

STONESOFT

Whitepaper

The Hidden Challenges of Securing a Virtual Environment

Table of Contents

| | |
|---|---|
| Executive Summary | 1 |
| The Challenges of Securing a Virtual Environment | 2 |
| How to Ensure You Have a Virtual-Ready Network Security Solution | 4 |
| Conclusion | 6 |

Executive Summary

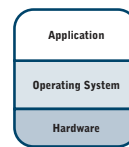
Virtualization is taking the IT industry by storm. In a recent *InformationWeek* poll, 70 percent of the respondents reported they're running at least one virtual server, yet less than 12 percent have a security strategy tailored to their virtual environment. Where does your organization fit in these statistics?

If you have already implemented or are in the process of implementing a virtualization strategy, your organization may be at risk for security threats that could have a much more disastrous impact on your operating environment than ever before. Since traditional security systems rely on hardware and special operating systems to protect your environment, they are rendered useless in a virtual environment where the goal is to reduce or eliminate hardware.

In addition, traditional best practices are now in question because physical segmentation and other methods are nearly impossible to implement. And finally, due to the nature of a virtual environment, network complexities are increasing faster than legacy management and monitoring systems, so visibility into the virtual and physical environments is extremely cloudy. Organizations need to take a closer look at a new means of securing their networks and sensitive information in the new virtual world.

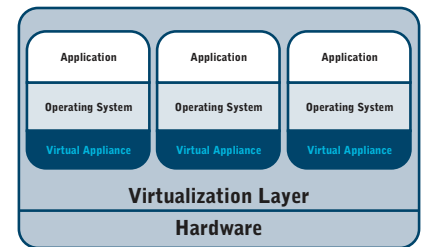
The purpose of this paper is to arm security professionals and IT leaders with a solid understanding of the potential risks of not incorporating new security technologies into their virtual environments. It explains the reasons why traditional systems don't work, and it provides a list of questions readers must ask to ensure their networks are virtual-ready.

Virtualization 101



Traditional x86 Architecture

- ✓ One operating system per server
- ✓ Software and hardware tightly coupled
- ✓ One application per server
- ✓ Typical load on server 5-15%



Virtualized Architecture

- ✓ Several operating systems per server
- ✓ Separation between software and hardware
- ✓ Several applications in server
- ✓ Typical load on server 50-70%
- ✓ Dynamically optimized resources

Virtualization allows many systems to run on a single physical machine. Each system thinks it is running on its own hardware, with its own resources, yet it is actually running as a virtual server within a larger system. Actual resources, such as storage, networking, and processors can be assigned and shared among the different systems. By consolidating the number of physical servers required to run their operations, organizations can significantly optimize their computing resources, reduce costs, and improve the reliability of their systems.

The Challenges of Securing a Virtual Environment

It's not very often that technology advancements come along that cause a dramatic shift in the fundamental way IT operates. The Internet had a major impact not only in the way we access, store and interact with information, but also the way application architectures and networks were designed to secure this information. Virtualization is having the same profound impact on today's IT environments.

Surprisingly, virtual environments have been around for more than 30 years. IBM® developed the first virtual computing resources with the mainframe and now offers a wide range of virtual servers and architectures. However, as processing power has grown exponentially during the past several years, the true value of virtualization can now be realized by all sizes of organizations. With the advent of VMware®, Parallels®, Xen™ and other virtualization technologies, today's organizations can now take advantage of this virtual machine approach.

Now that virtualization is moving into the mainstream, many organizations are jumping in the water without considering all of the associated security risks. These risks arise from the fact that a new way of doing business is being secured by an old, ill-equipped way of protection. Let's review why the traditional means of network security are introducing significant risks to thousands of organizations.

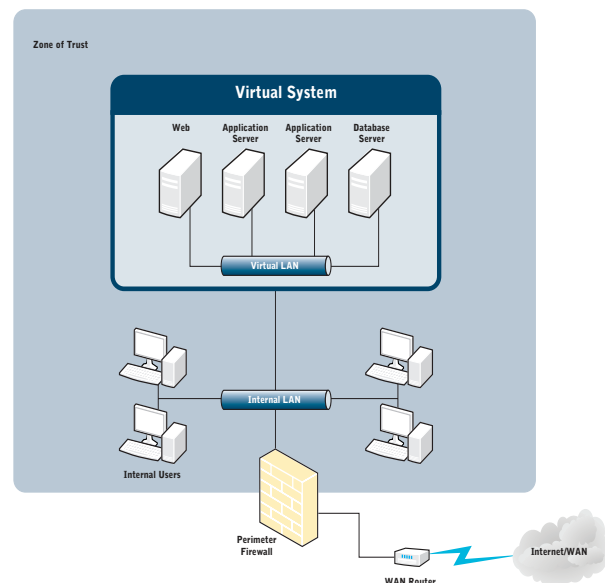
Traditional hardware-based security solutions are rendered useless.

