



Whitepaper

StoneGate: Balancing Security and Business Continuity

Table of Contents

Executive Overview	1
Navigating the Multi-Vendor Security Maze	1
Firewalls	1
VPNs	2
Clusters	2
Bringing It All Together	2
StoneGate: Eliminating the Multi-Vendor Maze	3
StoneGate Firewall	3
StoneGate Multi-Link	3
StoneGate VPN	4
StoneGate Clustering and Load Balancing	4
StoneGate Management System	4
Benefits of StoneGate's Total Network	5
Manage Multiple ISPs as a Single Connection	5
Scalable VPNs	5
True High Availability	5
Pushing the Envelope	5
Lower Hardware Costs	5
Reduced Management and Maintenance Time	5
Lower Cost of Deployment	5
Lower Cost of Communication	6
Reduced Downtime	6
Conclusions	6

Executive Overview

For most organizations today, reliance on the Internet for communications with customers, partners, and remote locations is a business necessity. Web-based applications that extend business across the Internet depend on secure and reliable access by authorized users. This generates a tremendous IT challenge regarding “network confidence”—the responsibility to make private network resources both continuously available to authorized users and protected from unauthorized access. The quest for network confidence requires a balancing act between security and availability that must be managed at the point where the private network meets the public Internet.

IT managers working toward total confidence in their networks typically configure and manage several technologies from multiple vendors to meet their communications requirements: firewalls for intrusion prevention, VPNs for secure communications links, and clustering solutions for high availability and load balancing. Any combination of these solutions will typically emphasize security or network performance, but not both. Regardless of the balance achieved, keeping those solutions working is a tremendous IT challenge. Sourcing from multiple vendors represents significant technology risk in terms of procurement, systems integration, life cycle management and cost, version control and interoperability. Reliance on a singular Internet connection represents a potential bottleneck and point of failure, and causes tremendous concern for the security and reliability of business-critical Web applications.

This paper surveys the network confidence issues facing IT managers, and provides an overview of StoneGate™, the combined firewall security and network availability solution from Stonesoft Corporation. By simultaneously protecting business-critical systems from intrusion, single-point failure and connectivity collapse, StoneGate provides a new level of network security and confidence to distributed enterprises and service providers.

Navigating the Multi-Vendor Security Maze

Network, security, and communications equipment vendors typically view Internet connections as either an opportunity to protect business-critical resources, or an opportunity to extend business-critical resources, but not as an opportunity for both. As a result, IT managers seeking a balance between security and continuous Internet accessibility must evaluate individual components with an eye toward piecing together a meaningfully interrelated system of solutions. Each part of that solution—firewall, VPN and cluster—introduces issues that must be considered in light of the overall solution.

Firewalls

Firewalls typically provide security at the point where the Internet connects to the corporate network, and are often the cornerstone to the enterprise security infrastructure. However, most contemporary firewalls may represent single points of network and Internet connectivity failure because they do not include load balancing and fault tolerance at the firewall or the ISP connection. They may also represent performance bottlenecks because they have not been designed for today’s Web traffic volumes. Firewalls typically provide security using one of the following technologies:

- Stateful connection tracking and packet filtering, in which dynamic packet filters open and close firewall “doors” based on packet header information. Once a packet stream passes through to its destination, the firewall door closes. This technique, which is the most popular

for Internet firewalls, offers high throughput and low overhead but allows direct IP connections to the internal network, which enables hackers to exploit application-level attack techniques to intrude on the protected network.

- Application-level proxy security, which addresses the shortcomings of stateful connection by eliminating direct access to services on the internal network. Internet firewalls based on this approach are very secure, but provide poor throughput performance because application-level proxying is CPU-intensive. This emphasis of security over performance and availability solves the security problem, but creates another because corporate Internet connections require performance and “always on” availability.

