

Augmented VPN

Optimizing Network Security,
Performance and Cost Efficiencies

Table of Contents

Executive Overview	3
Augmented Connections	4
Augmented Bandwidth	7
Augmented Priority for Business Traffic	9
Augmented Cost Efficiency	10
Security Bonus	12
Artificial intelligence in Augmented VPN	13
Assessing the Alternatives	14
Border Gateway Protocol (BGP)	14
External Load Balancers	15
Conclusions	16

Executive Overview

Comparing an augmented VPN to a traditional VPN is similar to comparing a car navigator to a simple road map. Both use the same basic information, but there is a huge evolutionary step between them. A car navigator has much more embedded functionality such as location awareness, current traffic information, search functionality, service locator, route tracking and other functions that have provided the evolutionary step forward.

A similar development is taking place in Virtual Private Networking (VPN). During the early phase of the globalization it was enough for a company to be able to connect their offices and production sites with each other with a simple VPN or point to point dedicated circuit. However, the situation has changed dramatically since those days.

There are three basic problems that companies are facing today:

1. The production systems are online and they need to be available at all times and from any location. One CIO said that one hour downtime for their systems had same stress level effect for him as a one hour divorce discussion with his ex-wife. The truth is that many companies cannot operate anymore without online systems like ERP, mail or cloud based services like Salesforce.com. Is there a cost effective way to provide backup connections if the Multi-protocol layer switching (MPLS) connection fails?

“One hour downtime for our systems had same stress level effect for me as a one hour divorce discussion with my ex-wife.”

2. The internet connection is always too limited and its usage is growing every day. How to differentiate between critical production traffic and other traffic? How to provide enough capacity for critical business traffic and yet allow other traffic when there is excess capacity? Is there a way to direct only production traffic via the MPLS connection and use a more cost efficient connection for the rest?

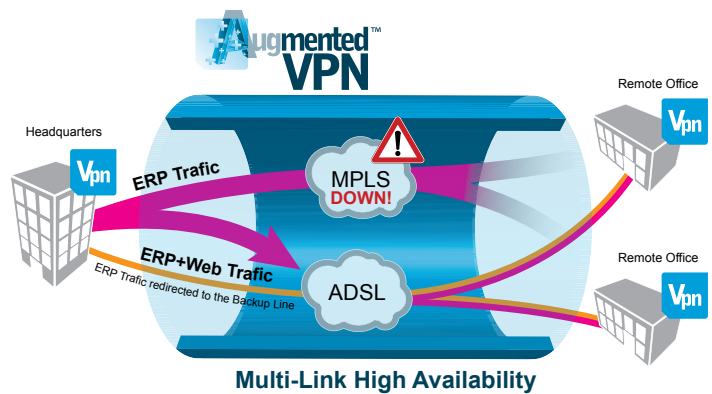
3. Network connection costs are too high. Many companies are global and they need to have a reliable and fast enough connection between their production sites and business offices. For example, an MPLS provides reliable connection between sites, but it will become very expensive if used between several countries around the globe.

This whitepaper will provide solutions to these three problems and, on top of that, an additional security bonus.

Augmented Connections

Let's take an example organization that had their production sites on the mainland USA and one of their sales offices in Bermuda. Their problem was that their Bermuda office was totally dependent from the connection to their production sites. They had one MPLS connection between the production site and the Bermuda office. The CIO was still worried because Bermuda is a known hurricane area. One big hurricane could disrupt the communication lines and put the company out of business for a long time.

The company compared several different options including satellite backup connections and an additional MPLS connection from another internet service provider using Border Gateway Protocol (BGP). All alternatives turned out to be quite complex and costly. The company ended up with StoneGate Multi-Link Firewall/VPN solution using two MPLS connections from two different internet service providers. This way they did not have to go through the cumbersome BGP setup and they got highly available connections.



About one year after that a category four hurricane swept over and took out one of the main internet service providers in Bermuda. Once that information was in the news, one of the Stonesoft support personnel called the organization's IT manager and asked if they had noticed that one of their internet service providers had been wiped out. IT manager said that he had not noticed anything - their connections were functioning flawlessly. This is just an example of the power of the StoneGate Multi-Link. The traffic from the failing internet service provider connection was automatically transferred to the still functioning one. Business continued like nothing had ever happened.

