

STONESOFT

Whitepaper

Enterprise Availability for Mid-Size Businesses - Managing In-Depth Network Security and Availability

Table of Contents

| | |
|---|---|
| Executive Overview | 1 |
| Who Needs Horizontal Integration? | 2 |
| IT Manager's Challenge | 3 |
| Benefits of A Unified Management Platform | 4 |
| Conclusions | 6 |

Executive Overview

- Enterprises of all sizes must be able to ensure that their networks are both secure and open for business.
- Mid-market enterprises lack the resources for enterprise-grade solutions that address both needs.

While the dot com bubble has burst, the Internet remains a de facto communications medium. But along with the viability of the Internet comes a new era of security threats that many mid-sized enterprises find themselves ill equipped to manage. Most organizations made their last major updates to IT infrastructures and systems to manage Y2K-related issues, long before the proliferation of today's increasingly sophisticated and more complex Internet-based attacks. From a security perspective, much has changed since Y2K, and as a result organizations are being pushed hard to keep up.

But perhaps an even greater challenge is how to ensure continuity and high availability for Internet communications, especially as organizations become increasingly dependent on the Internet for conducting business. CIOs of large enterprises are all too aware that they are expected to do more than secure their networks. They are also expected to keep their networks open for business. These issues are now appearing on the radar screen of IT managers of mid-sized organizations.

Companies of all sizes that require both security and network uptime are challenged by the increasing management complexity. Larger enterprises, however, have the resources and dedicated network specialists to maintain communication continuity as a separate function from network security. Smaller organizations usually do not have this option, and continue with limited resources and budgets for managing real-time communication needs.

The current security trend is to package and integrate multiple functions together, from network security tools such as firewalls and VPNs, to content security tools such as anti-spam and URL filters. This vertical integration between point security products may help from an administrative point of view; however, even greater benefits can be gained if cross-functional, horizontal integration is taken first. For example, by converging solutions for perimeter security and continuous business assurance technologies, these requirements become easier to manage for a single administrator or small IT staff responsible for both.

This paper addresses the challenges facing mid-sized enterprises in managing both security and network continuity, and how an integrated approach can save in both communication and operational costs. With continuous uptime, these organizations have the real-time capabilities that the market demands, allowing them to compete effectively against larger enterprises. The original Internet promise of leveling the playing field for companies of all sizes is still possible, providing that companies have the right tools.

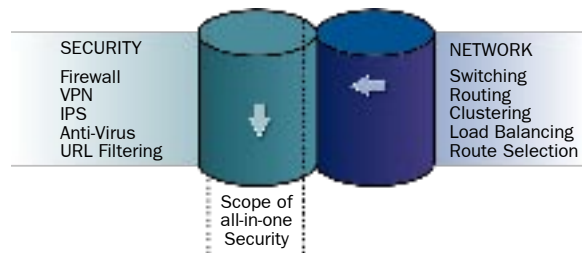
Who Needs Horizontal Integration?

- Security platforms are replacing point security solutions, but the levels of integration vary.
- Even more valuable synergies can be achieved through the convergence of network security and network availability assurance functions.

In the early nineties, IT security was minimal. Viruses were spread primarily through the use of at the network perimeter and other locations. Through all of this, security has been applied as an afterthought to the established IT architecture. The common practice has been to deploy "best of breed" point security solutions as needed, adding new ones as other threats emerge. Toward this end, enterprises have moved beyond network security to content security, adding solutions such as URL filtering and e-mail spam protection.

Compared to the networking side, where organizations have typically relied on a single vendor, the result is numerous point security solutions that must be separately installed and managed. To address this issue, security vendors are now introducing security “platforms” that unite multiple point solutions under a single umbrella. The idea is that by integrating several of these vertical products into a single vendor offering, the manageability, patching, support and maintenance will be simplified.

Currently, the level of integration between each platform’s components varies by vendor. In certain instances, especially in cases where security platforms are built via technology acquisitions, vendors are simply throwing a management “blanket” over the various point products and using APIs to establish translation. In this manner, they are essentially feeding coins into a parking meter until tighter and more beneficial integration can be established over time. Often, reaching the desired level of integration is turning out to be more challenging than realized, and as a result many more coins are being required.



