STONESOFT

Whitepaper

A Practical Guide to ISP Redundancy and Uninterrupted Internet Connectivity

Table of Content

Executive Overview

Today, enterprises require their mission critical communications to be available 24/7. In an effort to achieve their goal of end-to-end availability, many organizations turn to Internet Service Provider (ISP) multi-homing, which is the use of more than one ISP to guarantee connectivity and increase bandwidth at a lower cost. However, while ISP Multi-homing has been possible for quite some time, implementation has typically required complicated solutions such as redundant routers and switches, routing protocols and peering agreements between ISPs. In addition to being complex, these approaches are expensive both to implement and administer. Stonesoft solves the ISP multi-homing problem with its patented StoneGate Multi-Link Technology, providing highly-available ISP connectivity in a simple and straightforward manner. With StoneGate, Internet access is no longer a single point of failure in your enterprise network.

> "Any enterprise that requires consistently available access to and from the Internet should seriously consider using multiple ISP connections into the enterprise network."
>
> William Terril, Burton Group (Business Communications Review, May 2003)

This paper introduces StoneGate Multi-Link Technology as a solution to enterprises' ISP multi-homing needs. It discusses how Multi-Link optimizes the use of network providers— such as ISPs—and realizes the full benefits of virtual private networks (VPNs). It describes Multi-Link operating principles and functionality with respect to other relevant technologies. Finally, how you can fully benefit from implementing Multi-Link in your network.

StoneGate Multi-Link represents a significant advance in multi-homing technology. Enjoy guaranteed network access and the best throughput available at all times. Use multiple network providers for Internet connetcions and VPNs for optimal network performance. Reduce costs by eliminating the need for speciliazed network equipment, software and protocols.

The Challenge

As the role of Internet driven business grows, the reliability of connections and constant availability of services is an absolute necessity for corporations. Because of the risk of downtime, corporations have become very adept at making their networks highly available by implementing solutions such as redundant gateways, firewalls, switchers, routers, and other highly available network components. However, even with the use of such methods, the corporate network can be subject to outages if a network link, such as an ISP, fails.

> "With two separate lines coming in from two directions, we have eliminated our risk of data communication downtime."
>
> Charles Smith, Director of Management - Information Systems, Plaza Construction Corporation

ISP failure comes in many shapes, sizes and colors. For example, your ISP could be taken down by a Denial of Service (DoS) attack or by a malicious virus or worm. Outages may also occur from a routing misconfiguration by the ISP, which may take some time to locate and rectify. ISPs can also be brought down due to non-technical reasons such as a network line that is cut due to road construction, the ISP filing for bankruptcy, or some physical catastrophe such as fire, earthquake or flood. Whatever the reason, the result is the same; despite all efforts to make your network highly available, your connectivity comes to an abrupt halt just the same.

Figure 1 illustrates how individual ISP connections can create single points of failure in traditional network topologies.

In order to eliminate the ISP as a single point of failure, many corporations have had to deploy a battery of redundant external routers and switches, requiring the use of complex routing protocols, such as Border Gateway Protocol (BGP) and Hot Standby Routing Protocol (HSRP), and peering arrangements through ISPs. Others have viewed this approach as too complicated and expensive as it requires redundant hardware, more expensive routers, additional software and ISP arrangement costs, just to get started. Once implemented, administrators are faced with the daunting task of confi guring and maintaining the complex network in order to achieve high availability.

