Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

SPECIAL EDITION

White Paper no. 001 – Price: €5 – October 2008

SPECIAL VIRTUALISATION ISSUE

EXCLUSIVE INTERVIEW Léonard Dahan

STONESOFT

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

STONESOFT

White Paper no. 001 – October 2008
Special **Virtualisation Issue**

QUARTERLY REVIEW
White Paper no. 001 – Special Edition
www.globalsecuritymag.fr and
www.globalsecuritymag.com
ISSN: 1961 – 795X
Legal deposit: upon publication
Published by SIMP
RCS Nanterre 339 849 648
17 avenue Marcelin Berthelot
92320 Châtillon
Tel.: +33 1 40 92 05 55
Fax.: +33 1 46 56 20 91e-mail :
marc.jacob@globalsecuritymag.com

EDITORIAL STAFF
Publication Editor:
Marc Brami
Editor in Chief:
Marc Jacob
Assistant:
Sylvie Levy
Technical Manager
Raquel Ouakil
Photos
Stonesoft
Scientific Committee:
Pierre Bagot, Francis Bruckmann
Éric Doyen, François Guillot
Mauro Israël, Olivier Iteanu,
Dominique Jouniot
Patrick Langrand, Yves Maquet
Michel Van Den Berghe,
Thierry Ramard, Hervé Schauer
Wayne Sutton, Catherine Gabay
Zbigniew Kostur

ADVERTISING
SIM Publicité
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : ipsimp@free.fr

DESKTOP PUBLISHING
Imadjinn sarl
Tél. : 02 51 53 01 46
e-mail : pao-imadjinn@orange.fr

PRINTING
Imprimerie Hauguel
8-14 villa Léger
92240 Malakoff
Tél. 01 41 17 44 00
Fax 01 41 17 44 09
e-mail : info@imprimerie-hauguel.fr

SUBSCRIPTION
Price of the Special Edition:
€5 including tax (VAT 19.60%)
Annual magazine subscription:
€50 including tax (VAT 19.60%)

Exclusive Interview:
Léonard Dahan **STONESOFT** **P. 13**

CONTENTS

EDITORIAL

Virtualisation: is it time to question security schemes?

It is not very often that technology advancements cause a dramatic shift in the fundamental way in which IT operates. The Internet had a major impact not only on the way in which we access, store and interact with information, but also on how application architectures and networks were designed to secure this information. Virtualisation 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 virtualisation can now be realised by all sizes of organisations. With the advent of VMware®, Parallels®, Xen™ and other virtualisation technologies, today's organisations can now take advantage of this virtual machine approach.

Virtualisation has therefore taken the IT industry by storm. According to a recent InformationWeek poll, 70 percent of the respondents reported that they are running at least one virtual server, while less than 12 percent have a security strategy tailored to their virtual environment. In fact, as with the advent of any new technology, security is all too often the poor relation.

Yet risks exist and must not be overlooked. These threats often arise from the fact that these architectures are being secured using traditional methods that rely on equipment ill-suited to this new concept. Therefore, information systems security managers, information systems managers, etc. must rethink their security architecture and adapt it to virtualisation in order to reap the full benefits of this technology.

Marc Jacob

STONESOFT

VIRTUAL ARCHITECTURE SECURITY: A NEW PRIORITY FOR IT DEPARTMENTS

Interview with Klaus Majewski, Marketing VP at Stonesoft

According to Klaus Majewski, Marketing VP at Stonesoft, virtual architectures will be implemented to virtualise entire networks rather than simply for server consolidation. This means that security will become a top priority for all IT departments. The StoneGate Virtual solution is currently the preferred security solution for VMware architectures, but could also serve the same role for Microsoft Hyper-V architectures if the market so decides.

Global Securtiy Mag : What is your vision of the virtualisation market in the world and in particular in Europe?

Klaus Majewski : I see the virtualisation market as a rapidly growing market, even if the economy were to slow down, because it creates tangible savings for companies. It saves energy and floor space and makes companies independent from hardware manufacturers. Virtualisation allows companies to switch hardware platforms as they like and will not affect their production, because it hides the hardware beneath it. Virtualisation makes it easy to adapt to economic and business changes. You can add applications when you need them and remove them when you no longer need them. Virtualisation makes companies truly adaptive and agile. My vision is that within a year or two, virtualisation will evole from pure server consolidation to virtualising whole networks. People will see that it is essential to have security inside the virtual environment so that they can have protection similar to that of a physical environment, such as server segmentation, separate trust zones and inspection of the virtual traffic. Virtualisation will add its own peculiarities to this, such as the movement of virtual servers, stale virtual appliance images and so on, but these can be taken care of. People who are now implementing virtualisation are focusing primarily on server consolidation and security is not high on their priority list - and that is evident.

