STONESOFT

Whitepaper

Next Generation Management

Managing Complexity – Your Biggest Security Threat

Table of Contents

Executive Summary

The IT landscape within the enterprise is quickly changing. In just the last three years, many fundamental shifts have propelled enterprises into a new chapter of technology. The widespread adoption of virtualization has become a reality, and cloud computing is close behind. The new breed of mobile devices, like the iPhone, are not just a means of communication – in many cases, they are replacing PCs as the epicenter of business activity.

While the changes and advancements are too numerous to list, the impact they have had on network security has been alarming. In short, the enterprise network has never been more challenging to secure than it is today. Nor has it been more complex.

The sheer number of virus, worms, malware, ransomware and other external network threats is astounding. But, even more alarming are the number of internal threats – many of which are generated not by disgruntled or malicious employees but by the complexity of the network security infrastructure that aims to prevent these attacks. The most obvious culprit of this issue is network device management. Today's network devices are cumbersome to administer, requiring administrators to use multiple management consoles or even to manually configure each device.

In 2009, Gartner released a surprising statistic that addresses the challenges of growing network infrastructures and distributed networks. Approximately 99 percent of security breaches are caused by misconfigured devices.*

As a result, its becoming increasingly important to improve network security management – or risk costly consequences.

The issue of network complexity boils down to the following challenges that exist in current network device management today:

- **Human error** – Today's network devices must be manually configured through a variety of device management consoles. With dozens of network devices in the average enterprise network, this process has become polluted with human error and inefficiency, contributing to an increase in network security breaches.
- **Lack of correlation** – Currently, it is difficult for network administrators to correlate a specific security incident to a specific device. While they may get an alert that an incident has occurred, they have to search and locate the device at which the incident resides – wasting valuable time and resources.

*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.

- **Increased time to remediation** – Because of the lack of event correlation and the ever-expanding number of devices on the network, the time it takes to resolve a security incident is growing. This is of major concern as threats can quickly proliferate throughout the network, not to mention the negative impact of having a down or disrupted network to a company's overall operations.

- **Reactive versus proactive management** – The network security industry has long preached a proactive, process-focused approach. However, complexity within the network impairs an enterprise's ability to implement and smoothly execute critical security processes, such as routine policy updates.

- **Inefficient, ineffective reporting and compliance** – Creating network-wide reports through multiple device reporting tools is both time-consuming and ineffective. For many enterprises, there is no easy way to get a detailed and comprehensive view of network performance. Furthermore, as network security has become a crucial part of many regulatory and industry standards, the inability to easily produce accurate reports stands to threaten compliance.

- **Difficult to manage remote devices** – Today's enterprises are challenged to manage network devices in a single location; managing and configuring devices housed in remote locations (e.g. regional offices, partner locations) is nearly impossible without onsite support.

Making the Case for Next Generation Management

The thought of a widespread virus attack on the network is enough to scare even the sturdiest IT department. However, more and more enterprises are acknowledging what has been stated clearly above. An enterprise's biggest IT threat is network security management, with the sheer number and type of network devices that have to be managed posing a formidable challenge.

The average enterprise network contains dozens of firewalls, intrusion prevention systems (IPS) and SSL VPNs. In most cases, this mix represents devices from multiple vendors. Now, let's factor in the increase in virtualization, and now cloud computing, at the enterprise level. Since these environments can't be adequately secured with traditional physical devices, virtual security devices must be implemented and maintained.

Therefore, an enterprise can easily have 100+ physical and virtual devices from three or more vendors. And, herein lies the root of the problem. Traditionally, each device on the network has had to be configured and updated individually. This leaves ample room for human error, which blasts the door wide open to a multitude of network attacks.

Security is obviously the main concern in this scenario, but the costs associated with this traditional – or first generation – management approach are not to be under-estimated. In the 100-device scenario above, multiple full-time network administrators would be required to simply keep the devices up and running. Moreover, given the likelihood of a security breach due to device misconfiguration, this enterprise would likely experience network downtime, even data theft, that could cost hundreds of thousands (or millions) of dollars.

Another byproduct of first generation network management is the inability to resolve network security incidents expediently. Without a centralized and detailed view of network device activity, it is hard to determine the origins of threats and resolve the incident quickly.

What enterprises need is a single, centralized way to manage every network device, physical or virtual – regardless of vendor. This approach is a radical departure from the status quo and presents tremendous improvements in security, as well as significant reductions in network costs and resources.

For too long, traditional device management has been one of the root causes of network complexity. As the average network has multiple devices from multiple vendors, each device has to be configured and monitored with disparate consoles, which has an exponentially negative impact on the network. As described above, the use of separate device consoles promotes a labor-intensive manual approach to network management that is prone to widespread human error and slow threat mitigation.