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, organizations have become very adept in making their networks highly available by implementing solutions such as redundant gateways, firewalls, switches, routers, and other highly available network components. However, even when using such methods, the corporate network can suffer from outages if a network link to the Internet or to the other production sites fails.

Internet service providers can provide a variety of different network links, but they all are subject to a failure. Even MPLS connections are vulnerable. An ISP failure may come in many shapes, sizes and colors. For example, your Internet service provider could be taken down by a Denial of Service (DoS) attack or by a malicious virus or worm. Outages may also result from a routing misconfiguration by the Internet service provider, which may take some time to locate

and rectify. Internet service providers can also be brought down by non-technical reasons such as a network line that is broken because of a road construction, the Internet service provider filing for bankruptcy, or some natural hazard such as earthquake, landslide, volcanic eruption 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.

In order to eliminate the Internet service provider as a single point of failure, many corporations have had to deploy a battery of redundant external routers and switches, which require the use of complex routing protocols, such as Border Gateway Protocol (BGP) and Hot Standby Routing Protocol (HSRP), and peering arrangements through Internet service providers. Others have regarded this approach as too complicated and expensive as it requires redundant hardware, more expensive routers, additional software and Internet service provider arrangement costs, just to get started. Once implemented, administrators face the daunting task of configuring and maintaining the complex network in order to achieve high availability.

To illustrate this, 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 expenses. First, one is required to get provider independent IP address space and autonomous system number (ASN). This may not be possible for IPv4 addresses today.). Basically, an ASN is a unique ID that identifies corporate networks to routers on the Internet, and allows other routers to understand there is more than one way to get to the network. To make use of a provider independent address space, organization must negotiate agreement with at least two different ISPs on routing for their ASN. For medium-sized companies, or even some larger enterprises and service providers this may be challenging to arrange. Moreover, businesses with a tight budget also face the costs of upgrading routers with additional memory and software to perform the complex dynamic routing required by BGP.

What companies need is a way to make Internet service provider connections redundant with 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 the system, fault tolerant VPNs, load-balancing, scalability, upgradeability and manageability.

StoneGate Multi-Link Technology provides a simple way to creating Internet service provider redundancy and ensuring uninterrupted Internet connectivity. Multi-Link eliminates the need for complicated and expensive third party hardware and software solutions and makes network administration significantly easier. With StoneGate, Internet and VPN access is no longer a single point of failure in the network.

With Multi-Link, organizations can easily add multiple Internet connections to their network by utilizing multiple Internet service providers, leased lines or a combination thereof. This enables companies to:

- ensure that their network connection will be always available, even if your Internet service provider fails or it is taken offline
- improve their Internet performance with increased bandwidth
- provide for easy migration from one Internet service provider to another
- implement a gradual and transparent migration from costly leased lines with the option to keep them as backups when needed
- increase customer satisfaction

StoneGate Multi-Link eliminates the Internet service provider as a single point of failure by allowing the organization to establish multiple Internet links simply and cost effectively. All of the links are active and in use. If one link fails, traffic is automatically transferred over to the remaining links. Multi-Link supports all kinds of Internet links, such as ISDN, any type of DSL, leased lines, modem connection and even satellite. With Multi-Link, companies know they will always have Internet connectivity when they need it.

With StoneGate Multi-Link Technology, organizations no longer need to worry about their Internet service provider being taken down by a DoS attack or malicious virus. If a backhoe digs up the cable between them and their Internet service provider, they will remain connected. If their Internet service provider misconfigures their routing table, goes bankrupt or suffers a major catastrophe, their business continues as usual with StoneGate seamlessly routing their connections through the remaining network links.

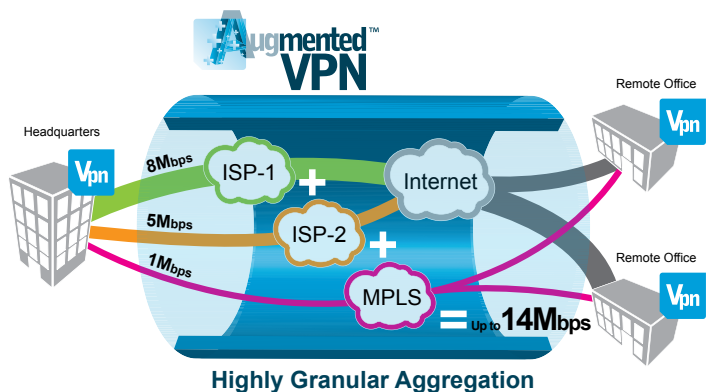
Multi-Link Technology comes pre-packaged as part of the StoneGate High Availability Firewall and Multi-Link VPN solution. As such, it comes with Stonesoft's clustering and load-balancing technology built-in. When Multi-Link is used together with clustered StoneGate firewall gateways, load balancing between 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, the implementation is remarkably simple and cost efficient. Unlike 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, the ISPs do not need to communicate with each other at all. This significantly helps to simplify implementation, system maintenance and troubleshooting.