Although Microsoft shows promise in the area of virtualisation, only customers will be able to decide on its value.

Global Securtiy Mag : Today, Stonesoft provides security solutions for the VMware ESX platform. What are you planning for other platforms (Citrix XEN, Microsoft HyperV, etc.)? Why?

Klaus Majewski : We are currently providing Virtual Firewall/VPN and Virtual IPS solutions for the VMware ESX platform because it is a clear market leader and currently has most mature virtual environment management tools available. We are also looking very closely into Microsoft HyperV, because it has enough potential to rival VMware's market position in the future. Microsoft has shown some promise in integrating its own management tools to manage virtual environments. The future will show how well customers value them. From Stonesoft's point of view, it does not take much effort to port our Virtual Solutions to HyperV, so we will do it if the Microsoft virtual environment proves to be a viable solution for our customers.

Using physical appliances to inspect the traffic on virtual environments is counter-productive.

Global Securtiy Mag : What do you expect from the VMware VMsafe Security Technology Partnership? What kinds of benefits could we expect from your VMsafe compliant solutions?

Klaus Majewski : VMsafe gives more visibility to the Virtual Machines and Hypervisor, but from the network security point of view I do not expect great new things. VMsafe allows virtual security appliances to inspect traffic before it arrives at the virtual applications and provides access to Vmware centralised management tools for virtual environments. StoneGate products can already now inspect all traffic before it arrives at the virtual applications and we have great centralized management for all elements of our virtual security solutions.

There has been a lot of fuss about using hardware security appliances to inspect virtual environment traffic through VMsafe. It might be a good fit for some customers, but I see it as a bit counterproductive with regard to virtualisation. Now we are again adding new hardware appliances, although the main idea of virtualisation was to reduce the amount of hardware. I see end-point products like anti-virus products benefiting more from the VMsafe technology than network security products. ■■■

STONESOFT

VIRTUALISATION AND SECURITY, AN ESSENTIAL TWOSOME

Interview with Lionel Cavalliere, VMware

Virtualisation has become an increasingly necessary technology. It provides significant cost reductions by lowering the number of physical machines and through subsequent savings in areas such as energy, implementation time, etc. In terms of security, elimination of the management console with the ESXi hypervisor (free) and the VMsafe program are clear advantages. Today, VMware has established itself as an OS supplier committed to offering greater security, says Lionel Cavalliere, VMware's EMEA Product Marketing Manager.

Global Security Mag: What is your view of the worldwide and European virtualisation market?

Lionel Cavalliere: The virtualisation market is continuously growing. According to IDC, it is expected to reach $3.6 billion in 2009 and will exceed $5 billion by 2012. Europe currently accounts for 29% of this figure and this percentage should increase significantly in the future. The market is divided into two parts: server virtualisation and workstation virtualisation. Today, growth is mainly driven by server virtualisation for data centres thanks to a fast ROI of 6 to 8 months. In fact, the primary use is server consolidation, which helps reduce the number of platforms and energy consumption. The workstation segment is currently taking off and has great potential.

GS Mag: How do you see your products evolving in the coming years?

Lionel Cavalliere: We have positioned ourselves as an OS supplier for data centres: our Virtual Data Center OS (VDC-OS) uses the "ESX Server" hypervisor implemented on the data centre's x86 platforms. This base offers the ability to unify material resources and provide application services natively. For example, our solutions allow users to enjoy high availability and fault tolerance through a simple mouse click.

GS Mag: How did you secure your hypervisor?

Lionel Cavalliere: We reduced the exposure surface by separating the management console from the hypervisor itself with "ESXi Server". As a result, this "light" hypervisor does not take up more than 32 MB on the drive while still being administrable. The management console was the main source of vulnerability for which we had to provide regular security patches to our customers. The ESXi approach is unique in the market and ensures a very high level of native security.

GS Mag: What is your strategy with your security publisher partners?