It is also important to note that this first generation approach to device management has caused the total cost of ownership (TCO) for network infrastructure to skyrocket over the years. Even when every device is up and running and properly configured, which is rarely the case in today's expansive enterprise networks, infrastructures are still vastly more expensive to run than ever before. This is because many vendors employ a bolt-on product marketing strategy, which requires enterprises to make separate solution or module purchases for log management, reporting, load balancing and other functionality. Each additional solution has to be managed, maintained and configured separately, which requires substantial time and effort from today's already overburdened IT departments.

The solution is a centralized, built-in approach to network device management. With this approach, and the technology to support it, enterprises can manage and monitor all devices from a single management console – including third-party and virtual devices.

For instance, using centralized management, an enterprise can address configuration using a "create once, deploy everywhere" functionality within the console. In other words, the network or IT administrator can create a rule or configuration once, then roll it out to every device on the network. Additionally, the console can facilitate automatic blacklisting of suspicious or malicious IP addresses so that every device on the network is guarded against potential threats originating from that sender or location. Most importantly, enterprises can finally respond to threats in real time, as the management console enables administrators to immediately see a threat as it emerges on the network, identify its location and the affected device, and configure the device accordingly.

Conclusion

The complexity of network security infrastructure has long been ignored as the primary issue threatening enterprise networks. As the IT landscape continues to evolve and the number of network devices continues to grow, enterprises must preempt this threat by changing the way they manage their networks.

A device agnostic, centralized approach to network security management is the critical first step in eliminating network complexity. The StoneGate Management Center makes this step simple for today's enterprises by giving them the ability to quickly and easily identify and resolve threats – regardless of the kind of device.

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 Management: An Introduction

Stonesoft has long advocated a centralized approach to network management through its StoneGate Management Center which manages the entire StoneGate Platform – including the StoneGate NextGen Firewall, IPS and SSL VPN devices. In 2009, Stonesoft became the first network security vendor to offer third-party event management capabilities, which effectively ushered in a next generation of network security management.

Unlike other network security solutions, the StoneGate Management Center enables real-time monitoring, alerting, troubleshooting, managing and reporting from a single management console and central repository. This gives administrators proactive control of their entire network – physical, virtual and now third-party devices. As a result, fewer resources are needed to manage network devices, incident resolution times are faster and fewer security breaches occur. With this trifecta of network savings, Stonesoft is delivering the lowest TCO on the market today.

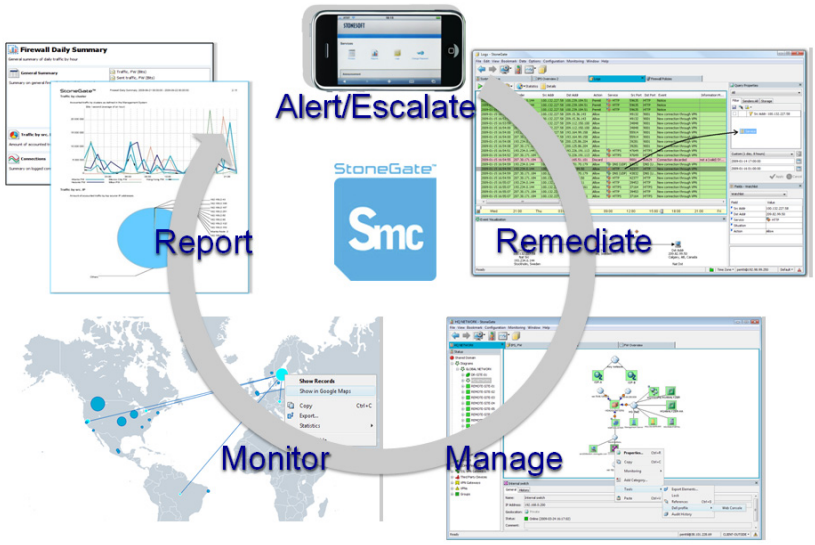

Figure 1: *The StoneGate Management Center enables real-time monitoring, alerting, trouble-shooting, managing and reporting from a single management console and central repository.*

Key features of the StoneGate Management Center include:

- **One-step Management:** The StoneGate Management Center allows enterprises to proactively manage hundreds of devices as easily as one from a single console – from simple device updates to immediately responding to security threats. Security policies and rules can be defined once and automatically updated to all devices, thereby eliminating costly misconfiguration errors and significantly decreasing threat response times.

