



Whitepaper

Proactive Control

A Checklist for Implementing a
Proactive Network Management Strategy

Table of Contents

Executive Summary	3
Choosing a Network Management Strategy	4
Evaluating the Options.....	6
Implementing a Proactive Network Management Strategy	10
Conclusion.....	13

Executive Summary

Whether by force or by choice, enterprise and government organizations worldwide are expanding and contracting at record speeds. IT leaders are expected to adjust and accommodate to the ever-shifting landscape while finding cost-efficient ways to maintain secure, always-on networks in both physical and virtual environments. At the core of IT operations is the strategy by which organizations choose to administer their complex network infrastructure for optimal security, availability and cost-efficiencies.

As organizations and IT leaders are being inundated with new technologies that promise to create “world peace” in the network management industry, IT leaders must decide which strategy is right for their organization today, and plan for the future. Traditionally, organizations have implemented separate best-of-breed solutions from different vendors, which has created a complex, redundant network of disparate solutions that hinder their ability to manage security and availability in any environment. The result? An incoherent infrastructure of systems that more closely resembles a plate of spaghetti than a well-tuned network infrastructure, as each new layer and device adds yet another level of complexity.

The purpose of this paper is to assist business and IT leaders in determining the right network management strategy and architecture for their organization and to provide practical advice on how to implement the best strategy to drive tangible bottom line value.

While a lot of vendors claim to have centralized management, the key is to look beneath the surface to understand the level of manageability they are really delivering. Is it a bolt-on approach or a built-in fully integrated approach? Does it provide the comprehensive visibility and tools needed to realize the promise of proactive network management?

Choosing a Network Management Strategy

Whether you are in a rapidly growing organization that is adding people, offices and systems at record-breaking speeds, or an organization in the midst of a reorganization that is turning to IT to save the profit line by cutting costs, IT is becoming a competitive weapon that can help organizations continue to not only survive, but thrive. However, this new view of IT comes at a time when market dynamics are putting more pressure on IT to constantly do more with less – less staff, less budget and less resources. Some of the dynamics driving pressures on IT include:

- **Increased network infrastructure complexities:** According to industry analysts, the complexities of today's organizations have grown ten-fold over the past five years. With the mass adoption of technologies, such as the latest virtual technologies, mobile computing devices, Web-based application services and real-time systems, network security and availability is becoming more critical to the success or failure of an organization. As organizations grow, so does the infrastructure needed to support them. Gartner commonly refers to this as the “network sprawling affect,” while others simply call it complexity and fatigue.
- **Truly distributed networks:** With the evolution of the mobile workforce, the traditional “security layer” now has infinite possibilities as remote users 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. Similar to the layers of an onion, each new layer has unique security and IT challenges, adding more costs and complexity.
- **Rapidly changing regulatory requirements:** In recent years, IT leaders have seen an explosion in regulations surrounding IT security, continuity, visibility and organization transparency. There is a constant struggle to turn mounds of data into usable information to help improve the organization's security posture and reduce costs. No matter how many or how difficult the compliance requirements may be, IT is expected to quickly adapt to enable every facet of the organization to be compliant. This translates into expenditures that chip away at the IT budget, leaving little investment for strategic initiatives that can help grow or stabilize organizations. It also presents new requirements for management tools to provide greater visibility, proof, and cause-and-effect of proper controls and policies to third parties.

- **Proactively transforming data into intelligence:** As organizations expand and utilize more technology – whether from distributed networks to multiple products – they also face strategic and tactical challenges of transforming their data into intelligent and useful information. From a strategic standpoint, they must find ways to easily access high-level reports and information in order to improve efficiencies and reduce costs. Tactically, the ability to quickly analyze data, such as logs, can significantly impact troubleshooting issues. What data is captured and what is not, as well as the ability to analyze and make use of the data are key differentiators in a true centralized management system. The significance of this can make the difference in an IT organization’s ability to shift from being purely reactive to proactively controlling their ever-changing networks.