Lionel Cavalliere: We have developed the VMsafe program. Thanks to the special position of the hypervisor, which fits between the hardware and the virtual machines, VMsafe offers a specific API that provides access to all the instructions executed in the virtual machines, their context, network exchanges, etc. This allows security publishers such as Stonesoft to offer their specific solutions, which are seamlessly integrated into our virtualised environments. A dedicated virtual machine then handles the security requirement without having to deploy agents individually on all the environment's virtual machines, as is currently the case.

GS Mag: What are the expected benefits of the VMsafe technology program?

Lionel Cavalliere: The benefit for our end customers is that they only need to update one virtual appliance for a given security requirement (antivirus, firewall, etc.) to protect all their equipment. Our approach disregards the hardware, which makes deployments much easier.

GS Mag: What is your message to information systems security managers?

Lionel Cavalliere: Virtualisation offers the best deployment platform for x86 applications, with faster, easier implementation. Our VMsafe program and its partners provide the security management that is vital to corporate environments. This approach bolsters our positioning and is an added plus for our customers. ■■■

STONESOFT

FROM ORGANISATION TO TECHNIQUE

THREE QUESTIONS FOR NICOLAS MONIER

Pre Sales Manager at DCI

Global Security Mag: What are the threats linked to virtual environments?

Nicolas Monier : First of all, a number of widely held views regarding virtual environment security should be discarded.
❶ A system does not become more vulnerable just because it is virtualised. It simply continues to have its usual flaws. It may be more sensitive to denial of service if the resources allocated are reduced to the minimum required.
❷ Even if there are no limits to hackers' ingenuity, and if we assume that one of them takes control of one of your virtual machines, it is unlikely that he or she will manage to reach the virtualisation system itself through a bounce attack. To mitigate such a threat, the administrator simply needs to ensure that a virtual host is not authorised to access a physical resource.

The risk lies elsewhere. The fact is that there are seldom as many physical interfaces as there are virtual hosts on a hardware platform. This therefore means creating hubs or virtual switches to which several virtual hosts are connected. A physical interface that allows the hosts to communicate with the outside world is then associated with each of these switches.

As a result, virtual networks are created which completely circumvent the segmentation rules applicable at the company:
- On the one hand, the hosts connected to a particular virtual switch must sometimes be distributed over the different segments (since they correspond to different security levels).
- On the other hand, depending on how these switches are configured, it is sometimes possible to move from one virtual segment to another.

GS Mag: What security strategies do you recommend to your customers?

Nicolas Monier : The first recommendation that I would make is a strictly organisational one. It is becoming clear that the physical network infrastructure will lose ground in the face of virtual switches (the manufacturer Cisco is already working at developing a virtual Catalyst switch). The decision as to who will be responsible for these virtual infrastructures must therefore be made quickly. Their management can be assigned to the "network" department, in which case the latter will need to adapt its security policy to this new environment. The decision can also be made to have the "systems" department be solely responsible for virtualisation, in which case "systems" engineers must be made aware of network security issues.

The second recommendation is to group virtual hosts by level of exposure to attacks and define a virtual switch for each level. It is also important to assign one VLAN (minimum) to each switch in order to protect virtual inter-switch security when network traffic moves onto the physical infrastructure (in which case the traffic is tagged and can therefore not re-enter the virtual system directly).

On the basis of these prerequisites, two options are available:
- Either traffic between virtual segments is routed and filtered via a physical firewall. In most cases, this means severe limitations in terms of bandwidth.
- Or traffic between virtual segments is routed and filtered via a virtual firewall, in which case network flow does not systematically leave the virtual infrastructure and high network performance can therefore be achieved. Such firewalls exist. A case in point is Stonesoft, a publisher that recently developed a firewall and a virtual IPS certified by VMware.

GS Mag: What projects are you currently seeing in this field (project size and types of enterprises)?

Nicolas Monier : Today, most requests are geared toward business recovery plans. The goal is to take advantage of virtualisation and the possibilities it offers in terms of duplicating systems in order to facilitate business recovery procedures after a disaster.
Most of the time, these virtualisation projects are combined with a storage bay acquisition project. In point of fact, the PC hardware platform(s) will support 4 to 20 virtual hosts and will not be able to take on the necessary storage capacity.

In most cases, virtualised servers include both internal business applications and Web access gateways. Indeed, these gateways are often included in business recovery plans. In addition, the systems engineer is often mindful of security issues and attempts to isolate the systems that communicate with the Internet in a different IP subnetwork (although this protective measure is not effective, it does show that "Systems" administrators are aware of security problems).

