STONESOFT

Whitepaper

The Evolution to the Next Generation Firewall

Meeting Today's Critical Enterprise Network Demands

Table of Contents

Executive Summary

Guided by a more optimistic economic outlook in 2010, many enterprises are determining which areas of their IT infrastructure need to be updated. It is not surprising that network security is on the forefront. While IT budgets were meager in the last 18 months, security threats to the corporate network were not. In response, enterprises are eager to reduce their vulnerability as they seek higher revenues and profitability in 2010 and beyond.

To narrow their focus on improving network security, enterprises should start by evaluating their existing firewall technology. This perimeter line of defense represents the frontline of the battle to secure the enterprise network. However, most organizations continue to use first generation firewall technology that provides only limited protection against today's sophisticated network threats.

While adequately capable in the early years of their development, first generation firewalls have become outdated within the context of today's network environments. Like any technology, these early firewalls are challenged to keep pace with increasingly complex infrastructures and sophisticated threats, precipitating the evolution of a new kind of firewall – the Next Generation Firewall.

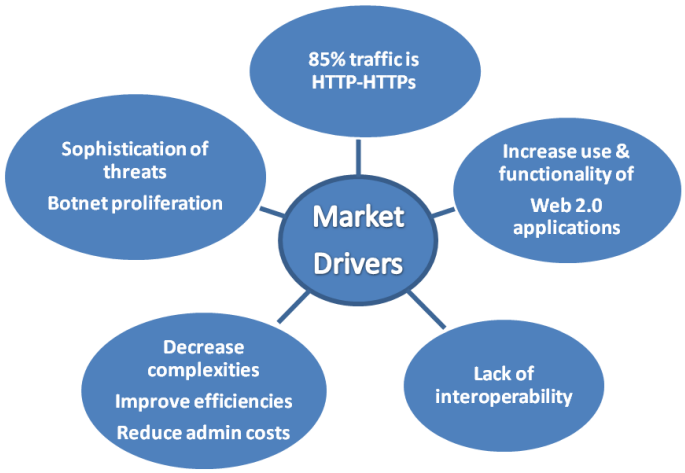
Before understanding the need for the Next Generation Firewall, it's important to understand the history of the first generation firewall. The market leaders that developed first generation firewall architectures in the early 1990's created devices that required separate management of the operating system, hardware and software. This made updates and patch management extremely cumbersome. Furthermore, these firewalls were not designed to inspect web traffic, which now constitutes an overwhelming majority of all network traffic as today's enterprises use the Internet to connect to applications and critical business information. With that, the network threat landscape has fundamentally changed, thereby limiting the effectiveness of first generation firewall devices.

Below is a summary of the five reasons first generation firewall technology must evolve*:

1. **Cannot protect against increasingly sophisticated threats resulting from Web 2.0.** The sophistication of network threats has exploded in the past 18 months, especially as it relates to preventing botnets, enabling secure access to Web 2.0 applications and cloud computing environments.

2. **Lack of detailed, real-time traffic inspection.** The rise of SaaS and HTTP/HTTPs traffic has overwhelmed first generation firewalls. In fact, nearly 85 percent of all network traffic is HTTP/HTTPs. First generation firewalls either fail to inspect – or at least thoroughly inspect – web traffic in real time. In many cases, firewalls have to be manually configured to support this traffic, which is crucial to facilitating business operations. The end result is an increase in the number of security breaches caused by human error in the manual firewall configuration process.

3. **Inability to meet the high availability requirements of today's enterprise operations.** Network availability continues to be an immense concern for today's enterprises. First generation firewalls are very limited in what they can do to support network availability. They do not facilitate the active/active clustering of firewalls that allow organizations to add capacity on demand, nor do they support ISP and VPN load balancing. Separate solutions are required for clustering, load balancing and failover.