Most of these problems are present at virtually every size organization, and if not addressed, can cause significant damage to both the brand and to the bottom line. In fact, 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 and downtime with “99 percent of security breaches caused by misconfigured devices. That’s not a training issue, that’s a complexity issue.

Everyone agrees: Staying on top of the latest technology advancements is the only way to stay on top of these problems. However, this is much easier said than done, and trying to review the clutter of marketing hype can be more challenging than one would think. It all starts with not just selecting the right strategy for your organization, but making sure that you have the right tools in place for effective, proactive management.

Evaluating the Options

To further understand which approach is right for your organization, let's review the primary strategies in place today, from both an architecture and management point of view:

1. Best-of-breed Network

Configurations:

Traditionally, selecting best-of-breed Products from different vendors has been a common practice for most IT organizations that rely on a layered approach to security.

Not only has this approach created complex, redundant infrastructures that are extremely labor intensive to maintain, it opens the doors to human error and security threats.

Most best-of-breed products have been designed as device-centric appliances with little regard for integration across a layered infrastructure. In addition, when it comes to managing policies and rules, updating configurations and devices, incident management and troubleshooting, this approach has created a siloed approach to managing security and availability.

Some organizations have started to consolidate the number of vendors in their networks, and as a result have turned to large vendors that offer suites of products. However, the majority of the challenges remain, because these solutions are not integrated on a common platform and designed to help organizations gain proactive control of their networks.

The challenges with best-of-breed network configurations include:

- **How difficult is it to quickly address security threats?**

With multiple products and vendors, the time and costs required to not only locate the cause of problems, but also resolve them is extremely high. The inability to quickly push policy or software updates in distributed networks severely compromises threat mitigation and makes it difficult to maintain standards.

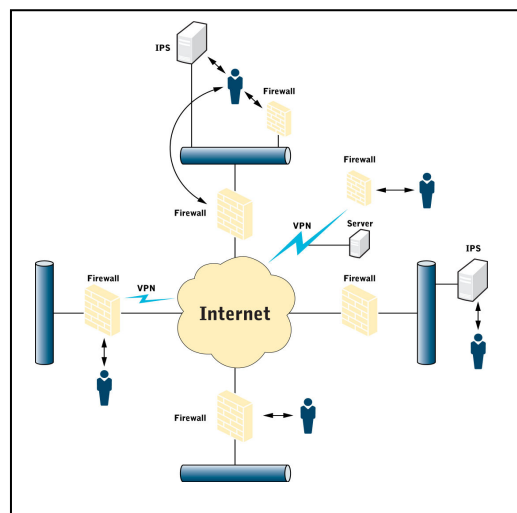


Figure 1 : Typical best-of-breed network configuration with disparate products managed by multiple administrators and no centralized control.

- **What impact will this have on your visibility across your infrastructure?**
Visibility across disparate point solutions becomes impossible and it is difficult to identify short- and long-term trends. If products have been acquired from different vendors and minimal effort has been made to integrate the solutions, the management capabilities are inherently limited.
- **What is the total cost of ownership (TCO)?**
Typically, this approach comes with an extremely high TCO in the form of operational and capital costs as well as the time and resources required to administer and maintain these solitary systems. In addition, organizations limit their ability to benefit from volume purchases from the same vendor.

2. Unified Threat Management (UTM): Selecting multiple products that have been integrated onto a single appliance. While this approach attempts to simplify the process on the surface, several issues arise such as:

- **What impact does this have on network performance?**
Recent industry review results showed a drastic impact on performance as each feature is enabled. In a *NetworkWorld* test of the leading UTM solutions, the review team concluded: “When we turned on their UTM features, however, systems that breezed through the 1,000 Mbps mark slowed dramatically. Out of 56 test results collected with various UTM features turned on, 36 registered results that were 250 Mbps or less.” That’s why organizations must carefully weigh marketing hype versus reality.
- **How does this affect your ability to implement a layered security approach?**
Typically this option introduces a single point of risk, because if one component is compromised, hackers can gain access to the “keys to the city.”
- **Can you ensure an always-on network?**
If an appliance is not available for a variety of reasons, a single point of failure is introduced. Regular routines, such as software patches or a simple glitch on one element, can cause chaos for the entire system.

