STONESOFT

Whitepaper

Next Generation Availability & Scalability

The Role it Will Play in Economic Recovery

Table of Contents

Executive Summary

Network availability and performance have always been critical to enterprise performance – but never as important as it is today. As companies emerge from a recessionary economic climate, they are under increased pressure to meet growing network and business demands with exceptionally lean resources. At the same time, these companies are fighting for business and can't risk the negative impact of a down network or a network that can't keep pace with growing business demands. Regardless of the size and type of company, the cost of downtime can be devastating.

Whether a result of Internet link downtime, organized security attacks, natural disasters or human error, a down or under-performing network generates long-term brand damage, low customer satisfaction and lost revenue. For companies trying to emerge from the recession ahead of the game, this can single-handedly change the outcome.

As the dependencies on the network are increasing, so are the costs and complexities of network connectivity and network infrastructures. The more complex the network, the more difficult it is to manage and the more prone it is to downtime. According to Gartner, complexity is the biggest threat to network security. Gartner also reports an alarming fact related to the source of downtime – a whopping 99 percent of all security breaches are caused by misconfigured network devices and appliances.* In addition, maintaining connectivity to meet compliance requirements has never been more important than it is today. As a result, many IT leaders are looking for new ways to cost-effectively ensure high availability and scalability without jeopardizing profits or compliance.

Recently, a new approach has made its way into forward-thinking organizations that are discovering how to significantly reduce the costs, complexities and downtime risks. This approach is called next generation availability and scalability.

This approach, to be discussed further in this paper, goes far beyond system redundancy and load balancing. It encompasses high availability technologies "built in" to network security solutions. This approach eliminates additional "bolt-on" solutions and added costs typically required to achieve the level of network performance needed in today's environments.

*Young, Pescatore, Greg, John (2008, August 12). Q&A: Is It More Secure to Use Firewalls from Two Different Vendors, G00146091, Inclusive – 3. Retrieved August 12, 2008, from Gartner.

Network Connectivity – The Roadblocks

"Reliability is always at the top of the list regardless of product category or customer type, because organizations of all sizes and shapes are becoming more and more dependent on reliable connections between their customers, business partners and employees."

- Infonetics User Plans for Security Products and Services Study

In today's 24x7x365 world, virtually every type and size of organization depends on constant network connectivity. According to Infonetics, organizations are losing as much as 2.2 percent of their annual revenue due to downtime. Whether it's internally among employees or externally with customers and partners, organizations expect to be connected anytime, anywhere – in fact, their business models often depend upon this very notion.

However, ensuring this dependable connectivity is becoming increasingly difficult. To understand these issues, let's review the changes and pressures that IT departments are facing:

- **Economic pressures to cut costs:** IT leaders have always been faced with the challenges of doing more with less – less staff, less budget and fewer resources – but the pressures have been further magnified in today's uncertain economic climate.

- **Network sprawl:** For many years, mission-critical applications resided on mainframes in a data center. The move in the 1980s to distributed computing environments took many critical systems off the monolithic, yet reliable mainframe and placed them on less reliable hardware. To compensate for outages, redundancy became a standard in network architectures. Disks, network equipment, processors, network cards and even the servers themselves were doubled up to ensure that a failure would simply transfer the work to backup systems resulting in network sprawl. The result? Today's network infrastructure is complex, costly and lacking in agility.

- **Increasing Web-based applications:** Over time, software applications have become increasingly Web-based. Web 2.0 technologies are being deployed to enable employees, customers, partners, contractors and consultants to be more productive. The implementation of these technologies continues to fuel organizations' dependence on the Internet. At the same time, many organizations have discovered that even dedicated lines, such as Frame Relay circuits, private T1s, and Multiprotocol Label Switching (MPLS) networks, are not immune to outages. Anything unexpected, from the more mundane "fiber seeking" backhoe at a nearby construction site, to a natural disaster can disrupt connectivity.

- **More stringent compliance requirements:** With an increased focus on regulatory requirements, auditors are looking for these controls to ensure an organization's compliance with Sarbanes-Oxley, the Payment Card Industry Data Security Standard (PCI-DSS), Federal Information Security Management Act (FISMA), DoD Information Assurance Certification and Accreditation Process (DIACAP) and other requirements. If an outage occurs in the systems that support the business processes and workflows, the risk of non-compliance issues and fines increases dramatically.