Augmented Bandwidth

Another case, an organization had problems with their Internet connection capacity. Their main business traffic consisted of CRM traffic, which was offered as a cloud service for them. First, they had a MPLS connection, but its bandwidth soon became a bottleneck when the other Internet traffic increased and their employees started to use social networking services like Facebook and LinkedIn. Social networking was part of their customer service and marketing approach, so they could not prohibit the use of those services. They increased the MPLS connection bandwidth to 8 Mbps and that provided relief for a while. However, quite soon even that pipe was almost 100% utilized.

Now they were facing a bigger investment decision, because their Internet service provider offered up to 8 Mbps connection using normal telephone (copper) lines. For speeds higher than 8 Mbps they either had to have a fiber connection from their internet service provider or a wireless radio link. Fiber connection speeds can go up to tens of gigabits per second and wireless radio links can go up to 100 Mbps. Both options would include additional hardware and set-up fees, because both options required the ISP to install new equipment to the premises. Neither option was not available immediately, whereby the setup time varied from 3-5 weeks up to 2 months. That was too long for the organization. They needed the new bandwidth immediately.



Fortunately, the company was using StoneGate Augmented VPN solution. Multi-Link technology allows aggregating several low cost lines to one bigger line. For example, two 5 Mbps ADSL lines can be used to create one 10 Mbps line. The company in question purchased two 5 Mbps lines from the Internet service provider to provide immediate relief to their bandwidth needs. In the future, they can add even more new low cost lines if their bandwidth needs increases. An additional benefit is also improved high availability, because the additional lines provide redundancy in case of a line failure.

Example of VPN configuration:

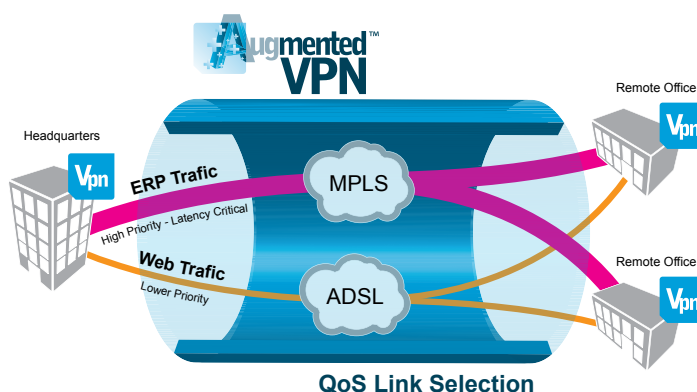
- CRM Traffic = priority 1 = forced on the MPLS link with backup line on ADSL 1
- HTTP Traffic = priority 4 = forced on the active links ADSL 1 + ADSL 2

Multi-Link improves VPN performance significantly, as it allows connections to transparently select different VPN links based on traffic volumes and network conditions. With QoS based preferred link selection configuration different traffic can be by default be directed to different links. Critical CRM traffic can have the best link as the active link and other links as backup links. Unimportant traffic can then have only some of the links in use so that bandwidth is always saved to more critical traffic.

Higher bandwidth and lower latency help support new technologies such as Voice over IP (VoIP) and video conferencing. Last but not least, the company benefits from increased customer satisfaction based on a better user experience.

Augmented Priority for Business Traffic

Let's take, for example, a global retail company that had been using one MPLS connection from each of their locations to their central datacenter where their main SAP system was located. The problem was that the SAP traffic did not always have enough bandwidth available. The reason for this this bandwidth problem was that the other traffic (email, Internet browsing and so on) was driven through the same MPLS connection. The retail company wanted to remove the other traffic from the MPLS connection, to make sure the SAP traffic would always have enough bandwidth. The company had a lot of offices, so adding a second MPLS connection everywhere was too costly. Raising the capacity of the MPLS connection was also considered, but it was expensive and additionally there was the problem of a single point of failure of the MPLS connection. Even though the company had good service level agreements with their Internet service provider, their maximum compensation for the connection outage was as high as the subscription payments they had already paid. In case of a connection outage, it would not cover the production losses, so the company wanted to have a cost effective backup connection for the SAP traffic.