3. Security Information and Event Management (SIEM): An approach where a third-party product is implemented to track information and events across a network, however this option presents its own set of challenges such as:

- **Can your administrators quickly pinpoint and address security threats and other incidents in your network?**

While SIEM products may give administrators visibility into incidents in their organization's network, these products are not designed to provide any tools for troubleshooting and quickly addressing incidents before they get out of control.

- **What complications will arise by introducing yet another product with new capital, operational and administration costs?**

Managing multiple vendors and multiple products is one of the major frustrations IT leaders face because it unnecessarily drains resources and impacts their ability to respond to organizational demands.

- **Will the data give you useful information for day-to-day operations?**

Implementing a SIEM product oftentimes means getting inundated with lots of data that requires additional resources to analyze and manage the data. In fact, many times it's more data than is needed, or the wrong kind of data that is really useful for pinpointing and quickly responding to any network issues.

- **What is the TCO?**

Typically, this approach comes with a large capital investment as well as the time and resources required to administer and maintain these solitary systems.

The Value of a True Centralized Control Platform – Proactive Control

In an effort to relieve some of the pains associated with disparate best-of-breed products designed to plug holes in the network infrastructure, there has been an industry effort to centralize the management of these products. Ironically, some attempts to solve this problem have caused more problems than they solve due to the time and resources that must be dedicated to integration initiatives that are often massive undertakings.

The primary driver in attempting to centralize the management of disparate products is to reduce the "technology fatigue" that naturally arises in a best-of-breed network configuration. However, unless products focus on delivering true centralized control, spending the time and money needed to make a best-of-breed configuration workable can cause even more technology fatigue and management headaches.

With a true centralized control platform in place, organizations are able to significantly simplify their infrastructure, because all of the solutions reside natively on a common platform and leverage a single communication language, a single set of tools and a single interface from which all components can be monitored and actively managed. Instead of being developed by multiple vendors with various platforms using different languages, all of the solutions come from a single source and are designed with each other in mind – all with the same DNA in place. As a result:

- Full-fledged interoperability between network security devices and always-on technologies is possible;
- Visibility and manageability of even the most complex networks increases;
- Easy access to critical data increases network security, performance and compliance;
- Rules and policies can be automatically shared and updated across networks;
- Real-time data from different sources can be quickly pinpointed and correlated to reduce incident management times; and
- Organizations are positioned to gain the lowest TCO.

As a result, organizations can reap the benefits of a simplified infrastructure that is much easier to manage, and most importantly realize the promise of proactive network management.

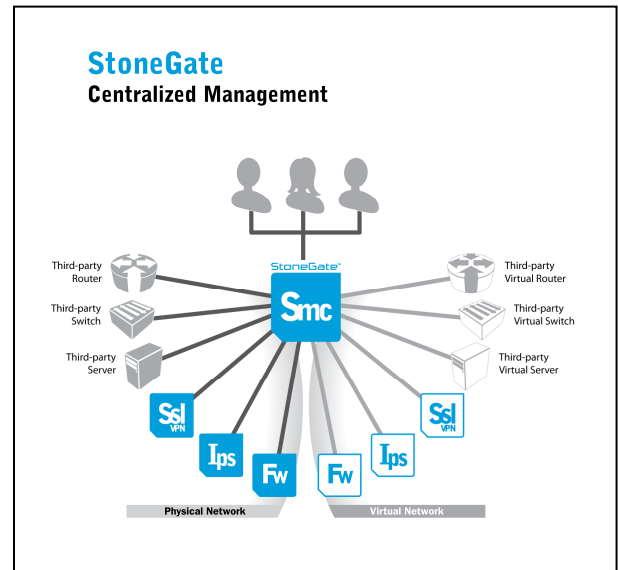


Figure 2 : True centralized control platform for simplifying the management of even the most complex networks – including physical and virtual devices, as well as third-party device events.