Traditional firewalls, using either security technology, typically run on a range of off-the-shelf operating systems, including Microsoft® Windows® and such Unix-based systems as Linux® and Solaris™. These operating systems offer far greater capabilities than firewalls require, which poses a potential problem; the presence of a standard operating system on a fire-wall creates opportunities for attack by enabling intruders to compromise the firewall through the underlying operating system.

VPNs

WANs (wide area networks) have long been used to extend access to remote locations via private, leased line connections that, while expensive, provide high grades of service and service level agreements. The Internet has opened up new communications opportunities, with IP-based VPNs (virtual private networks) using the Internet as a more cost-effective transport than leased lines. VPNs are often integrated into firewalls to provide security at the VPN termination point.

IP-based VPNs extend a network’s perimeter into and through the public Internet, by providing encrypted and secured point-to-point data communications pipelines. Ongoing concerns about operational reliability and actual costs of VPN implementation have significantly hampered adoption, and leased lines continue to provide the most popular means for wide area communications and VPNs.

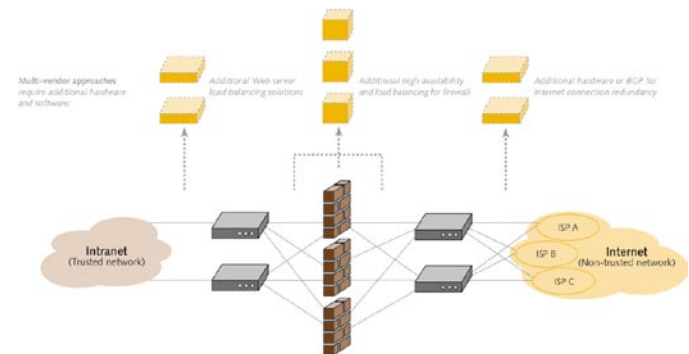


FIGURE 1. Traditional approaches require independent, multi-vendor systems

Clusters

High availability, load balanced clusters introduce redundancy to firewalls, Web servers and other server resources, removing them as possible single points of failure in a network. Dynamic load balancing allows effective utilization of computing resources by balancing traffic load among firewall nodes and/or clustered servers for maximized throughput and fault tolerance. If a firewall node or server goes down, failover and redistribution of traffic to operational resources within the cluster takes place transparently—and connections are never lost, thereby improving customer satisfaction and internal efficiency. The biggest challenge in deploying these combined, multi-vendor clustering and security solutions is their integration and management. Another practical challenge is seamless failover when a component fails, which ideally ensures that all concurrent connections through the firewall or VPN remain operational so that users receive a consistently high quality experience.

Bringing It All Together

Firewalls, VPNs and clustering solutions, as well as the underlying operating systems, each typically represent a discrete solution. Because they all must be sourced, deployed, operated, managed

and supported independently, there is a significant challenge to making them work in an integrated fashion. Network managers responsible for an organization's secure Internet connection can attest to the mix of planned maintenance outages, as well as unplanned outages and loss of connectivity, that inevitably compromise total network confidence. For service providers, such compromises in network confidence have a dramatic impact on customer satisfaction.

These are the reasons Stonesoft created StoneGate. It provides total network confidence to distributed enterprises and service providers by simultaneously protecting business-critical systems from intrusion, single-point failure and connectivity collapse.

StoneGate: Eliminating the Multi-Vendor Maze

StoneGate addresses the inherent technology risks associated with separately sourced security and high availability solutions. A fully integrated security-availability solution, StoneGate combines several network elements including firewall, VPN, load balancing and high availability clustering in a single software product, all administered under a single interface for simplified configuration and management. Together, StoneGate's components represent an immediate path to total network confidence by providing the highest level of security, performance, and scaling required for organizations with growing Internet dependence and traffic volume. Additionally, the unique capabilities provided by Stonesoft's patent-pending Multi-Link TechnologySM eliminates Internet connectivity as a single point of failure.

For more information on multi-layer inspection, please refer to the Multi-Layer Inspection white paper, available from Stonesoft.