At the core of any virtualization strategy is the removal or reduction of servers and hardware. The majority of traditional security solutions, such as firewalls and intrusion protection systems (IPS) are hardware-based, meaning they reside on an appliance and sit in front of the system they are securing. When the hardware goes away, the security device is only able to throw a blanket of protection over the entire virtual environment, not each individual component.

To further compound the problem, most security solution providers use ASIC-based hardware, which are purpose-built systems designed to do one thing – provide security. For these solutions to work, this chip must be present, and in a true virtual environment, there is no room for extra, single-threaded computer chips.

And finally, since hardware-based security solutions are typically placed at the edge of the environment, an organization is more vulnerable to attacks from the inside, which represents 59 percent of all attacks according to the most recent CSI Survey 2007.

Virtualization Challenge



The fundamental challenge to virtualization is that the various tiers of a typical application architecture are collapsed onto a single virtual system and placed into a single zone of trust with all the internal users. This "flattening" of the architecture exposes the systems to threats from internal users, and removes any ability to defend the most critical assets if a system is compromised.

Traditional security control models are compromised.

Every IT architecture has at least three levels: 1) the back-end database where critical customer or organizational information is stored and the gold-mine most hackers seek to penetrate; 2) the application middleware that enables the end user to perform the desired action on the data and; 3) the front-end Web servers that enable the outside world to interact with the previous two levels.

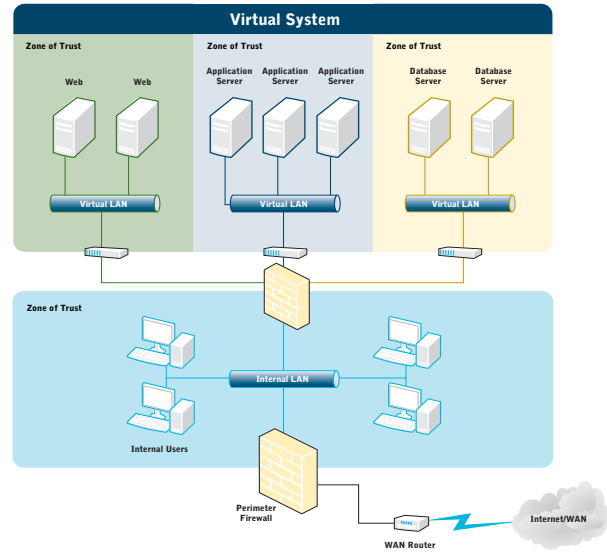
So the application can perform as intended, security devices are typically put in front of the Web server level, and configured to let Web-based traffic come through. However, according to many analyst reports, nearly 80 percent of all security breaches occur from attacks launched through Web-based protocols. When the Web server is compromised in the traditional model, that single server and application is impacted.

In a virtual environment where multiple applications and servers reside on a single server, once the hacker has penetrated this layer, he/she has access to everything on tens or hundreds of systems, applications and databases. In addition, because the traditional controls placed around each application are not present in a virtual environment; an organization's ability to audit who accessed what information, when, is severely compromised. This leads to concerns among auditors and threatens to generate "material weaknesses" in an organization's compliance report.

Traditional segmentation strategies become ineffective.