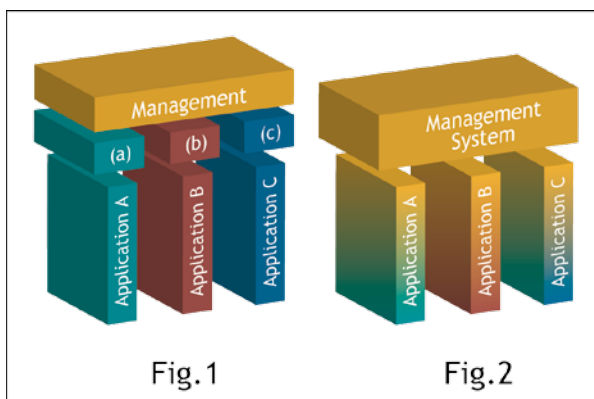
INTEGRATION TRENDS

Trend A—security vendors adding more security functions to security products.

Trend B—network vendors adding security products to their portfolios

For simpler and less demanding networks, these all-in-one security solutions may prove to be ideal, once the underlying integration issues are resolved. However, for those seeking defense-in-depth and design flexibility, there is still a fair amount of skepticism.

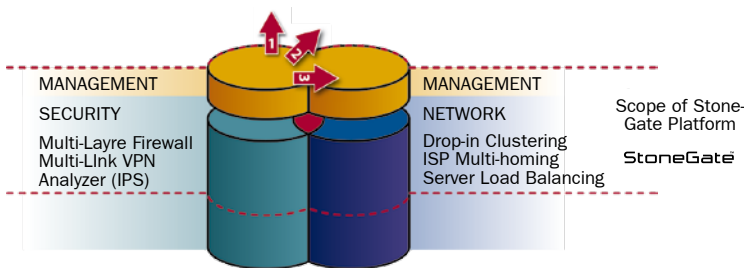
What is especially noteworthy is that in the race to deliver integrated platforms, most vendors have overlooked the juncture where security and networking overlap. For organizations that need network connectivity uptime in addition to security, load balancing and end-to-end communications assurance play a key role. Attempting to ensure high availability using a “bolt on” approach may actually undermine any gains made through vertical security integration initiatives.



INTEGRATION VS. UNIFICATION

Figure 1 illustrates how the use of APIs reduces management flexibility and power. Figure 2 shows complete control and transparency can only be achieved during the system design phase.

In fact, more valuable synergies can be achieved by integrating gateway load balancing, ISP multi-homing and route optimization with firewall functionality, rather than by integrating firewall and AV protection. For example, in the former, much of the routing administration becomes management-free, by simply configuring the firewall default routes. Where in the latter, firewall administration and AV management are distinct functions managed separately, even if they are managed through the same management console.



STONEGATE INTEGRATION

StoneGate blends network security and availability for cross-functional synergies.

Management system integration trends:

- (1) incident and alert handling,
- (2) security enforcement,
- (3) systems and data control.

Again, mid-sized enterprises typically do not have a hard division between their IT security and network teams, nor do they have the luxury of

having networking specialists assigned to manage business continuity functions. For these reasons, establishing a cross-functional, horizontal integration between the firewall/VPN and essential network availability components can be very beneficial. While this does not mean that other functional integration would not make sense, it is where the biggest infrastructure and manageability simplification can be realized.

IT Manager's Challenge

- Security management is becoming more and more complex and threats expand and gain in sophistication—especially for distributed enterprises.
- Continuous uptime is critical but costly for most enterprises.

Security Management

Fundamental challenges facing IT managers include not only network security but also security manageability, especially as it relates to today's highly distributed business architectures. Just as the sophistication and frequency of threats are expanding, so is the management aspect of security solutions. As one example, continual patching requirements are one of the biggest challenges of firewall security. Even firewall appliances often have a separate and sometimes proprietary operating system that requires its own patching apart from that of the firewall software application.