Implementing a Proactive Network Management Strategy

Where do you start when your organization is moving at lightning speeds? IT organizations are forced to try to refresh while keeping operations running 24x7. Changes are expected to happen with zero downtime and zero impact on the organization. As many organizations have moved to “follow-the-sun” approaches that require IT to maintain availability 24x7, there is no good time for maintenance downtime.

Stonesoft suggests following these three steps to implement a proactive network management strategy for optimal network security and resilient connectivity.

1. Determine the right place to start.

The old rip-and-replace approach is no longer possible as organizations are forced to do major technology refreshes every two or three years, according to leading industry analysts. Look holistically at your infrastructure from both a security and availability standpoint and evaluate which components are most critical to replace at this time. Is it your firewalls because your organization experienced a painful outage? Is it your IPS because you need to protect vulnerable internal systems? Is it your SSL VPN solution because your employee base continues to become more mobile? Select your starting point and begin evaluating technology partners.

2. Choose the right partner to help you execute your strategy.

With so many variations and solutions on the market, use this checklist when selecting your vendor of choice:

- **Solutions should offer true centralized management.**

While a lot of vendors claim to offer centralized management, organizations need to take a close look at the approach vendors use in their fundamental architecture. Is it a built-in fully integrated approach or bolt-on approach requiring the purchase of additional products?

That’s why many organizations are turning to Stonesoft, a global organization that has been helping organizations simplify network security since 2001. Stonesoft is the only vendor that provides proactive control with one true centralized command center for real-time management of the most complex networks. This centralized command center – called the StoneGate Management Center – manages the entire StoneGate Platform including its integrated firewall/VPN, IPS and SSL VPN solutions for both physical and virtual environments, as well as third-party device events.

- **Solutions should be easy to use.**

Ease of use is at the core of simplicity. As organizations simplify their infrastructures and deploy easy-to-use administrative tools, they are able to significantly reduce incident management times and start to take proactive control their networks.

REDFolder, a leading managed service provider, implemented the Stonesoft solutions and commented, “Since we were working with a prominent credit card services organization, we knew hackers were scanning our system. However, the minute we turned on Stonesoft’s solution, it was like turning on a light switch. Immediately, we had analysis and reports that provided clear details of who and what was trying to access our network, which enabled us to diffuse potential threats ahead of time.” (Ron Peters, president and founder of REDFolder)

- **Solutions should offer the depth of functionality needed to manage today’s complex networks. For instance, the StoneGate Management Center includes the following built-in functionality at no additional cost:**

- **Third-party Event Management:** Gives organizations access to real-time device monitoring, event correlation, logging and reporting of the switches, routers and security appliances from different vendors across their entire network. Administrators can significantly streamline troubleshooting and incident management time. And, most importantly, they can get this functionality built-in with the StoneGate Management Center without the need to implement a separate SIEM system.

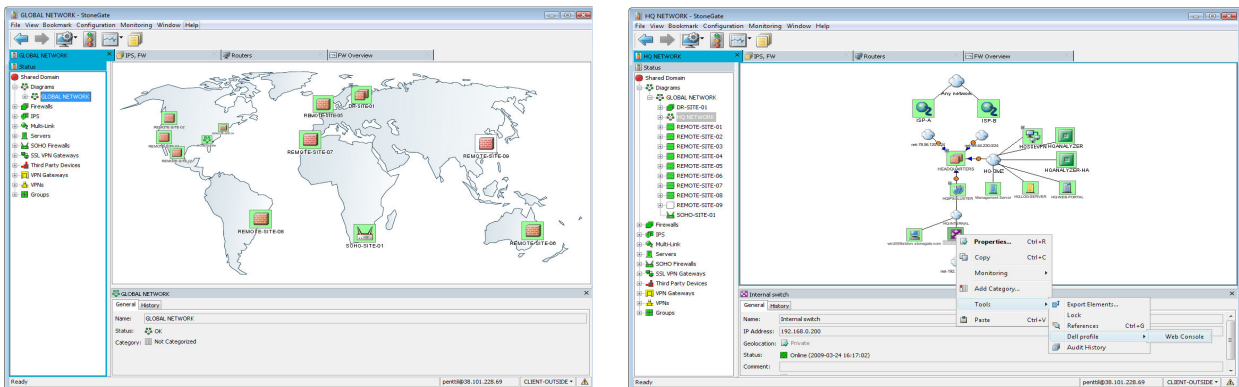


Figure 3: With third-party event management, administrators gain real-time visibility across their entire network – physical and virtual environments, as well as third-party devices.