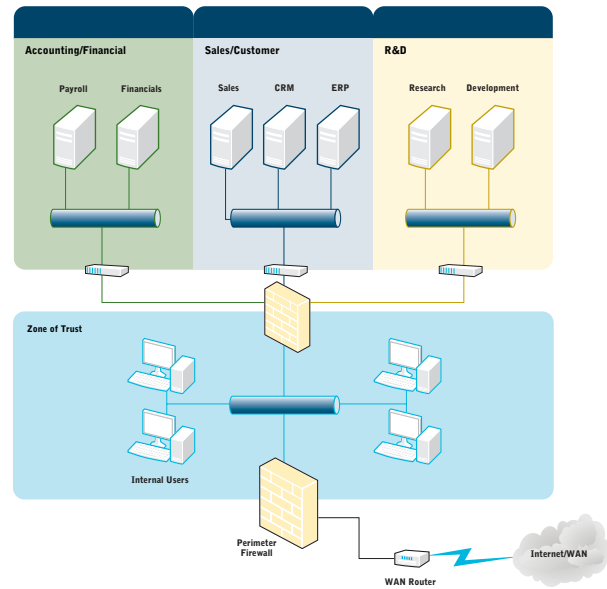
Most IT leaders understand the importance of segmentation, especially those of publicly traded companies that must follow the strict guidelines of Sarbanes-Oxley and other regulatory requirements.

External Firewall Virtualization



Organizations looking to improve virtualization security have had to look at applying existing hardware based products external to the virtual environment. Since the network security components cannot be virtualized, the organization still cannot see into the virtual environment, creating additional challenges to compliance and auditing. In addition, the architecture doesn't leverage the full benefits of virtualization, creating additional costs in complexity, power, cooling and more.

Multiple Virtual Systems



Another approach in an attempt to resolve the virtualization security challenges is to create multiple zones of trust using multiple virtual systems, each virtualizing only one aspect or zone of the architecture. Physical, hardware based appliances provide traditional network security products to protect the systems. But this approach also increases the physical hardware again, which can significantly reduce the return on investment (ROI) that virtualization could have provided. It also increases the complexity, power, cooling and other requirements, including the data center footprint.

Compliance best practices call for the segmentation or “compartmentalization” of key functions such as HR, R&D and Payroll in the IT infrastructure. Many organizations also apply segmentation strategies by creating zones of trust to defend against both internal and external threats. These tactics help eliminate the chance of the wrong people seeing the wrong information.

In virtual environments that are still dependent on legacy security solutions, segmentation becomes more challenging because it requires IT leaders to set up multiple physical servers to run different virtual environments – one for each, such as HR, R&D and Payroll. This situation jeopardizes the number one goal of virtualization – reducing the additional hardware, costs and complexity. In addition, the pooling cost benefits are now compromised, server space remains a problem, and the complexities of the network create an even greater security and availability risk.

Traditional management consoles cannot present the whole picture.

If the hardware-based network security system cannot reside between the virtual servers or within the virtual applications on those servers, the management consoles are not able to collect and provide visibility in to the activity of the virtual environment. For example, legacy security devices that are placed in front of the virtual system cannot report how much network traffic is passing between the virtual systems. They cannot alert the administrator if the physical system is about to max out or if it needs to be re-architected. Without these vital pieces of information, the ability for IT leaders to know when an attack is underway is severely compromised or when capacity is being reached. As a result, the organization is more prone to network outages.

How to Ensure You Have a Virtual-Ready Network Security Solution

Based on the challenges described, we can conclude that software-based security solutions are the only option to protect your virtual IT infrastructure and the benefits expected out of your virtualization initiatives.

Stonesoft, a global organization that has been helping organizations secure information flow with leading edge network security and resilient connectivity solutions for nearly 20 years, offers software-based security solutions that have been proven in virtual environments since 2002. With StoneGate Virtual Security Solutions, organizations can take full advantage of the benefits provided by virtual server technology with the confidence that their networks are secure and readily available.

Ensuring Virtual Environment Security for MSPs

The unprecedented security, ease of use and flexibility that StoneGate solutions offer can help pave the way for conversion to server consolidation for all types of organizations. However, virtualization is particularly attractive for Managed Service Providers (MSPs) with hundreds of customers, firewall clusters and IPS appliances. Instead of having to set up environments with dozens of servers, MSPs can now manage multiple customer environments with just one computer.