4. **Lack of correlation capabilities & limited network visibility.** The inability of first generation firewalls to correlate network events greatly inhibits an enterprise's ability to proactively manage and detect network threats. This presents a major roadblock to network visibility. At best, most first generation firewalls can only provide a snapshot of network activity through a basic management console. The ability to drill down and investigate specific threats is virtually impossible – especially as today's enterprise networks typically include dozens of firewalls from different vendors. For example, a first generation firewall may alert you to a threat, but is unable to pinpoint the specific firewall. Rather than immediately resolving the threat and updating all network firewalls to prevent a similar attack, administrators spend valuable time simply trying to find the point of origin. This inefficiency is a threat in itself.

*Young, Pescatore, Greg, John (2009, October 12). Defining the Next-Generation Firewall, G00171540, Inclusive -- 2. Retrieved January 7, 2009, from Gartner. 2008 CSI Computer Crime & Security Survey, Inclusive – 2, Retrieved January 7, 2009 from CSI.

5. **Complex & expensive to manage.** First generation firewalls have to be managed individually and configured manually. Today's networks are made up of a complex configuration of network devices, all of which have to be monitored and updated on a routine basis. Without an easy way to see network activity and configure devices, managing first generation firewalls can be chaotically inefficient. This is compounded by the fact that today's networks are typically made up of devices from various vendors, all of which have their own separate management console. Finally, as virtual network devices gain popularity, device management becomes exponentially more difficult as network visibility decreases. With first generation firewalls, enterprises have no way to manage *all* virtual and physical security devices from a single point of view.

The Risks & Costs of First Generation Firewalls

Inherent in the shortcomings of first generation firewalls are a myriad of costs to the enterprise. The cost of a down network, or a breach in customer payment data, can devastate a company's revenues and regulatory compliance.

Even when first generation firewall threat detection is at its best – which still lacks depth of inspection – they are difficult to manage. An average enterprise has dozens of firewalls from different vendors to manage and configure – often manually – which introduces a new set of challenges. In fact, Gartner Research estimates that 99 percent of security breaches stem from misconfigurations at the device level. In other words, the management of first generation firewalls has become a major network security threat. It is rife with human error, not to mention demanding of precious IT resources.

The firewall industry has placed revenue above results. Realistically, it is nearly impossible to secure a network within the base purchase price of a first generation firewall. These days, securing a network requires a combination of powerful firewall inspection capabilities, simplified management of network devices, high availability capabilities that keep every firewall up and running, and reporting to ensure compliance. First generation firewall technology only provides inspection – and a limited version of that. To achieve secure perimeter protection, enterprises must pay extra for bolt-on modules or products that accomplish the rest.

This industry model of delivery is quickly becoming outdated. No one would expect to buy a car and then pay extra for the doors, yet that is what traditional firewall vendors seem to expect out of the enterprise market. Fortunately, times and technology are changing.

Understanding the Next Generation Firewall

To compensate for the limitations of first generation firewalls, a new kind of firewall device has recently appeared on the network security scene: the Next Generation Firewall. While several organizations claim to provide Next Generation Firewall technology, the truth is that there are very few “pure” Next Generation Firewalls on the market today. False vendor claims have led to much confusion about what constitutes a true Next Generation Firewall. As of the publish date of this whitepaper, Gartner Research has done the most thorough and decisive job in defining Next Generation Firewall standards.

According to their definition, a Next Generation Firewall must demonstrate the following functionality:

1. **Existing first generation firewall functionality.** The Next Generation Firewall leverages all of the capabilities of first generation firewall technology, while addressing far more than perimeter network traffic inspection. The Next Generation Firewall integrates high availability technology that helps keep the network up and running. This includes the support of active/active clustering (as opposed to active/inactive or hot standby clustering) that allows organizations to add capacity on demand without bringing down the firewall, along with ISP and VPN failover functionality. Additionally, it inspects all traffic in real-time.