- One-step Management:** Allows organizations to proactively manage hundreds of devices as easily as one – from simple device updates to immediately responding to security threats – from a single console. Security policies and rules can be misconfiguration errors and dramatically decreasing threat response times.
- Accelerated Incident Management:** Delivers one common, correlated view of physical and virtual networks, as well as third-party events, combined with a powerful data mining engine to significantly reduce the time for troubleshooting, incident investigation and resolution. In addition, administrators can capture historical incident records to more proactively manage network security.
- Central Repository:** Enables “create once, deploy everywhere” configurations since all components share a common element database. The results are 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.
- Real-time Monitoring & Alerting:** Provides the most comprehensive real-time dashboards of network activity compared to other systems that offer a crude snapshot of events at best. Using easy-to-interpret graphical views, geographic pinpointing of IP addresses, customized alert policies and drill-down and filtering capabilities, organizations 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 from any device.

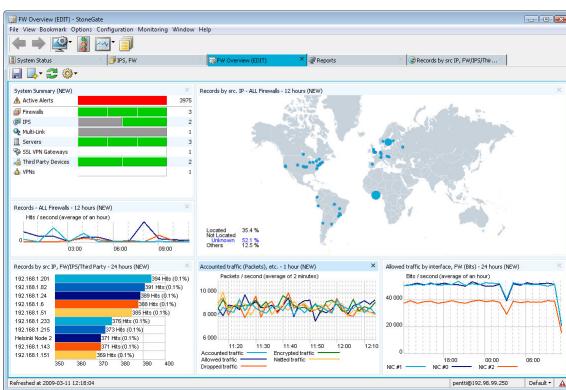


Figure 4 : With real-time monitoring and alerting tools, administrators can quickly pinpoint and address incidents before they get out of control.

- **Interactive Reporting & Compliance Tools:** Includes easy-to-use, customizable graphical report designs, 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.

3. Determine your most important metrics and measure, measure, measure.

Set a baseline before beginning any implementation and ask your vendor to help you throughout the process. According to Forrester Research, 75 percent of all IT investments are justified by measuring ROI. For AIT Worldwide Logistics, a leading transportation and logistics company, ROI and reliability were at the top of its list when re-evaluating its network security vendor. The company implemented Stonesoft's solutions and was able to reduce communication line costs per station by 86 percent. At headquarters, which is the hub for the frame relay, the company saved nearly \$400,000 in the first year.

Conclusion

To respond effectively to today's challenges of increased costs, complexities and regulatory issues, IT leaders are re-evaluating their network management strategies for the future of their organizations. By implementing the true centralized management platform that is offered by Stonesoft, forward-thinking IT leaders are realizing are not only realizing the promise of proactive network management, but delivering significant bottom line value to their organizations.

About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) delivers proven, innovative solutions that simplify network security management for even the most complex network environments. The award-winning StoneGate Platform unifies firewall, VPN, IPS and SSL VPN, blending integrated threat management, end-to-end high availability and network optimization, into a centrally controlled system. As a result, Stonesoft provides an unparalleled level of proactive security, always-on connectivity and compliance at the lowest total cost of ownership 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.

About the Author

Matthew McKinley is a senior network security analyst for Stonesoft Inc. McKinley has more than 10 years of experience in the network security industry, including more than six years with some of the industry's leading managed security service providers (MSSPs). In the MSSP market, he was responsible for multiple, large-scale centralized management deployments for organizations across the U.S. He designed a remote management solution for IPS devices. Additionally, he developed the audit reporting necessary to meet GBLA, Sarbanes-Oxley, PCI and FISMA standards. Writing contributions include articles and whitepapers on a wide variety of topics including virtualization and VPN architectures. He has also led training sessions on virtualization, perimeter security and intrusion prevention techniques.



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