



Whitepaper

---

# **The Secret to Simplified Firewall and VPN Security**

---

# Table of Contents

---

Executive Overview	1
Upgrading to Complexity	1
Firewall/VPN issues	1
Multi-homing issues	2
Upgrading to Simplicity	2
Conclusions	4

# Executive Overview

In today's world, more and more businesses are seeking to gain efficiencies in their resources. Forced to do more work with fewer people, organizations are looking for ways to improve the manageability and scalability of their networks without increasing their costs. At the same time, the business world demands unprecedented continuity; 24x7 Web services and back-end systems are a requirement in even the smallest enterprises.

"Business uptime is paramount, network security cannot become a business prevention function."

- anonymous CEO of a retail chain

In this white paper, we examine some of the issues surrounding the dilemma of managing these increasingly complex network systems with fewer and fewer resources. This paper addresses organizations looking to

- add high availability to their firewall and VPN (virtual private network) gateways,
- improve bandwidth and availability by multi-homing their ISPs, and
- find ways to reduce their structured costs at the same time.

"The complexity of securing my network is getting out of control."

- director of security and continuity, same retail chain

Any organization or service provider struggling with the increasing complexity of their existing solutions should review this paper for insights into simplifying firewall and VPN security.

## Upgrading to Complexity

Today's network environments frequently include a firewall and/or a VPN solution. Firewalls have become the established cornerstone of perimeter security defenses for any corporate network. The 2003 FBI/CSI Survey reports that 98 percent of businesses have firewalls in place. Yet firewalls begin layering complexity onto the network infrastructure.

### Firewall/VPN issues

Firewalls can be a single point of failure. Whether software-based, or appliance, if the firewall fails for any reason, network connectivity is interrupted. For many organizations, an interruption of even a minute or two can mean millions in lost revenue. Firewalls require maintenance as well. Software-based solutions require the administrator to maintain the operating system level patches to keep current with operating system vulnerabilities, plus maintain the patches on the firewall software itself. Appliances, though not faced with the same layered approach as software, require expensive, proprietary upgrade components to achieve even a modicum of scalability.

"Patching security holes and vulnerabilities has become a full-time job for many IT shops."

- Keith Ferrell, tech Web

VPN gateways face similar complexity challenges. They too, require complex patch management. VPNs also require aggressively negotiated and more expensive service level agreements (SLAs) with the network provider or ISP to ensure reliability. Organizations not wanting to rely on the ISP often spend even more money on dedicated leased lines (or frame relay networks) to ensure the VPN reliability they need. Though the cost of the loss of an ISP for a few minutes may seem high, the loss of a VPN for many organizations can be exponentially higher.

Both firewalls and VPNs can be made highly available in different ways, depending on the vendor's approach. Software-based solutions can be made redundant with the addition of clustering softwa-

re. This allows for a basic hot-standby configuration, or a more robust active-active cluster. Some go so far as to load balance across multiple nodes. Hardware appliances often tend to be more simplistic in their high availability options. They offer basic hot standby or a basic active-active system only.

But beyond the cost factors, clustering solutions for firewalls and VPNs add even more complexity. For software-based solutions, the administrator now needs to have the time to upgrade and maintain the patches on the operating system. Then they need to keep up with upgrades and patches for the firewall/VPN software as well. On top of that, they need to maintain the clustering solution. This maintenance means more than just upgrading, maintaining and patching the clustering software and verifying its functionality. It also means that all of the other patch work and maintenance of the operating system and the firewall/VPN software need to be carried out two or more times - once for each node in the cluster.

For many administrators, this complexity means hours and hours of maintenance work. A minor version upgrade of the firewall/VPN software can take up to a week (or more) to implement, in addition to the time it takes to stage and test it in a lab beforehand.

## Multi-homing issues

The complexity battle doesn't end at the firewall/VPN gateway itself. Achieving availability at the gateway is insufficient if the Internet provider (ISP) fails. Thus, many enterprises have implemented, or are looking to implement, solutions to manage multiple network providers. Such multihoming is traditionally accomplished by BGP (Border Gateway Protocol), a routing protocol designed to allow for 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 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.

"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)

"Companies have avoided multi-homing (connecting to multiple ISPs, generally for redundancy) because of the challenges of implementing Border Gateway Protocol (BGP)."

- Johna Till Johnsson, Network World

Were the issue of the ISP multi-homing just in the redundancy of the ISPs, it might not seem complex. But there is also the issue of load balancing traffic to the servers behind the firewall. This requires still other clustering software or the addition of hardware load balancers in the demilitarized zone or DMZ network where the Web or application servers reside. Often, such load balancers or clustering solutions are from yet another vendor. The multiple vendors now required (for the operating system, the different Internet providers, the firewall software, the VPN solution, the high availability software, and the load balancers) add costs in administrative time [each system has its own commands, user interface, and set of metaphors and ways of doing things], add complexity [ensuring that all components are patched, configured and working properly], and add costs [in administrative skill sets/training, maintenance and support contracts, and service level agreements].