Security policies must also be enforced across the distributed organization, which often has more branch locations than branch-resident IT specialists. To that end, many IT teams are finding that with regard to firewall vendors' central administration claims, the devil is in the details.

For example, while security policies can be set remotely:

- Can version upgrades also be performed remotely? If so, how are they done during regular business hours without adverse impact on productivity?
- If a new OS or application vulnerability is found, is it possible to change firewall rules across multiple firewall gateways?
- Can a rapidly spreading worm be remotely prevented from entering any of the company's sites?

At the same time, there are new security products that have promised to deliver added layers of defense, but have also added to the management burden. For example, the first generation of IDS tools has often created more trouble than value, due to an overwhelming number of false alarms. Administrators have to keep up with these alarms to determine which are accurate, or set thresholds high enough to reduce the number of alarms. Unfortunately, this

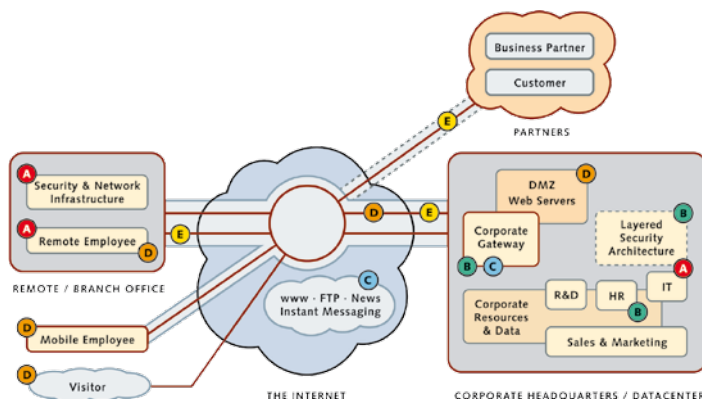


FIGURE 1 - MANAGING NETWORKS AND DISTRIBUTED SECURITY IS COMPLEX AND CHALLENGING

(A) Network and security administrators are forced to search for better ways to administer remote sites due to continuous patching, upgrades and traveling.
 (B) Insufficient firewall-only protection and the uselessness of early IDS/IPS is driving the functional integration of the best capabilities of both technologies.
 (C) The business case for ISP multi-homing without complexity is fueled by the criticality of the Internet, combined with the unreliability of a single ISP and the IT staff workload.
 (D) Web-enabling business applications requires a fresh look at the DMZ. Now it has to be both secure and highly available, but usually networks cannot be entirely redesigned.
 (E) Fault-tolerant IPsec VPN and load balancing between frame relay circuits and Internet traffic overcomes the issues of frame relay becoming a bottleneck and the security of MPLS is not yet proven.
 (A through E) A simplified infrastructure, holistic system approach with unified management, logging and reporting is the best starting point to support new business processes and a remedy to regulatory governance pains.

also means that some attacks are missed. Or, if the product is also an IPS tool and capable of blocking suspect traffic, the feature may be turned off completely, increasing the chance of a catastrophic event. The truth is that very few enterprises in the mid-market have the staff required to properly manage event correlation using the current IDS solutions.

Continuous Business

IT management challenges also exist within the realm of ensuring service availability, Internet performance and site-to-site connectivity. Distributed organizations, as well as those expanding outside the corporate walls to interact with customers and partners, require reliable communications. This means always-on connections, and no downtime or performance issues.

For example, in a Web-enabled scenario, where Web services handle new orders over the Internet, poor service availability or downtime can translate to disruptions in the logistics control chain, lost revenue or even lost customers. While using firewalls to form a demilitarized zone or DMZ around Web servers is a tried and true practice, there is more required for uptime assurance. A pool of Web servers is needed for redundancy and to handle peak loads, and the protecting firewall gateway must also be made redundant and load-balanced for the same reason.