From an economic standpoint, the most striking phenomenon is the market's shift from large enterprises toward large SMEs. We are currently receiving requests from organisations with 1,000 to 3,000 workstations who wish to virtualise 10 to 50 critical servers and have budgets of €30,000 to €200,000.

STONESOFT

SYSTEM, NETWORK AND SECURITY TEAMS MUST WORK TOGETHER

By Laurent Boutet, Stonesoft

Virtual environments have become very popular among companies of all sizes. It is true that this technology offers numerous advantages in terms of productivity, cost, and operation. However, all technological innovations, and especially those met with great enthusiasm, shift or create security problems that must not be overlooked. Laurent Boutet, Pre-Sales Engineer at Stonesoft France, believes that the main threat to virtualisation is users' ignorance of potential risks. In his opinion, one of the key points of these implementations is collaboration among the various teams involved: system, network, and security.

The main problem that we generally encounter is the company's ignorance of the risks related to flexible use and production of virtual environments. These environments are often viewed as a system function, whereas network and security teams need to be fully involved from the design phase. Virtual architectures are, in fact, based on virtual networks that require the same security strategies.

Unfortunately, a virtual environment is often treated as a black box. As a result, security and the network go only as far as the periphery of these architectures. It is there that we have seen some cases of serious segmentation errors. Most problems result from an incorrect configuration or, usage, not the technology itself.

Securing virtual architectures requires collaboration among the network, security and system teams

The first step must be an organisational one – close collaboration among the network, system and security teams is essential. Virtual architectures must be viewed in the same way as traditional environments, with the same security, monitoring, audit, control and partitioning strategies. However, they must not stop at a server or blades, but go much deeper into the virtual architecture.

System Environments: virtual machines must be secured in the same way as physical machines

Each virtual machine must be treated as a physical machine. This means that the same approach must be taken as for a traditional enterprise server, from tightening up the OS to anti-virus software and access strategies.

The problem lies in the ease with which machine clones can be implemented and applications duplicated. Being content with cloning a machine that was tightened up or patched three years ago must be avoided at all costs. Moreover, creating a large number of R&D, pre-production and production environments and, at times, putting them within close reach, can prove catastrophic. At times, machines, which have been forgotten about after a few days of testing remain active without any management. To offset the speed and ease with which an environment is set up, a strict procedure must be followed to ensure that the security of this future platform is properly implemented.

The hypervisor on which the entire system is built must also be tightened. These are, by their very nature, highly optimised and tight systems; however, many elements must be controlled and somewhat traditional rules must be implemented, such as separating maintenance flows from production flows, protecting remote access, authentication, password management policies, limiting file access, and so on. It is also important to disable certain functionalities specific to these environments for production servers: disabling the copy and paste feature between the host system and the console is a perfect example of this. Finally, for complete control, the architecture must be protected by physical Firewall and IPS equipment and, in particular, the flows related to operating these environments.

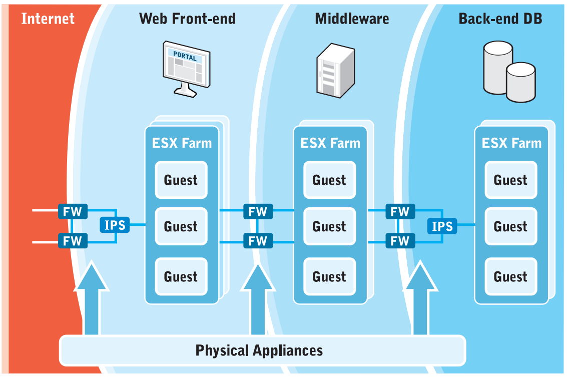
Network security: Three segmentation strategies for virtual environments

There are three possible strategies for implementing segmentation between the various zones of virtual servers.

The first entails consolidating a series of servers belonging to a given zone within a single virtual environment dedicated to this zone. Each zone retains one machine that is on its own, which ensures complete segmentation by the existing physical Firewall and IPS equipment.