"Using StoneGate with dual broadband connections saves us \$300.00 per month per location."

- Charles Smith, MIS Director Plaza Construction Corporation

# Upgrading to Simplicity

There is another approach to the whole multi-vendor complexity issues surrounding the firewall/VPN security components. Though many organizations tend to overlook it by focusing on the details of each piece, it is possible to achieve a manageable, scalable firewall and VPN security solution that includes high availability, clustering, multi-homing and server load balancing without the incredibly complex nature of upgrading piecemeal systems and adding even more components.

Stonesoft's StoneGate High Availability Firewall and Multi-Link VPN solution represents a new, more simplified approach to network security, while also providing the defense agility and business continuity assurance that organizations require. By replacing the cornerstone of the network firewall with StoneGate, organizations can immediately reap the benefits of all of the above features, without having the additional complexity.

StoneGate is designed to resolve the complexity problems plaguing most medium and large enterprises and service providers. It provides an integrated operating system that reduces patch management and upgrade headaches for system administrators. Upgrades that could take a week or more now only take a few minutes to an hour or two. StoneGate also includes remote upgrade capabilities, and an upgrade version replaces the firewall/VPN, operating system, drivers, high availability and multi-homing components at once.

But StoneGate goes beyond simplified upgrades. It also includes multi-homing as part of the firewall/VPN solution, negating the need to peer BGP with multiple, competing providers. It takes minutes to setup, and does not require the upgrading of border routers. StoneGate always chooses the fastest path through the available providers, and it can even failover the VPN links in the event of an ISP failure.

VPN multi-homing helps to reduce structured costs and complexity. By providing VPN failover through multiple ISPs, leased lines or frame relay costs are no longer necessary. Inexpensive business DSL lines can replace the costly private lines, while still maintaining the security and reliability required.

StoneGate, having reduced the costs of operating system licenses, firewall/VPN software, clustering technologies, BGP and its associated costs, and external hardware load balancers, also reduces costs in other areas. Support and maintenance costs can be reduced, as the solution requires support and maintenance from fewer vendors. StoneGate reduces administrative costs as well. Tasks that took administrators days or even weeks, now take only minutes or hours. Because clustering and load balancing are built in, an administrator can upgrade a firewall or VPN gateway in a few minutes. This can occur during the day, while the system is up and running and in use. If the system encounters a problem while the upgrade is being carried out, traffic can be transparently failed over to the remaining active nodes in the cluster.

Another example of simplified administration with StoneGate is its unique Drop-In Firewall Clustering (DFC) technology that neatly sidesteps the configuration difficulties typically encountered when setting up a firewall cluster. DFC enables administrators to effectively "drop" a firewall cluster into their existing network infrastructure.

StoneGate also includes a centralized management system. This system creates a central repository of log and system data and monitoring of all firewall/VPN gateways across the enterprise, regardless of their location. Although centralized, the GUI client enables multiple administrators to upgrade, manage and monitor the systems simultaneously from multiple locations. StoneGate's reduced costs and easier administration support a lower total cost of ownership (TCO) and improved return on investment (ROI) for firewall and VPN investments.

"StoneGate centralizes control/access, load balancing and VPN functions. We also like the graphical user interface and the ease with which we can upgrade to new releases."  
- Carlos Quesada Diaz, IT Department, Banco Zaragozano, S.A.

"Current solutions for clustered or load balanced firewalls require coordination between network and security operations groups. In the future, solutions that provide improved operational efficiencies for deployment, management and resource utilization will be well positioned in the marketplace."  
- Mark Fabbi, Gartner Vice President

"StoneGate not only offers excellent performance but is the most cost-effective as it combines the operating system, the firewall and load-balancing all in one package."  
- Director of Organization/IT, Hamburg Sud

# Conclusions

To ensure advanced security and business continuity, many organizations are faced with the dilemma of upgrading to complexity. Small and medium enterprises, large enterprises and service providers alike are working to upgrade their existing firewall/VPN cornerstones to the latest practices in high availability, and also attempting to improve scalability, while keeping tight budgets in mind. At the same time, administrators are forever spending their time maintaining and patching these systems instead of planning for the future, as more and more organizations are forced to do more with less.

“StoneGate is positioned to change the way large organizations look at high availability and network security.”

- Chris Christiansen, Vice President, Internet Security Software, IDC

Stonesoft's StoneGate firewall and VPN offers an alternative approach to this upgrade complexity. Instead of upgrading and adding on to existing solutions, it can be better to step back and replace the cornerstone instead, in order to build on a more reliable foundation that is designed for the manageability, availability and scalability required by the modern enterprise. Administrators can have real world business security, while also having the time to look to the future and work on other problems instead of having to maintain the existing house of cards. Organizations can save money and experience a lower TCO by making an investment in the right upgrade path - the one to simplicity. Because at the end of the day, isn't it better to manage the security policies rather than security technology?

## 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

Copyright 2006 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.