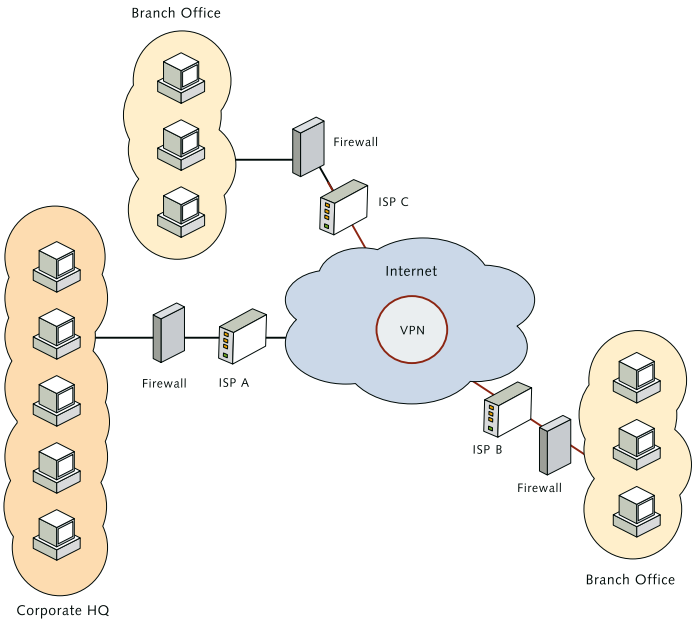

Figure 1: Traditional Approaches: Single Points Of Failure

To illustrate this point, we simply need to examine BGP a bit further. BGP is a routing protocol designed to allow the creation of redundant routes to a set of networks. BGP, however, creates additional complexity and expense. For example, BGP requires attaining an autonomous system number. Basically, this is a unique ID that identifies your corporate networks to routers on the Internet, and allows other routers to understand there is more than one way to get to your network. But this ASN, as it is often known, requires your ISPs to cooperate. For medium enterprises, or even some larger enterprises, and service providers, this cooperation between competing ISPs may be difficult to achieve. Those businesses on a tight budget also face the costs of upgrading routers with the additional memory and software to perform the complex dynamic routing BGP requires.

What companies need is a way to make ISP connections redundant in a single simple solution, without expensive hardware or software, complex configuration or cooperation between service providers. Ideally, this solution should also address additional challenges such as the security of your system, fault tolerant VPNs, load-balancing, scalability, upgradeability and manageability.

The Solution: StoneGate Multi-Link Technology

StoneGate Multi-Link Technology provides a simpler way to create ISP redundancy and ensure uninterrupted Internet connectivity. Multi-Link eliminates the need for complicated and expensive third party hardware and software solutions and eases the pain of network administration considerably. With StoneGate, Internet access is no longer a single point of failure in your network.

With Multi-Link, you can easily add multiple Internet connections to your network by utilizing multiple ISPs, leased lines or a combination thereof. This enables you to:

- ensure that your network connection will be always available, even if your ISP fails or its taken off line improve your Internet performance with increased bandwidth
- provide for easy migration from one ISP to another
- implement a gradual and transparent migration from costly leased lines or frame relay with the option to keep them as backups when needed
- increase client and customer satisfaction
- save money

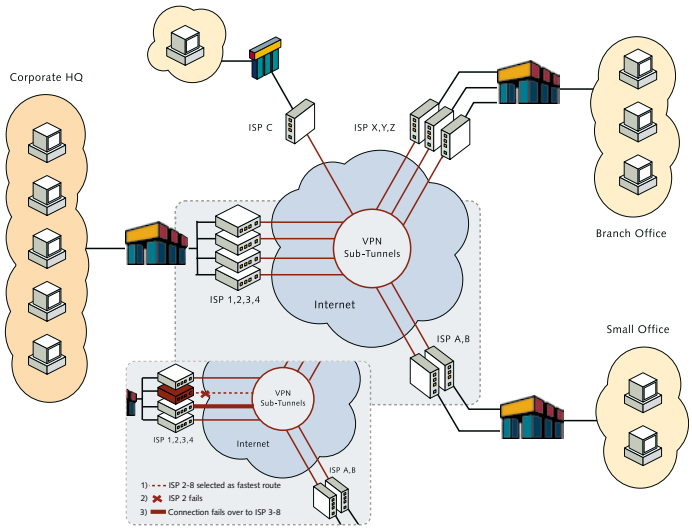

Figure 2: StoneGate Multi-link Technology

StoneGate Multi-Link removes your ISP as a single point of failure by allowing you to establish multiple Internet links simply and cost effectively. If one link fails, traffic is automatically failed over to the remaining links. Multi-Link supports all sorts of Internet links, such as ISDN, DSL, leased lines, modem connection and even satellite. With Multi-Link, you can guarantee that you always have Internet connectivity when you need it.

