for business-critical applications traffic should be looking to load balancing devices that can spread traffic across several ISP links.

Load balancing automatically detects when a gateway stops responding or goes down and quickly reassigns/routes the traffic among the remaining operating links. This safeguard helps you provide uninterrupted, continuous Internet connectivity to your users.

Load balancing equitably distributes the traffic between multiple links to improve the overall performance.

This capability in turn makes it possible to deploy many links rather than a single link.

At the same time, the one-to-one relationship makes it difficult to ensure a high availability of Internet access. In order to ensure that the access is available to the users, single points of failure must be identified and eliminated. In addition to distributing load, a load-balancer must therefore also offer high availability by detecting failures and working around them.

Most of the load balancers:

1. Distribute requests across the pool of links randomly and an already over-burdened gateway may receive even more requests. Worse yet, when a link is down or fails, users may still try to connect to it and receive the dreaded "server down" message.
2. Use the complex BGP (Border Gateway Protocol), which requires coordination and cooperation with ISPs. BGP also requires a certain amount of expertise for implementation and is less flexible.



The optimal utilization of provisioned resources i.e. multiple ISPs requires advanced load balancing and failover to ensure uninterrupted connectivity.

All solutions do not support dynamic weight allocation to the gateways. In most cases unavailable gateways are not recognized and thus proper gateway failover procedure is out of the question.

Cyberoam automatically senses load on each link and dynamically balances load on each link.

For load balancing, Cyberoam uses weighted round robin method. It distributes the traffic across links in proportion to the weights assigned to each link.

Gateway Weight can be selected based on:

- Link capacity
- Bandwidth availability
- Link/Bandwidth cost

For example, if a particular link is not an efficient link, then most requests should be routed through the better link or the traffic is routed to the least expensive link to minimize the bandwidth cost across the varying priced links.

Employing a weighted round robin of load balancing algorithm for traffic including distribution, Cyberoam enables maximum utilization of link capacities across various links based on the aforesaid parameters. It also provides

1. Flexibility of utilizing the total bandwidth of all the links.
2. Bandwidth management flexibility across different size links, preventing bandwidth bottlenecks while minimizing the costs of inefficient bandwidth utilization.

Thus, Cyberoam allows aggregation of links to provide lower bandwidth redundancy while minimizing the spending on idle and costly links.

In other words, Cyberoam distributes traffic across various links, optimizing the utilization of links to accelerate performance i.e. minimizes the response time and reduces operating costs.

Gateway Failover

Any gateway failure means loss of network availability. By deploying multiple links and configuring the connections for automatic failover from one to another, availability can be improved.

Failover is a mode that automatically redirects the traffic to the alternate surviving gateway if any of the gateways fail.

Cyberoam checks the health of the gateways dynamically i.e. continuously checks the status of all the gateways detecting failures in real time and automatically redirects traffic to the operating gateways to guarantee full availability.

Cyberoam selects the active link according to user-configurable load-balancing criteria i.e. defined as weight. This is done transparently without user's knowledge and users see one fast link.

Dynamic allocation makes sure if failover should occur, the traffic is diverted to the surviving gateway. This results in high availability.

Apart from the features stated above, Cyberoam supports few more features:

1. Load balancing on different links without the need of the ISPs' cooperation and the complete operation is transparent to the User.
2. No additional hardware cost for load balancing i.e. Cyberoam is a software solution for load balancing and does not need any hardware component hence saves the cost and time needed to reconfigure the existing setup.
3. Complete view on real time and historical link utilization and performance.

Conclusion

Multiple links enable greater network capacity, performance and availability.

With Organizations' increasing trend towards relying heavily on network-intensive applications, Users and IT staff will benefit from deploying multiple links.

Each link adds more capacity. Cyberoam automatically balances the traffic across all the links. Since the distribution of traffic among the links is automatic, there is no need to

reconfigure the network. The existing IP address is shared by all of the links, and traffic is always balanced among them.

Combining load balancing with failover is a cost-effective, flexible strategy to provide high availability and high performance. Cyberoam presents an excellent solution for organizations seeking to implement this strategy. By offering high availability and failover solutions, Cyberoam helps you to achieve the goal of providing a speedy and continuous service.

For more information on Cyberoam's Unified Threat Management, go to www.cyberoam.com

Download a free evaluation copy at www.cyberoam.com/trialversion

Contact
info@cyberoam.com



Elitecore Technologies Limited

www.elitecore.com

India

Tel: +91-79-26405600, Fax: +91-79-26407640

USA

Tel: 201-484-7581, Fax: 201-777-2113

Australia

Tel: 61-413939862, Fax: 61-296319091