StoneGate Firewall

The firewall engine built into StoneGate is based on Stonesoft's patent-pending Multi-Layer InspectionSM technology, which combines the benefits of both stateful inspection and application-level proxy technologies. Unlike other firewalls, it provides a scalable three-level security environment that is flexible and extensible. Multi-layer inspection includes: packet filtering in selected instances where stateful connection tracking is not practical, stateful connection tracking when appropriate, and application-level security through protocol agents, which provide the security of application-level proxies, but are modular and flexible. In combination and according to administrator-configured rule bases, StoneGate offers the flexibility and high-performance environment with which to manage three levels of security in way that is appropriate to specific Internet traffic and protocols. In addition, StoneGate runs on a hardened Linux operating system integrated directly into StoneGate, minimizing the security threats caused by loopholes in operating system configuration.

For more information on multi-link technology, please refer to the Multi-Link Technology white paper, available from Stonesoft.

StoneGate Multi-Link

Especially important to StoneGate's total network confidence is the unique multi-link technology, which can connect a single firewall cluster to multiple network providers. Multi-link also provides load balancing, fault tolerance and failover across all connected networks, eliminating the single point of failure that can arise when a network is connected to a single provider. This unique capability also provides for a very real increase in available bandwidth between the private network and the Internet. StoneGate can dynamically select the best connection, and allows for incrementally increased bandwidth by adding new Internet connections from additional ISPs and managing them as a single virtual Internet connection.

StoneGate VPN

StoneGate's VPN security is based on the IPsec standard, but takes VPN connectivity and reliability to an entirely new level with the built-in multi-link technology. It uses multiple network links of varied performance and technology, load balances routing, and provides for failover between VPNs and VPN clusters. Multi-link constantly monitors subtunnels across the multiple network links, and can move VPN traffic from one to another for optimal performance. The result is that VPN connectivity can be retained with only a single functional subunnel. To increase performance, StoneGate dynamically monitors the availability and throughput of the network providers and always directs traffic to the available provider with the highest throughput.

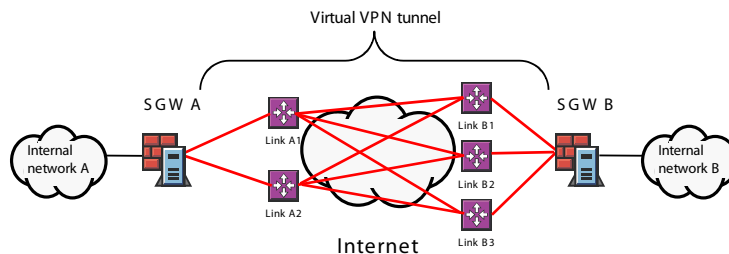


FIGURE 2. StoneGate multi-link VPN technology

StoneGate Clustering and Load Balancing

StoneGate provides high availability and load balancing among firewall nodes for maximized throughput and fault tolerance. Based on Stonesoft's industry-leading StoneBeat® technology, which is currently used in more than 5,000 installations, StoneGate's clustering solution is designed to eliminate single points of failure. If a firewall/VPN node or server fails, the other nodes or servers in the cluster automatically and transparently take over its tasks without affecting established connections. StoneGate extends typical firewall and VPN high availability solutions to include fault tolerance for multiple network providers, as well as load balancing to back-end data and application servers. StoneGate's clustering capability provides a scalable infrastructure that easily adds new firewalls or servers, and allows for non-disruptive maintenance. A firewall node or server can be taken offline for upgrading or reconfiguration without disrupting Internet access or VPN traffic, and without bringing down a hosted application. This means that maintenance can be performed whenever it's convenient—eliminating the need for emergency fixes or off-hour maintenance scheduling.