Of course, ISP performance issues are another impacting factor, since service availability is also affected beyond the corporate gateway or DMZ. Border Gateway Protocol (BGP) is the most common method for providing redundancy for Internet connections. However, BGP requires special hardware and complex management, as well as the negotiation of cooperative agreements between competing Internet Service Providers (ISPs). In addition, BGP does not readily address route optimization, a requirement that brings added complexity. For these reasons, Internet performance reliability has been placed outside the reach of many mid-sized enterprises. These organizations have been left to take their chances with the intermittent quality of Internet services, or to forego the Internet for critical business communications altogether. In fact, it is the Internet's uncertainty that has caused many organizations to avoid VPNs in favor of frame relay networks for connecting WAN and branch offices.

In comparison, frame relay is more costly than IP, the bandwidth is usually low, and the provisioning takes much longer. However, frame relay's advantage lies in its ability to provide service level agreements (SLAs), where the Internet has been best effort only. Frame relay is also perceived as more secure, although this is an illusion. This is because its data is transported over shared networks, just like IP VPNs. As a result, many organizations have begun to also encrypt their frame relay traffic.

What is needed is a simple means to form fault-tolerant VPN connections, where IPsec (IP security) tunnels would transparently migrate and always utilize the fastest possible route between multiple network connections at both ends. This would need to be accomplished without complex BGP, immature Multi Protocol Label Switching (MPLS) technology, or other methods that add to the management burden.

Benefits of A Unified Management Platform

- StoneGate makes the management of network security and network availability possible.
- IP reliability helps mid-market organizations leverage the Internet to compete better.

Stonesoft has built the evolution of StoneGate for IT managers who are responsible for the full gamut of networking, security and service availability of physically distributed enterprises. These administrators know that network security is only one aspect that needs to be cared for when high availability of a mission-critical service is required.

The StoneGate Platform for Security and Business Continuity addresses challenges for the IT manager with:

- A central console for managing network security as well as key aspects of network service availability.
- A multi-layered security approach that goes beyond the firewall
- Shared tools and unified management concepts for greater security and administrative efficiency
- The ability to manage ISP failover, load balancing and route optimization for reliable Internet services and site-to-site communications assurance.

In fact, a unique strength of the StoneGate platform is that it unifies management tasks for both network security and network high availability. The latter is vital for organizations that want to reliably conduct business over the Internet, or wish to replace existing (for example, frame relay) connectivity with a much more cost-efficient solution. Stonesoft's patented Multi-Link™ technology performs load balancing between multiple ISPs for continuous Internet access and fastest throughput. In this manner, it can ensure a transparent and fault-tolerant VPN tunnel over the Internet, as well as "always on" connections for corporate use and Web enabled services.

The StoneGate platform also extends the total security concept, with the unification of the StoneGate firewall/VPN and the new StoneGate IPS. Stonesoft's investment in building a solid security management architecture is now paying off, in the form of seamless functional integration of defense-in-depth security components. StoneGate IPS stems from the StoneGate platform, rather than being a "bolt on" solution. This approach enables full-fledged interoperability between security components, which, for the user, means overall greater security and more efficient incident management across the enterprise. It also eliminates double efforts when defining intrusion detection and perimeter security concepts, as well as non-comparability of log and audit data due to mismatched formats, a major problem in forensic activities.

It is also important to note that the StoneGate IPS addresses the single most problematic aspect of legacy IDS tools - the hundreds to thousands of false alarms generated daily. As a next generation IPS, it delivers much more accurate event detection to significantly reduce the administrative burden and lower the cost of security incidents. (For more information on the StoneGate IPS, see the Stonesoft white paper, *Winning the Battle Against False Positives*.)

Subsequently, there is a growing misperception that today's "deep inspection" firewalls replace the need for IDS/IPS as a separate function altogether. However, while deep inspection firewalls do offer certain aspects of intrusion detection and even prevention, most vendors can attest that these capabilities are akin to a "light" version only. It should not be considered a replacement for a purpose-built and fully functioning IPS as an added layer of defense. The ideal is for firewall and IPS to be separate but integrated, in order to ensure defense agility and therefore greater protection, while also eliminating a single point of compromise, as is the case with all-in-one solutions.

Management Simplicity

With the StoneGate platform, organizations can increase their security levels while gaining administrative simplicity. This compares to the escalating management requirements that often come when security suites expand. StoneGate customers decrease their administrative and training costs by having only a single consistent management system and not having to train three times—once for each product, firewall, VPN and IPS.