To understand if your current solution is virtual-ready, the following questions should be addressed with your network security provider:

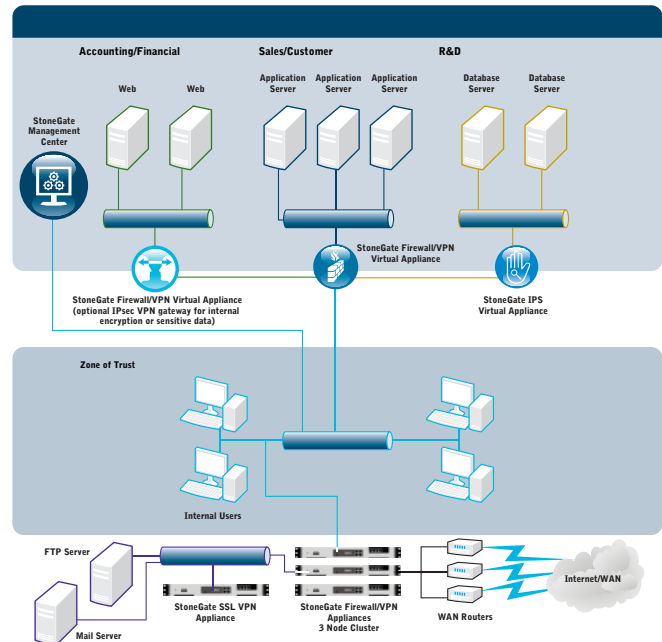
1. Can your current products support a virtual environment? If so, how and what additional components must be purchased to enable the same level of security we currently get with our hardware-based products?

StoneGate solutions are designed from the ground up to be a secure software-based system, which means the ability to operate in a virtual environment is already imbedded. There are no extra costs associated with the StoneGate Virtual Security Solutions. Stonesoft, with more than five years of virtualization experience, is offering a range of VMware certified virtual appliances for firewall/VPN, IPS and SSL VPN.

The StoneGate Firewall/VPN operates under the principle that what is not expressly permitted is denied. The StoneGate IPS allows good traffic, while stopping bad traffic in its tracks. StoneGate provides virtual systems with true stateful inspection firewall/VPN, IPS, and SSL VPN that combines the power of signatures with anomaly analytics. In addition, the StoneGate Firewall/VPN provides multi-layer inspection, where the firewall can function as a basic packet filter or a stateful inspection firewall, or it can perform deeper packet inspection at the application layer – each available on a rule-by-rule basis as selected by the administrator.

Leveraging VMware capabilities, StoneGate Virtual Security Solutions are extremely easy to implement. Since the StoneGate Firewall/VPN, IPS, and SSL VPN include their own integrated and secured operating system, there is no need to install an operating system in the virtual machine first. In addition to simplifying the installation process itself, this integration of the operating system also reduces administrative time, as there is no need to remove extraneous packages, applications, and services, users, groups, and files, verify filesystem permissions, downloads and install appropriate patches or service packs, and all the other work that goes into installing the operating system first.

Virtualization with StoneGate



Stonesoft's StoneGate virtual appliances provide the ability to protect the virtual networks using a virtual firewall/VPN, add additional protection to the database servers with a virtual inline IPS. The StoneGate Management Center, which provides robust, centralized management of all StoneGate components, can also be virtualized, allowing an organization to achieve the full benefits of virtualization while providing the peace of mind that the new environment is secured from internal and external attacks. Both physical and virtual security devices are managed from the same console.

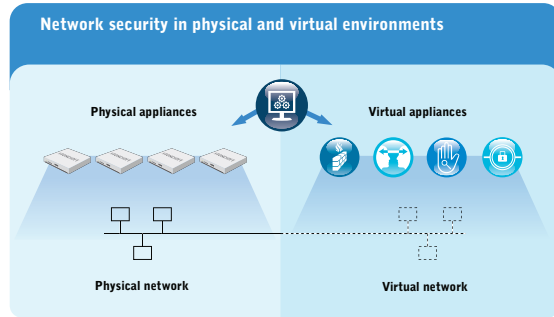
2. Does your product have the ability to monitor detailed activity throughout the virtual and physical environments from a single management console?

The flexibility of the StoneGate architecture to run in both virtual and physical environments further benefits organizations that strive to centrally manage their entire network architecture from one platform. The StoneGate Management Center can manage instances of virtual and physical StoneGate devices, clusters of virtual and physical StoneGate devices, and software-based versions running on standard x86 hardware. It also enables unified policy management for each. Administrators can monitor, control and change software versions for perimeter clusters on x86 servers, StoneGate appliances at remote locations, and VMware virtual machines – all from within the same user interface and the same management center.