- **Truly distributed networks:** With the evolution of the mobile workforce, remote users can access networks from literally anywhere in the world. Organizations are challenged with managing not only their headquarters, but also scaling out to semi-trusted locations, such as branch offices, and to even less-trusted networks for remote and mobile users. Each new network layer has unique connectivity challenges, adding more costs and complexity.

- **Demands for new technologies:** Today's organizations are deploying new technologies, like voice over IP (VoIP) and video conferencing, as a way to gain operational efficiency and competitive advantage. However, making sure that current networks can scale to meet the new bandwidth demands and ensure quality of service presents a whole new set of issues for IT departments.

- **Virtualization risks:** A recent Gartner survey reported that approximately 40 percent of virtualization deployment projects were undertaken without involving the information security team in the initial architecture and planning stages. Typically, the operations team will argue that nothing has really changed – they already have the skills and processes to secure workloads, operation systems and the hardware underneath. While true, this argument ignores the security threats and potential downtime when there's an attack to the new layer of software in the form of a hypervisor and virtual machine in these virtual networks. Unfortunately most products don't have built-in high availability needed ensure that virtual networks never go down.

The result? IT leaders are struggling to maintain complex, redundant and costly networks. Furthermore, they are seeking new ways to trim costs in equipment, communications and resources and still ensure the highest levels of connectivity.

A Better Approach

What companies need today is network technology that features built-in network availability and scalability technology. Rather than add to network complexity by purchasing separate solutions to achieve this functionality – not to mention the added costs of managing them – companies should source solutions that simplify the network while boosting overall performance.

When evaluating different options to optimize their networks and save costs, organizations should consider the following key points:

- **Built-in versus bolt-on functionality:** Taking a close look at specific functionality and asking some basic questions will help uncover which solutions deliver the built-in functionality you need to ensure connectivity. For example:
  - How is continuous uptime achieved? In most cases, you need to purchase another set of expensive redundant systems.
  - Does the solution offer instantaneous, transparent failover or is your network at risk of going down for hours?
  - Can the solution cluster up to 16 nodes so you can easily scale and increase the performance of your network? Most products can only cluster up to two or four nodes.
  - Does the solution offer active-active load balancing? Most solutions only offer active/passive functionality so you don't get the full benefits optimizing traffic to accommodate current and future network requirements.

- **Flexibility and scalability:** The ability to choose the technologies that fit your environment and budget and still ensure the highest level of connectivity and security is critically important. A few key questions to consider include:
  - Can your company leverage any variety of connections from MPLS to cable modems – and have the confidence of continuous uptime?
  - Can your current technologies easily scale to accommodate growth, remote networking and the latest technologies?

- **Manageability:** Efficiently managing all of the components impacting connectivity from a single console is a critical component to any organization's ability to ensure continuous connectivity. A few key questions to ask include:
  - Can you manage virtual, physical and third-party devices all from a single management console? This is key in being able to detect, address and remedy security threats that threaten network availability and performance.
  - Can your administrators efficiently manage your network across multiple systems? Most products hardly provide visibility into networks, let alone the tools administrators need to easily manage both physical and or virtual environments.
  - Can deployments be done with minimal or no interruptions? In most cases architecture and configuration changes must be done off-hours to minimize the impact on operations.

Conclusion

Network complexity has clearly made network costs and security a significant concern – especially as businesses recover from the economic woes of the last 18 months. However, as companies try to reduce network costs and boost security, they must put equal focus on network availability and scalability. A down network could very well be the costliest threat.