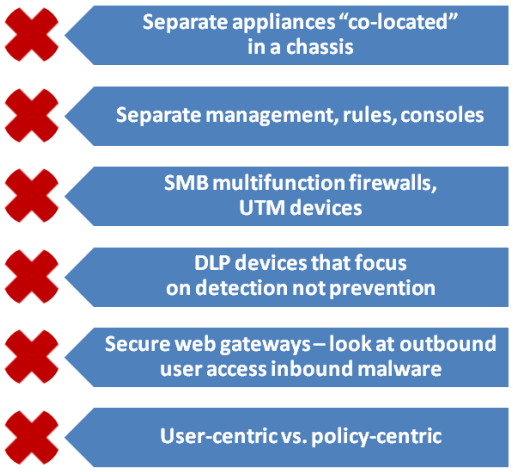
2. **Integration of firewall & intrusion prevention system (IPS) capabilities.** Whereas a first generation firewall only inspects traffic at the perimeter, the Next Generation Firewall adds another layer of detailed traffic inspection. For example, this integration allows the firewall to block an address that is continually loading the IPS with bad traffic – rather than just inspect traffic at an incident level. This integration also enables the sharing and reuse of rules syntax, centralized management of firewall and IPS capabilities, and consistent policy and rules enforcement. As a result, the Next Generation Firewall not only improves security, it simplifies network management by eliminating redundancies in the updating, configuration and maintenance process.

3. **Single platform for traffic inspection & policy configuration.** The Next Generation Firewall provides a single management interface for administrators to manage traffic and achieve true network visibility. This interface drastically reduces extraneous complexities and redundancies in the network management function by allowing enterprises to manage policies across all network devices, as well as quickly identify or predict security threats for faster resolution.

5. **Integrated deep packet inspection.** The Next Generation Firewall also enables deep packet inspection to eliminate threats inherent in web traffic (HTTP/HTTPs). The Next Generation Firewall enables enterprises to open encrypted web traffic and treat it with the same inspection as clear-text HTTP data – thereby eliminating a critical blind spot in network protection.

6. **Application awareness.** Whereas first generation firewalls were application-agnostic, the Next Generation Firewall is able to identify applications and enforce network security policies at the application layer. This happens independent of port and protocol.

7. **Support for inline, bump-in-the-wire configurations.** To adequately secure the network perimeter, firewall inspection must occur at network speed. This requires high availability technology that ensures every firewall is working and that traffic can easily be re-routed and balanced regardless of any issues happening across the network. Next Generation Firewalls must include this high availability technology.



As clearly as Gartner Research has defined the Next Generation Firewall, they have also pointed out what a Next Generation Firewall is not. It is *not* a combination of separate appliances co-located on a single chassis. It is *not* a multi-function firewall or unified threat management (UTM) device. It does *not* feature separate management consoles. It is *not* a data loss prevention (DLP) device that focuses on detection rather than prevention, and it is *not* a secure web gateway. Finally, it is *not* a user-centric device that focuses on access; it is policy-centric.*

*Young, Pescatore, Greg, John (2009, October 12). Defining the Next-Generation Firewall, G00171540, Inclusive – 3-4. Retrieved January 7, 2009, from Gartner.

Conclusion

The first generation of firewall technology was developed for first generation networks. With the proliferation of sophisticated network threats, many of which are a byproduct of advances in Web 2.0 and cloud computing, enterprises have been challenged to secure their networks within the limits of their budgets, staff and available technology.

The rise of Next Generation Firewall technology is quickly giving enterprises the ability to more effectively secure their networks at the perimeter level – as well as address several other formidable network concerns like availability and lack of centralized management. Through its long history of developing market leading high availability and centralized management technologies that are built in with its firewall solutions – not to mention advanced security performance – the StoneGate NextGen Firewall is uniquely qualified to lead the Next Generation Firewall evolution.

The StoneGate NextGen Firewall

Stonesoft is one of the few vendors to provide a true Next Generation Firewall solution that uniquely integrates advanced firewall/IPS capabilities with its patented high availability technologies and sophisticated next generation management.