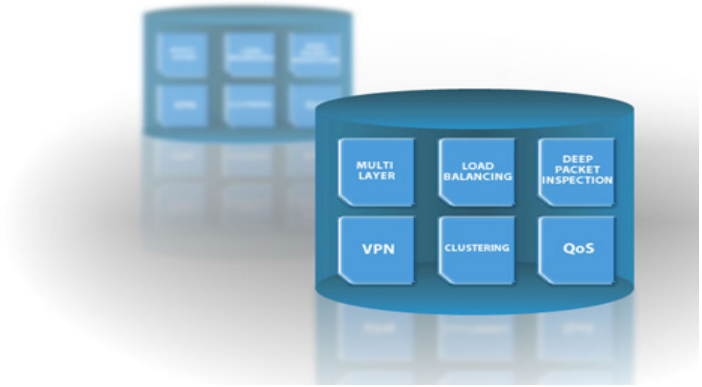

Figure 2 : *The StoneGate Management Center has a built-in central repository. Common elements such as server, application and network groups created for use in firewall policy can be re-used in all other configurations, such as IPS, alert policies, filters and reports.*

- **Central Repository:** Built upon a common element database, the StoneGate Management Center enables "create once, deploy everywhere" configurations since all components are shared within a central repository. Rules can be created once in the StoneGate Management Center, then deployed across all devices on the network.

  This results in easy component re-use, less administration and fewer human errors. The central repository stores all configuration information for fast recovery, provides customizable role-based access for multiple administrators, and enables the creation of end-customer domains for managing different customer environments with a single management server.

- **Third-party Event Management:** As mentioned above, the StoneGate Management Center provides the first platform for proactive network security management of entire networks, including physical and virtual environments, as well as third-party devices. This gives enterprises access to real-time device monitoring, logging and reporting of the switches, routers and security appliances from different vendors across their networks. As a result, administrators can significantly streamline troubleshooting and incident management time.

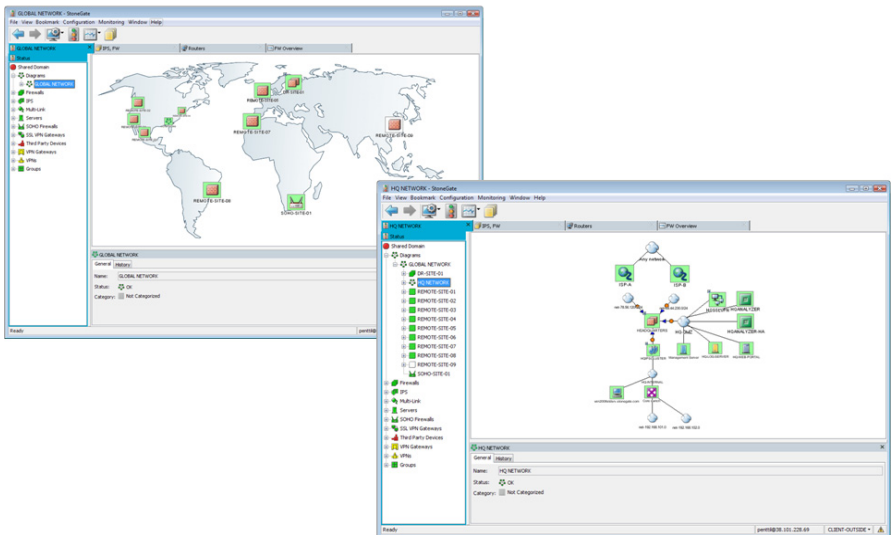

Figure 3 : *The StoneGate Management Center provides the first platform for proactive network security management of entire networks, including physical and virtual environments, as well as third-party devices. For instance, from the global monitoring view you can drill down to a more detailed view of one of the sites and the third-party devices at that site.*

- **Accelerated Incident Management:** The StoneGate Management Center delivers a common, correlated view of physical and virtual networks, as well as third-party events. In addition to being able to quickly spot threats, events and incidents across the network, the StoneGate Management Center features a powerful data mining engine that significantly reduces the time for troubleshooting, incident investigation and resolution. In addition, administrators can capture historical incident records to manage network security more proactively.

- **Real-time Monitoring & Alerting:** Where other systems offer only a crude snapshot of events, the StoneGate Management Center provides the most comprehensive real-time dashboards of network activity available on the market today. Using easy-to-interpret graphical views, geographic pinpointing of IP addresses, customized alert policies and drill-down and filtering capabilities, network administrators can quickly address anomalies and attacks. In addition, a Web portal gives administrators and MSSPs' end customers the ability to monitor network security anytime, anywhere and with any device.

- **Interactive Reporting & Compliance**: The StoneGate Management Center features easy-to-use, customizable graphical report templates, automated report generation and distribution, comparative analysis of security policies, as well as system auditing and audit trails to significantly streamline the entire process of ensuring regulatory compliance.

- **Rule-base Optimization:** The StoneGate Management Center features built-in rule optimization and validation tools that make it easier to manage and administer rules than ever before. Network administrators can organize security policies with templates, sub-rule bases and aliases, thereby minimizing human errors and eliminating unused and/or redundant rules. They can also create rules directly from logs for faster incident management.

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