Strategy 1

Retrofitting Hardware for Virtual Environments

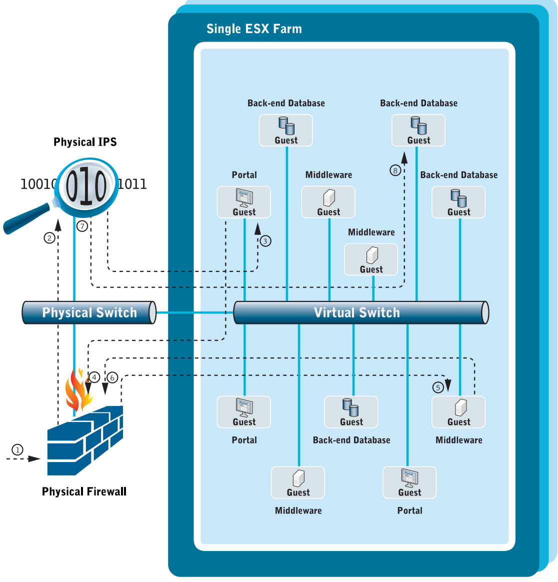


This is often the first approach to server consolidation. However, it does not provide the optimisation expected from virtualisation since there will be as many physical machines as there are different zones to protect.

From a security standpoint, there seems to be little change from before; however, it is no longer possible to easily audit, communications within these systems, for example with an IPS. The result will therefore be a loss of visibility. In addition, some administrators take the liberty of creating incorrectly segmented subzones since it is faster and easier to do so from a production standpoint.

Strategy 2

VLAN Tagging

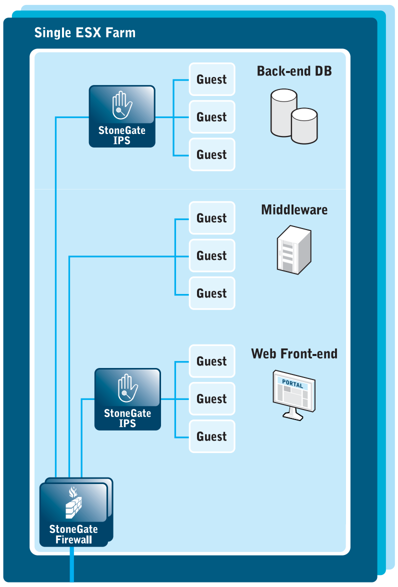


The second strategy involves combining all the zones in the same virtual environment. In this case, unlike in the previous one, the resources are indeed optimised; however, various zones must then be properly segmented within the virtual system and related to the physical network by dedicated links. VLANs will be used intensively; however, the drawback is a loss of visibility in the virtual systems' internal communications and, more importantly, an error of any kind can quickly cause the segmentations to be bypassed. In addition, limitations on the number of interfaces can quickly make this type of architecture difficult.

The third strategy entails combining segmentation and network security in the virtual environment. Virtual Firewalls and IPS, which have the same capabilities as their physical counterparts, are then used. Here again, resources are fully optimised; however, it is essential to properly segment the zones and build the virtual network architecture. Being inside the system itself helps to simplify this process and even deploy double bastion strategies, for example, or strategies involving monitoring of inter-server communication by IPS. However, this strategy still requires that physical security equipment is used to protect the physical equipment.

Strategy 3

StoneGate Software-based Virtual Architecture



A centralised console of the security elements which provides complete visibility of the physical and virtual environment is the key to successfully achieving the proper configuration, monitoring and auditing of these environments. Indeed, client architectures will require a combination of these three strategies, which could mean a relatively large number of nodes that will need to be managed with considerable consistency. ■ ■ ■

STONESOFT

SECURE VIRTUAL ARCHITECTURES WITH COMPLETE FLEXIBILITY

Interview with Léonard Dahan, Stonesoft

Léonard Dahan has been working as the Manager of Stonesoft's France and Benelux subsidiary for the past three years. His development strategy is to maintain close, long-term relationships with his partners, employees, and customers. Today, Stonesoft is one of the few vendors that offer security solutions for virtualised architectures central to these environments. These appliances are sold in the form of licences in order to offer customers greater flexibility.

Global Security Mag: What are your roles and responsibilities at Stonesoft?

Léonard Dahan : I am responsible for Stonesoft's France and Benelux subsidiary. In addition to the business and organisational aspects of my position, I am thoroughly committed to developing quality personal relationships with my employees as well as with our customers and partners. These are indeed complex issues and time is needed to create a climate of trust and to ensure lasting relationships and partnerships. I am fortunate to be working for a Finnish company where human values are taken into account. My role, therefore, is to define a marketing strategy that is in line with my parent company's objectives and respects our corporate culture. Stonesoft's aim is to develop long-term relationships and protect the interests of its customers and partners.