StoneGate Management System

StoneGate is designed as an integrated solution, with components that are all managed via a centralized, enterprise-wide management system that eliminates the burden normally associated with multiple firewalls. The StoneGate management system controls the operating system on each firewall host; there is no need to operate the firewalls themselves after the initial setup. The management system provides an extensive suite of management tools, including rule base templates, inheritance, sub-rule bases, multiple administrator levels, extensive log filtering and pruning, and hierarchical management levels and hierarchical policies. This greatly simplifies administration of all StoneGate's capabilities.

By integrating components and centrally managing their capabilities, StoneGate succeeds in eliminating the multi-vendor maze that has marked attempts to ensure total network confidence to date. StoneGate provides an optimum balance of security, performance and high availability. All components are created by and sourced from a single vendor, deployed and operated as a single software solution, managed through a single comprehensive interface and supported by a single customer care organization.

Benefits of StoneGate's Total Network Confidence

StoneGate also makes it possible for IT managers to conveniently and economically meet the total network confidence challenge with benefits and capabilities that would otherwise have been unthinkable, thanks to the addition of multi-link technology.

Manage Multiple ISPs as a Single Connection

By extending a private network connection to multiple ISPs and managing that connection as if it were a single connection, StoneGate provides distributed organizations and service providers with far greater security and availability than would be possible through any combination of separately sourced components anywhere.

Scalable VPNs

For distributed organizations, StoneGate means the ability to extend business-critical resources to all organization segments, with the highest degree of availability and security. VPNs can be effectively extended worldwide, with the public Internet replacing expensive leased lines as a thoroughly secure means of transmission.

True High Availability

For e-businesses, StoneGate ensures that customer transactions continue as normal, suppliers stay connected, and information keeps flowing regardless of any single point of failure due to planned or unplanned maintenance, equipment loss, targeted attack, system overload or excessive peak traffic.

Pushing the Envelope

Service providers realize the benefits StoneGate provides to distributed organizations and e-businesses while serving as a significant new business enabler. Through its ability to provide access assurance resulting in total network confidence, StoneGate propels new and differentiated grades of service (GoS) and lucrative service level agreements (SLAs), paving the way for higher margin service offerings and for more widespread deployment of secure IP services, such as VPNs and voice over the Internet.

In all cases, StoneGate provides significant cost reduction on a number of important fronts.

Lower Hardware Costs

Rather than requiring proprietary or high-end hardware for operation, StoneGate can provide enterprise-level throughput even on cost-effective, off-the-shelf Intel® or UltraSPARC™ platforms.

Reduced Management and Maintenance Time

StoneGate effectively eliminates the need for network administrators to deal directly with firewall administration. It reduces and simplifies management, while enabling maintenance during business hours.

Lower Cost of Deployment

StoneGate eliminates the need for separate high availability, load balancing, VPN and firewall solutions, which translates directly to a reduction in hardware, software, rack space and operating cost.

Lower Cost of Communications

With the new level of confidence StoneGate brings to IP connections, StoneGate makes it much easier to replace traditional, expensive leased lines with IP-based connections. Multi-link can even provide the capability to test and bring up new ISP connections as demand dictates, or as attractive pricing becomes available, without threatening connectivity.

Reduced Downtime

For many organizations, the ultimate benefit of StoneGate is that it brings the same kind of continuous performance and connectivity to the Internet that we have come to expect from electric and voice utilities.

Conclusions

Managing both security and availability is a balancing act that often forces organizations to choose between high availability and security in the quest for network confidence. The delicate security–availability balance is best managed at the point where the private network meets the public Internet, where IT managers have had to select and integrate individual firewall, VPN and clustering components from multiple vendors. This process carries tremendous technology risk in terms of procurement, systems integration, life cycle management, cost control, version control and interoperability.

StoneGate effectively eliminates the need to navigate a multi-vendor maze, and represents the industry's first integrated solution for balanced security and availability. By interrelating the firewall, VPN, high availability and load balancing functions—and adding the unique multi-link capability of orchestrating communications via multiple ISPs—StoneGate enables IT managers to meet one of the biggest challenges facing businesses: protecting business-critical resources while making them readily accessible, without sacrificing performance.

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

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.