Stonesoft takes a three-dimensional approach to security management: security policy enforcement, alert and incident handling, and systems and data management for all products combined. With the StoneGate Management Center, security policies and concepts can be

shared across products, with functions such as log filtering and browsing managed via the same tool. The StoneGate Management Center correlates event data from multiple sources, using generated intelligence to make the appropriate alerts and coordinate corrective actions. It also helps to relieve the extensive configuration requirements and large data sets that often come with defense-in-depth strategies. Data is kept in a single location, and can be categorized in an easy-to-understand and maintain manner. As part of this, log and audit data management, and license management, are handled in the same place.

Does Stonesoft's approach for security and continuity provide benefits for large enterprises? Yes, mainly by means of simplifying what they already have. But for mid-sized enterprises, the impact is even more profound. In particular, the ability to manage not only network security but also network availability adds an important function that was previously out of their reach, due to capital issues, staff limitations, or simply because ISPs were unwilling to cooperate.

To offer an analogy, in the past, only large corporations could afford the big laser printers, capable of high-quality color printing, and those functions were managed by in-house copy and print centers. Today, much smaller enterprises, and even the different departments within those enterprises, can now afford quality color printing equipment. In this way, Stonesoft makes both advanced, multi-layered network security and continuous business accessible to mid-market organizations. Such capabilities place initiatives that once belonged solely to large enterprises—projects such as VoIP and real-time logistics over the Internet—within the realm of these organizations, as well.

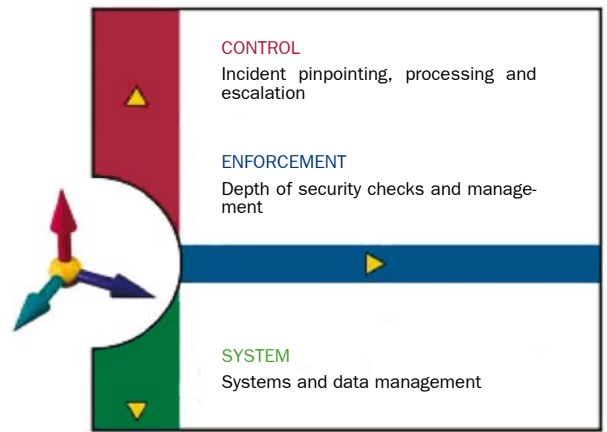


FIGURE 3
The three dimensions of security and system management. The importance of the system and data management will grow over time and is generally the weakest link in the security industry. The maintainability and the structure of the contained data becomes important for tight policy definitions, forensics and trend analysis, and audits and organizational governance.

Conclusions

- Infrastructure simplification helps resolve today's increasing management requirements.

The StoneGate platform offers the ability to converge defense in depth network security with network high availability assurance, within a true centralized management environment.

Why are many IT managers of mid-size organizations evaluating or deploying new technologies, even when their IT staffs are not growing? In most cases, limited resources and budgets do not prevent IT managers from evaluating new technologies. In fact, it is quite the opposite, as they often have no other choice than to consider new ways to meet the increasingly higher service expectations of users. At the same time, however, there is a rising concern over increasing management complexities and associated costs.

Infrastructure simplification can help in resolving today's increasing management requirements. IT managers can start by optimizing their architectures for fewer add-ons and point solutions. When they choose products, they should consider solutions that do not necessarily have the highest numbers of integrated components, but those that have the right ones, providing the highest synergy among the most key functions.

IT managers should ask the following questions:

- Do my Y2K-era security tools still provide the defense agility required? Can I keep up with the growing volume of security threats?
- How can I deliver greater network protection without growing administrative requirements exponentially?
- Does my current LAN infrastructure provide communications continuity to support new Internet-based business processes?
- Can my current WAN infrastructure be quickly and easily scaled to support corporate growth expectations?

The StoneGate platform can help IT managers in mid-size enterprises resolve all of these issues. It offers the ability to converge defense in depth network security with network high availability assurance, within a true centralized management environment.

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