More than five years' experience in securing virtual architectures

GS Mag: Can you describe your virtual architecture security solutions? Can these current products support a virtual environment? If so, how does one proceed and what additional components must be purchased to enable the same level of security that current hardware-based products offer?

Léonard Dahan : StoneGate solutions are designed to be secure software-based systems throughout the communication chain, which means that the ability to operate in a virtual environment is already built in. There are no extra costs associated with the solutions for a virtual environment. Stonesoft, with more than five years of virtualisation experience, offers a range of VMware-certified StoneGate virtual appliances for firewall/ VPN, IPS, and SSL VPN.

The StoneGate Firewall/VPN solution operates according to a simple principle: anything that is not expressly permitted is denied. The StoneGate IPS solution allows normal traffic, while stopping harmful traffic in its tracks. StoneGate provides virtual systems with a true stateful inspection Firewall, VPN, IPS and SSL VPN, which combine the power of signatures with anomaly analytics. In addition, StoneGate Firewall/VPN includes a multi-layer inspection function, where the firewall can either function as a basic packet filter or as a stateful inspection firewall, or perform deeper packet inspection at the application layer. Each option is available on a case-by-case basis as selected by the administrator.

Leveraging VMware capabilities, StoneGate virtual appliances are extremely easy to implement.
Since the StoneGate Firewall/VPN, IPS, and SSL VPN solutions come with their own integrated and secured operating system, there is no need to install this in advance in the virtual machine. This integration of the operating system not only simplifies the installation

process itself but also reduces administrative time. It eliminates all the tasks associated with installing the operating system, such as deleting extraneous software packages, applications, services, users, groups and files, verifying file system permissions and downloading and installing patches and service packs.

Stonesoft's StoneGate virtual appliances provide the ability to protect virtual networks using a virtual Firewall/VPN and add additional protection for database servers via a virtual inline IPS. The StoneGate Management Center (SMC), which provides robust, centralised management of all StoneGate components, can also be virtualised, allowing the organisation to achieve the full benefits of virtualisation while providing assurance that the new environment is secured from internal and external attacks. Both physical and virtual security devices are managed from the same console.

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

Léonard Dahan : The flexibility of the StoneGate architecture, which allows it to run in both virtual and physical environments, further benefits organisations that wish to manage their entire network centrally from one platform. The StoneGate Management Center can manage instances of virtual and physical StoneGate devices, clusters of virtual and physical StoneGate devices, as well as software-based versions running on standard x86 hardware. It also enables a 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 centre.

StoneGate enhances virtual system security by providing traffic logs and filtering and audit capabilities

GS Mag: How does your product help me mitigate threats in a timely manner throughout my virtual environment?

Léonard Dahan : Thanks to its built-in logging and audit capabilities, StoneGate can further enhance the security of the virtual system by providing logs of traffic in and out of the system and between the virtual machines and networks. Filtering capabilities allow administrators to quickly isolate the entries they are looking for based on a number of criteria, such as source or destination IP address, user authentication information, time of day, and more. Audit features track access and changes to security policies and network elements, including the Firewall/VPN and IPS device properties and routing information. Combined with various administrator roles and permissions, these functions allow the organisation to have very strict control over the security of its systems, both virtual and physical.

Moving from the world of hardware to a world of service

GS Mag: Can you describe your marketing strategy?

Léonard Dahan : Stonesoft is strengthening its position as a pioneer in the Security and High Availability market. We are currently in our 5th half-year period of double-digit growth. The quality of our R&D department is enabling us to break new ground and announce innovative leading-edge solutions. In keeping with the latest developments, we have recently received the VMware Virtual Appliance certification for our FW and IPS technologies, which makes us the first vendor to offer a complete certified security solution (FW and IPS) for VMware ESX environments.
This new market must be part of our enterprise development and we need to adapt our organisation accordingly. With these solutions, we are moving from the world of hardware to one of service.
With a StoneGate Virtual FW licence at €699 and a StoneGate Virtual IPS licence at €995 in the form of an annual licence fee, we will be making several changes in our Distribution organisation in France and Benelux.
In addition, given the large number and diversity of VMware resellers in France and Benelux as well as our economic model, emphasis will be placed on a two-tier model in the coming months.
On a practical level, in order to reach a volume market, we have developed innovative marketing tools in the form of videos to promote our expertise among specialised virtualisation resellers as well as users.