This case illustrates the issues that organizations are facing today. The retail company solved their problems with the use of Augmented VPNs. They bought an additional ADSL connection to all their offices. That was a very cost effective way to get more bandwidth to each location. Then they used StoneGate Multi-Link technology for load balancing the traffic between the ADSL and MPLS connections. They used quality of service (QoS) feature for the SAP traffic prioritization. That means that SAP traffic has always priority in the MPLS connection and the other traffic is automatically directed to use the ADSL connection. If there was unused capacity on the high quality MPLS connection, the other traffic was able to use it. This way the expensive and high quality MPLS connection was utilized close to 100% all the time. On the other hand, the cost effective ADSL connection provided capacity expansion whenever needed.

Example:

- SAP Traffic = priority 1 = high priority on the MPLS link
- HTTP Traffic = priority 4 = normally using ADSL + low priority on MPLS link

Augmented Cost Efficiency

A global manufacturing company wanted to use lower cost Internet connections to provide connectivity between their production sites and sales offices. They had several conflicting requirements:

- The production facilities were in developing countries where production costs are low, but the local infrastructure did not provide reliable Internet connections, or if it did, the connections were very expensive.
- The ERP system required low latency connections, MPLS connection with strict SLA, if possible
- The use of VoIP service wherever possible in order to save costs
- The network infrastructure (800 sites) should be centrally manageable by 2-3 persons

In many developing countries landlines are either non-existent or of very poor quality and reliability. However, there is a relatively good chance that the wireless infrastructure is in place. With StoneGate Augmented VPN, it is possible to use first for example, 3G wireless connections and add fast landline connections later on when they are ready. If the landline connections break up or are out of order then StoneGate Augmented VPN can automatically use the 3G connection as a backup.

MPLS connections are moderately priced when used within one country. If there is a need for MPLS connections globally then the pricing starts to rise sharply as the distance between the sites grows. In this case the ERP system needed low latency connection and the MPLS can provide it. Fortunately, the ERP system does not require much bandwidth, but Internet usage and VoIP calls do. The manufacturing company decided to use a very low bandwidth MPLS line for ERP traffic and directed all the other traffic to lower cost ADSL lines in order to keep global connections costs low. They were able to manage that using StoneGate Multi-Link VPN technology that seamlessly combined different ISP connections.



Managing 800 sites is not an easy task if you do not have centralized management. StoneGate Management Center provides a clear overview of the VPN infrastructure and allows centralized remote management for all VPN devices. Currently, the company is managing their 800 sites with 2 administrators.

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 technology solves this problem by adding fault tolerance and transparent fail-over to VPN tunnels.

Augmented VPN provides further cost savings by allowing companies to migrate from expensive leased line solutions to more cost effective ones. This migration is made simple by the fact that they can keep their current connections during the migration, and make the final transfer after they have tested the new lines and completed their setup process.

Security Bonus

Augmented VPN provides good security that is built-in to the solution. A high percentage of the traffic that flows through the Augmented VPN is security critical, so encryption is a must. Although MPLS connections are said to be secure, they are not encrypted. The traffic flows in clear text format inside the internet service provider's network. Often, augmented VPN is used to encrypt the MPLS traffic, to make sure that the traffic is not read by anybody else in the network.

Augmented VPN offers possibilities for traffic deep inspection, anti-virus, anti-spam, anti-spyware and, finally, anti-evasion checks. As the global forerunner in anti-evasion research, Stonesoft is able to provide unparalleled protection against Advanced Evasion Techniques (AET).



Artificial intelligence in Augmented VPN

Load balancing traffic between several different Internet Service Providers is not as easy as it sounds. Especially handling different problem situations gracefully can be challenging. Augmented VPN uses several cutting edge technologies, including fuzzy logic, to solve VPN load balancing and high availability issues.

Here are a couple of examples of problems that might occur if the load balancing or VPN resilience is not done correctly.