About Stonesoft

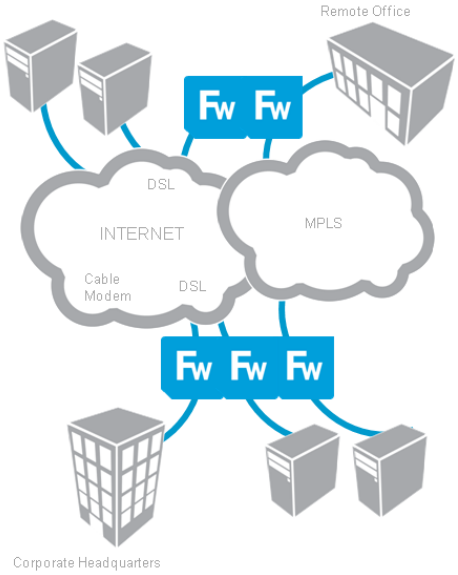
Stonesoft Corporation (NASDAQ OMX: SFT1V) delivers proven, innovative solutions that simplify network security management for even the most complex network environments. The StoneGate Platform unifies management of entire networks—including StoneGate and third-party devices—blending integrated threat management, end-to-end high availability and network optimization into a centrally controlled system. As a result, Stonesoft provides the highest levels of proactive control, always-on connectivity and compliance at the lowest total cost of ownership (TCO) on the market today. Founded in 1990, the company is an established leader in network security innovation with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com and http://stoneblog.stonesoft.com.

StoneGate Next Generation Availability & Scalability

Stonesoft maintains a rich history in integrating high availability and scalability functionality into its network security solutions. In fact, it's a fundamental part of what sets the StoneGate solutions apart from others in the marketplace. Unlike other vendors, Stonesoft uses a "built-in" approach to optimizing network availability, scalability and cost efficiencies. The company's patented high availability technologies are built into all of its solutions, thereby eliminating the need to purchase additional bolt-on solutions.

The elimination of additional network purchases isn't the only efficiency achieved through Stonesoft's unique approach. Stonesoft's one-of-a-kind technologies and clustering mechanisms translate into zero downtime for today's networks. In other words, the network never fails on Stonesoft's watch – and there is never a need to take the system down for maintenance.

Through higher productivity, simplified management and reduced costs, Stonesoft is transforming the way organizations secure their networks. The StoneGate family of virtual and physical network security solutions includes the following built-in technologies – each of which are redefining the standard for high availability and scalability:



- **Multi-Link™ Communications:** Stonesoft's patented Multi-Link technology eliminates network links as single points of failure, by providing seamless VPN failover across multiple circuits. Regardless of the type of connections needed – DSL, leased lines, cable modems and even satellite – Multi-Link can load balance an unlimited number of circuits through a single appliance to ensure high availability, superior active/active performance, and optimization for VoIP and other emerging technologies. When multiple circuits are required for redundancy, Multi-Link also eliminates the cost and administration of BGP routers.

- **Drop-in Active Clustering:** Enables the unique clustering of up to 16 devices so organizations are assured the highest availability and scalability from the core to the edge of their networks without the need for expensive standby systems. With drop-in technology, clusters can be easily added into existing infrastructures without complex configuration requirements. When a three-node cluster is configured with a Multi-Link dual circuit, a Five 9's nearly fault-tolerant network can be achieved.

- **Dynamic Server Load Balancing:** Distributes traffic between servers to balance the load efficiently and ensure that services are available when needed. User connections can be intelligently redistributed across server pools based on server availability. When configured with a two-node or three-node firewall cluster, maintenance can be done as needed during business hours with no down time.

- **IPS Clustering:** Ensures that IPS systems protecting internal systems never go down. With the unique ability to cluster StoneGate IPS in a serial or parallel configuration, organizations can be assured that if one IPS sensor should fail, the other IPS sensors in the configuration will automatically take over and monitor the traffic to keep the information flowing securely. With each IPS added to the cluster, throughput performance increases significantly to ensure scalability for expanding organizations.

- **StoneGate Management Center High Availability:** Enables up to four standby management centers and real-time replication of repository data in the event of downtime so network monitoring never stops.

- **SSL VPN Gateway Redundancy:** Provides clustering of two SSL VPN appliances to form a mirrored access-point pair to ensure that even remote mobile connections never go down.

- **Mobile (IPsec) VPN Gateway Redundancy:** Provides clustering of multiple links to ensure mobile VPN connections are continuously available.

STONESOFT

www.stonesoft.com

Stonesoft Corporation
International Headquarters

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
tel. +358 9 4767 11
fax. +358 9 4767 1234

Stonesoft Inc.
Americas Headquarters

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