StoneGate Multi-Link Technology comes prepackaged as part of Stonesoft's StoneGate High Availability Firewall and Multi-Link VPN solution. For more information on the StoneGate Firewall and the entire StoneGate Security Platform, please visit Stonesoft's Web site at: http://www.stonesoft.com/ products/

With StoneGate Multi-Link Technology, you no longer need to worry about your ISP being taken down by a DoS attack or malicious virus. You can rest easy knowing that if a backhoe digs up the cable between you and your ISP, you will remain connected. If your ISP misconfi gures their routing table, goes bankrupt or suffers a major catastrophe, your business continues as usual as StoneGate seamlessly routes your connections through the remaining network links.

However, continuous connections are not the only benefit to StoneGate Multi-Link Technology. In addition, it also improves the performance of your Internet connectivity. It does this by load balancing both inbound and outbound traffic across any number of Internet connections, choosing the fastest available outbound connection. Since every connection is the fastest available, combined throughput exceeds that of a single connection with fluctuating service. Your network benefits from momentary performance peaks and avoids delays.

Multi-Link Technology comes pre packaged as part of the StoneGate High Availability Firewall and Multi-Link VPN solution. As such, it comes with Stonesoft's clustering and load-balancing technology built-in. When Multi-Link is used together with clustered StoneGate firewall gate-

ways, load balancing between nodes provides further reliability to the network architecture. Connections lost due to node failure can be recovered transparently, with no apparent loss of service.

Even though the problems that Multi-Link solves are complex, implementation is remarkably simple and cost efficient. In contrast to traditional solutions, StoneGate's Multi-Link Technology requires no additional or specialized hardware or software. This significantly reduces comparable implementation and maintenance costs. Furthermore, Multi-Link provides ISP redundancy without the need for peering agreements between competing ISPs. In fact, your ISPs don't need to communicate with each other at all. This helps simplify implementation, system maintenance and troubleshooting tremendously.

Multi-Link provides further cost savings, by allowing you to migrate from expensive leased line solutions to more cost effective ones. This migration is made simple by the fact that you can keep your current connections during the migration, and only fully transfer over when you have completed the process.

Making Your VPNs Reliable with Multi-Link

VPNs offer enterprises a cost efficient way to secure their communications compared to other alternatives, such as leased lines. However, VPN connections have proven to be unreliable and therefore, risky for business critical communication. StoneGate Multi-Link solves this problem by adding fault tolerance and transparent fail over to your VPN tunnels and VPN client connections. With Multi-Link, your VPN connections can become as reliable and even more secure than your old leased lines.

> "We needed a solution that would not only secure the VPN, but would assist with performance rather than be a drain on it."
>
> Ales Zupan Ph.D. Si.mobil

Transparent fail over means that your customers and internal users remain constantly connected, even if one or more connections are lost. Multi-Link improves your VPN performance significantly, as it always chooses the fastest route for your users' connections. Higher bandwidth and lower latency helps support new technologies such as Voice over IP (VoIP) and video conferencing. Increased customer satisfaction based on a better user experience improves your bottom line.