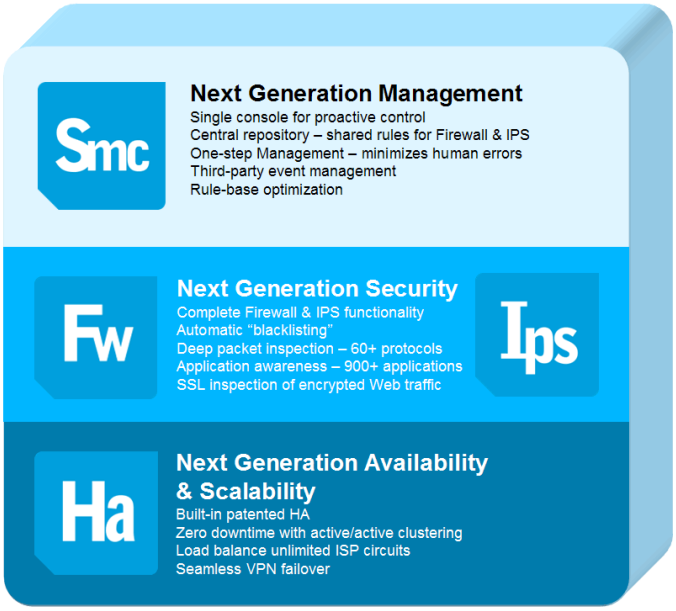
It is important to note the evolution of Stonesoft's firewall technology over the years as it has much bearing on how Stonesoft is leading the Next Generation Firewall market today. In the late 1990's, Stonesoft – which pioneered the market-leading StoneBeat™ clustering technology for firewall devices – decided to take the lessons it had learned from the fundamental flaws of first generation firewalls and develop a more sophisticated solution. Stonesoft released the first StoneGate Firewall/VPN software solution in 2001 and the appliance model where the hardware, software and operating system could be managed as a unified device in 2003. Therefore, Stonesoft has primed its device architecture for Next Generation Firewall capabilities from the very inception of the StoneGate Firewall/VPN solution line.

As outlined below, the StoneGate NextGen Firewall solution is delivering unmatched levels of security, availability, scalability and manageability for today's enterprises:

- **Next Generation Security:** With integrated firewall/IPS functionality for both client- and server-side, the StoneGate NextGen Firewall solution thoroughly inspects all aspects of network traffic, from basic Web browsing to peer-to-peer applications and encrypted Web traffic in the SSL tunnel. With deep packet inspection support of more than 60 protocols and 900 applications, the StoneGate NextGen Firewall solution provides many ways to protect against increasingly sophisticated threats – including application awareness, SSL inspection, nested inspection and IPv6 support.

- **Next Generation Availability & Scalability:** Stonesoft has long been praised for the fact that all of its network security solutions feature its patented, built-in high availability technology – Multi-Link™. Its presence in the StoneGate NextGen Firewall ensures that the enterprise network never goes down and that traffic load is balanced over any number of ISP circuits. Furthermore, the StoneGate NextGen Firewall supports active/active clustering of up to 16 firewall devices and seamless VPN failover. In sum, a single investment in a StoneGate NextGen Firewall can effectively replace load balancing, failover and clustering solutions – thereby reducing operational costs while actually improving overall network performance.

- **Next Generation Management:** With its advanced firewall and IPS integration, the StoneGate NextGen Firewall simplifies network security management. Through a single console, enterprises can manage all network devices – even third-party devices – to achieve complete visibility across the network. The StoneGate NextGen Firewall also provides one-step management capabilities, such as automatic blacklisting, that allow one-time configurations that can be pushed to other StoneGate devices. Furthermore, it features a central repository that allows rules to be shared between the firewall and IPS.



Stonesoft is one of the few vendors to provide a true Next Generation Firewall solution that uniquely integrates the full functionality of the StoneGate Firewall/IVPN and StoneGate IPS with its patented high availability technologies and sophisticated next generation management.

The StoneGate NextGen Firewall exceeds the current standards set forth for Next Generation Firewall solutions. While many established firewall vendors strive to "retrofit" their existing technology to meet these standards with a fundamentally flawed architecture, the StoneGate Next Generation Firewall is rooted firmly in built-in, integrated functionality that improves security, availability, scalability and manage-ability. (Figure 1) On the flipside, new Next Generation Firewall startups are lacking the experience in core first generation firewall capabilities. This highly differentiates the StoneGate NextGen Firewall from any other product on the market today. As mentioned above, Stonesoft has maintained and executed a strategic approach to built-in security functionality within every solution it has brought to market for the past 10 years.

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.

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