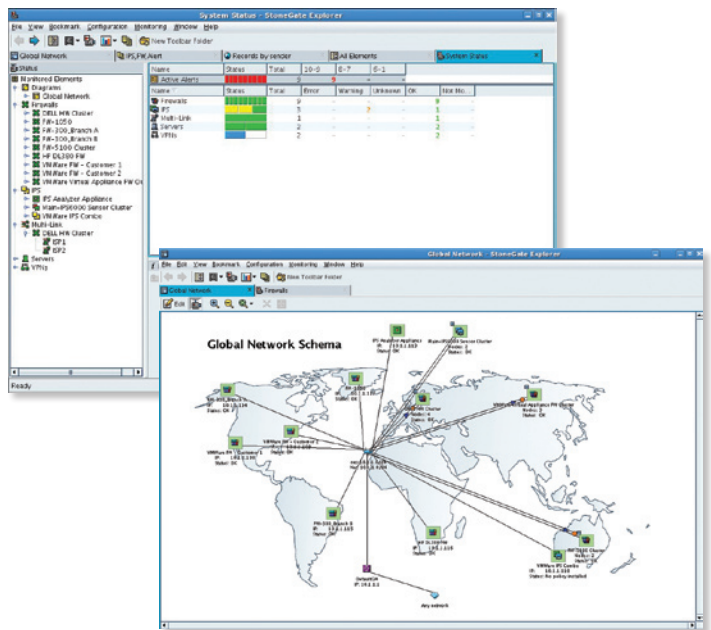
3. How does your product help me mitigate threats in a timely manner throughout my virtual environment?

With advanced logging capabilities and auditing built-in, StoneGate Virtual Security Solutions can further enhance the security of the virtual system by providing logs of traffic in and out of the system, and between virtual machines and networks. Powerful filtering capabilities allow an administrator to quickly isolate the particular entries they are looking for, based on a number of different criteria, such as source or destination IP address, user authentication information, time of day, and more. Auditing features track access to, and modifications of security policies and network elements, including the firewall/VPN and IPS device properties and routing information. Combined with different administrator roles and permissions, an organization can have very strict controls on the security of their systems, both virtual and physical.

StoneGate Virtual Security Solutions



StoneGate Management Center



Conclusion

With virtualization moving into the mainstream, security professionals and IT leaders have an added responsibility of ensuring these new environments are just as secure as the physical systems of the past. This calls for a new look at network security strategies, systems and management/monitoring tools. As one of the only providers of a suite of software-based network security and resilient connectivity solutions, Stonesoft is uniquely positioned to help organizations of all sizes secure their virtual IT infrastructures.

About Stonesoft

Stonesoft Corporation (OMX: SFT1V) is an innovative provider of integrated network security solutions to secure the information flow of distributed organizations. Stonesoft customers include organizations with growing needs requiring advanced network security and always-on connectivity.

StoneGate™ Secure Connectivity Solution unifies firewall, VPN, IPS and SSL VPN blending network security, end-to-end availability and award-winning load balancing into a centrally managed system in physical and virtual environments. The key benefits of StoneGate Secure Connectivity Solution include low TCO, excellent price-performance ratio and high ROI.

StoneGate Management Center provides centralized management for StoneGate Firewall/VPN, IPS and SSL VPN. StoneGate Firewall and IPS work together to provide intelligent defense throughout the organizational network while StoneGate SSL VPN provides enhanced security for mobile and remote use.

Founded in 1990, Stonesoft Corporation is a global company with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com.

About the Author

Mark Boltz is a senior solutions architect for Stonesoft Inc. Boltz has presented at information security conference and trade shows, including classes in virtualization security at SHARE, presentations on dynamic routing protocols at SANS, network security manageability at RSA and voice over IP security at Internet Telephony Conference and Expo. Writing contributions include articles on information security and business continuity planning for the International Legal Technical Association (ILTA), as well as virtualization security for CSO. He has more than 18 years of experience in information technology, including more than a decade focused on information security. Boltz holds certifications as a certified information systems security professional (CISSP), a certified information systems auditor (CISA), and the NSA's IEM in addition to being a certified StoneGate instructor (CSGI). He resides in northern Virginia and is a member of the Information Systems Security Association (ISSA) Northern Virginia chapter, the FBI Infragard program, the League of Professional Systems Administrators (LOPSA), USENIX-SAGE, IEEE Computer Society, the Computer Security Institute (CSI), and ISACA.



STONESOFT



Tel North: 0151 2031400 Tel South: 0118 9071600

Email: Info@castleforce.co.uk Web: www.castleforce.co.uk

IT Security Reseller – Penetration Testing – IT Security Consultancy – IT Security Awareness Training