Added Security

StoneGate Multi-Link Technology is an integrated part of the StoneGate Firewall and VPN. As such, it allows you to introduce added security and manageability to your network at no extra cost. You can utilize the StoneGate Firewall functionality as a "second skin" firewall, or as your primary enterprise security solution depending on your needs. StoneGate's powerful features such as uni.ed management with StoneGate IPS, remote upgradeability, and built-in reporting tool add even greater value. For more information on the StoneGate Firewall and the entire StoneGate Security Platform, please visit our Web site at: http://www.stonesoft.com/products/

Assessing the Alternatives

As previously explained, technologies other than Multi-Link can be used to support multiple ISP connections, although they fall short of the performance you can expect from Multi-Link Technology. For instance, Border Gateway Protocol (BGP) routes connections using an algorithm that determines the shortest path, calculated by the number of hops (routers) between source and destination. Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) are used to make routers highly available. All these specialized protocols, whether they are used for router redundancy or for choosing the fastest route, are not required but can coexist on your network with your StoneGate Multi-Link implementation.

Border Gateway Protocol (BGP)

Organizations that maintain multiple Internet links to ensure high Internet availability often implement Border Gateway Protocol (BGP), which can be described as follows:

- BGP is routing technology that selects packet routes from all available ISPs.
- BGP shares the load but because it does not measure performance it does not perform true load balancing.
- BGP offers high availability for outbound packets but cannot manage problems routing inbound packets.
- BGP chooses carriers without measuring their performance. When BGP chooses slow or congested carriers, network performance suffers.

Limitations

BGP is an ISP-level solution. It is not designed for implementation by end users so it requires specialized ISP resources and equipment. For instance, implementing BGP requires an ISP-independent IP address range. This poses significant risk of service failures leading to incorrect routing unless the end user successfully negotiates dedicated cooperation between rival ISPs. The implementation is itself a multi-step process with several activities that fall well beyond the normal bounds of software configuration. The implementation team must negotiate agreements between rival ISPs, acquire and configure sophisticated hardware and routing schemes, and must possess advanced BGP programming expertise.

In comparison, Multi-Link is a single solution that requires no additional or specialized hardware or software. This significantly reduces comparable implementation and maintenance costs. Multi-Link selects the connection with the fastest throughput, while BGP cannot tell whether a path with more hops is faster than a congested path with fewer hops. Finally, Multi-Link resides on the StoneGate gateway and does not require additional processing capacity or hardware, while BGP resides on the router and requires extra processing capacity to calculate the shortest path, which is an added expense.

External Load Balancers

External load balancers are appliances that sit in front of a network gateway. They are not dependant on BGP or any other routing protocol, and in fact, use methods similar to Multi-Link in order to address multiple ISPs.

Limitations

External load balancers require special equipment and constant maintenance. Even under the best circumstances however, they cannot participate in a VPN network without slowing network performance.

Like BGP, the end user wanting to implement load balancers must purchase specialized hardware. External load balancers require specialized network components to use multiple ISPs, such as a pair of gateways and a pair of load balancers (for achieving high availability on the load balancers), which adds to the cost of implementation.

External load balancing equipment requires constant supervision, administration, and system updates, adding to maintenance costs. Administrators must also ensure the separate con. gurations of the gateway and the load balancing box are consistent, adding to the technical complexity of the management process.

Conclusions

Multi-Link Technology provides a simple and cost effective way to create ISP redundancy and ensure uninterrupted Internet connectivity. Designed for ease-of-use, implementation requires no specialized equipment, software or ISP peering agreements. It enables you to seamlessly integrate multiple network providers to create fault tolerant and highly available connections without having to change your existing network infrastructure.

When compared to other ISP multi-homing solutions, StoneGate increases performance by providing true ISP load balancing, provides greater flexibility for implementation and significantly reduces administration costs, all while adding security to your network with the StoneGate Firewall. In addition, Multi-Link provides a significant increase in VPN reliability and performance. The ability to fail over VPNs among multiple providers is unique to Multi-Link technology, and cannot be achieved by other means.

STONESOFT

Stonesoft Corp.

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 712 34

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 6681 125
fax. +1 770 6681 131

Stonesoft Corp.

90 Cecil Street
#13-01 Carlton Building
Singapore 069531
tel. +65 6325 1390
fax. +65 6325 1399