- Traffic goes to only one ISP link even though there are multiple active links available
- Traffic goes to a link of a poor quality even though a better link is available
- Traffic goes to a standby link even though an active link works
- Switching to a standby link takes too long

Fuzzy logic fits nicely to this kind of problems because it is multi-value logic. Instead of 0 or 1, there are multiple values. This means imprecise data and therefore fuzzy logic is required; it can use imprecise data and calculate “degrees of truth”, providing answers to question like:

- How high is the load
- How close to failover are we

Fuzzy logic uses input variables, fuzzy sets, output variable, rules and defuzzification in order to give an answer. Fuzzy logic helps the Augmented VPN to work optimally even in a very fast changing and unpredictable environment. In addition to fuzzy logic, the Augmented VPN uses Multi-Link technology that allows it to choose always the fastest Internet Service Provider line. For more information about Multi-Link technology, please read the whitepaper “StoneGate Multi-Link; Ensuring always-on connectivity with significant savings”.

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 that can be expected 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 used for router redundancy or for choosing the fastest route, are not required but can coexist in the network with 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 a routing technology that selects packet routes from all available ISPs.
- BGP can be configured to use static load sharing. . It does not perform true load balancing. For example, some statically configured networks always use link A and some other networks always use link B.
- 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 has not been designed for implementation by end users, so it requires specialized ISP resources and equipment. For instance, implementing BGP requires an provider independent IP address range (it is very difficult to get provider independent IPv4 addresses any more). This poses a significant risk of service failures which may lead to incorrect routing unless the end user successfully negotiates dedicated cooperation between competing ISPs. The implementation itself is a multi-step process with several activities that fall well beyond the normal bounds of software configuration. The implementation team must negotiate agreements between two ISPs, acquire and configure sophisticated hardware and routing schemes, and have 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 additional expense.

External Load Balancers

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

Limitations

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

Like with BGP, if the end user wants to implement load balancers, he 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 configuration of the gateway and the load balancing box is consistent, which adds to the technical complexity of the management process.

Conclusions

Augmented VPN provides a simple and cost effective way to create fast, secure, high capacity connections between sites and ensure uninterrupted Internet connectivity. Designed for ease of use, the implementation requires no special equipment, software or Internet service provider peering agreements. Multi-Link enables organizations to seamlessly integrate multiple network providers, creating fault tolerant and highly available connections without having to change their existing network infrastructure.

For a constantly available network, organizations usually rely on several Internet service providers or WAN (Wide Area Network) access points in order to ensure always-on connectivity and increase bandwidth while keeping a low TCO. With Stonesoft's Augmented VPN, the aggregation of all Internet Service Provider links is now possible. Link aggregation is a unique feature that enables organizations to combine different Internet service provider lines in order to obtain a single high capacity tunnel.

Studies show that employees are increasingly use applications that have been designed to be installed in a professional environment (Skype, MSN, Facebook...). This phenomenon also has a significant impact on bandwidth, which is often used for non-critical activities, and puts the quality of business applications and productivity of the organization at stake. Stonesoft's Augmented VPN enables the prioritization of network flows and the definition of bandwidth portions dedicated to different types of flows. Business applications can have priority on high quality Internet connections and the rest of the traffic can use more cost effective Internet connections.

A Virtual Private Network delivers the best return on the investment in securing communications. However, the lack of reliability of VPN links is risky for critical communication within organizations. The StoneGate Multi-Link Technology solves this problem by adding load balancing of VPN tunnels and fault tolerance due to automatic transparent failover to active or backup VPN.

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 the 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.

About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) is an innovative provider of integrated network security solutions to secure the information flow of distributed organizations. Stonesoft customers include enterprises with growing business needs requiring advanced network security and always-on business connectivity.

StoneGate™ secure connectivity solution unifies firewall, VPN, IPS and SSL VPN blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system. The key benefits of StoneGate secure connectivity solution include low TCO, excellent price-performance ratio and high ROI. The virtual StoneGate solution protects the network and ensures business continuity in both virtual and physical network environments.

StoneGate Management Center provides unified management for StoneGate Firewall with VPN, IPS, and SSL VPN. StoneGate Firewall and IPS work together to provide intelligent defence all over the enterprise network while StoneGate SSL VPN provides enhanced security for mobile and remote use.

Founded in 1990, Stonesoft Corporation is a global company with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com.



Stonesoft Corporation International Headquarters
Itälahdenkatu 22 A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
Network Security

Stonesoft Inc. Americas Headquarters
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131