Our goal is to develop a relationship of trust with our customers

GS Mag: What is your message to information systems security managers?

Léonard Dahan : With virtualisation moving into the mainstream, security professionals and IT managers have an added responsibility of ensuring that these new environments are just as secure as the physical systems of the past. They must therefore take a new look at network security strategies, systems and management/monitoring tools. Stonesoft is one of the few companies to offer a suite of network security and business continuity software solutions. Since our role is to develop long-term relationships and protect the interests of our customers and partners, the team at Stonesoft France and Benelux is always ready to contribute their expertise in securing virtual infrastructures to explore the architectures of tomorrow. ■ ■ ■

INTEGRATION OF STONESOFT FIREWALLS UNDER VMWARE OFFERS A DECIDED ADVANTAGE!

Interview with Frédéric Le Guillou, Chief Technology Officer (CTO)

For many years, Cegedim has offered hosted solutions using an ASP model and, in some cases, in SaaS mode. The company has long placed its bets on virtualisation, deploying only virtual architectures at data centres. For Frédéric Le Guillou, Chief Technology Officer at Cegedim Group, the integration of Stonesoft firewalls under VMware offers a decided advantage which should allow the company to manage the integration of its worldwide IT systems with more flexibility.

Global Security Mag: Can you tell us about Cegedim, as well as your roles and responsibilities at the company?

Frédéric Le Guillou: Cegedim, the world leader in CRM for the health care industry, designs exclusive databases and high value-added software solutions. It demonstrates its expertise in four sectors:

- CRM and strategic data, including services for pharmaceutical laboratories;
- health care professionals and pharmacists;
- health care insurance services for health insurance professionals;
- technologies and services for businesses in all sectors.

For many years, Cegedim has offered hosted solutions for all four sectors using an ASP model and, in some cases, in SaaS mode. This has enabled the company to develop expertise in these areas built on a high-level hosting base with worldwide coverage.

My position at Cegedim is that of Chief Technology Officer (CTO) Cegedim Group and my main responsibilities include developing and defining the strategy of the hosting base in line with the requirements of our business units.

GS Mag: Which IT environments are you responsible for?

Frédéric Le Guillou: The Cegedim Group's IT department serves the company's internal IT needs and develops solutions for our customers via two IT services catalogues built on a common base. Cegedim's teams manage all the technical and logistical areas of the IT services offering, be they the physical infrastructures of the data centres, the server platforms, or its own private global telecommunications network.

Cegedim has always placed its bets on virtualisation

GS Mag: For what types of applications and customers have you deployed virtualised architectures?

Frédéric Le Guillou: Cegedim has always placed its bets on virtualisation. It began with three zSeries mainframes and extended this concept to include the Open world and AIX. Cegedim naturally turned to VMware in 2004, adopting the ESX product. Today, hundreds of virtual machines are deployed, half of which are used on behalf of our customers, to host proprietary and legacy solutions. The internal IT department has pioneered the use of virtualisation for all types of environments, from development to production. Cegedim has true expertise in virtualisation and in the operational organisation crucial for its maintenance.

GS Mag: What is your current strategy for securing your virtualised architectures?

Frédéric Le Guillou: Our virtualisation strategy involves three phases:
- implementation of virtual server platforms at data centres, already completed;
- virtualisation of the network infrastructure and firewalls, in the process of being finalised;
- complete virtualisation, provision of a virtual data centre, scheduled for 2009.

Virtual and physical architectures enjoy the same overall security mechanism: filtering and routing of flows by clusters of StoneGate appliances. The security policies of the physical network and the virtual networks are consistent and their management is centralised.

Combining virtualisation with Stonesoft appliances allows us to consolidate our servers safely and securely

GS Mag: As you consolidate your servers, what are your new requirements in terms of security?

Frédéric Le Guillou: We are currently merging the hosting infrastructures of our former competitor, on the one hand, and the internal IT infrastructure, including both companies' networks, on the other hand.
The merger strategy must address extreme requirements in terms of business continuity while maintaining the level of security defined in the Cegedim Group's security policy and adhering to the guidelines for optimising the IT master plan.
Virtualisation of the environments helps us attain these objectives and enables us to avoid nearly insurmountable constraints in this context.
By deploying a StoneGate solution on a virtual base, it's easy for us to provide our subsidiaries with a virtual server that includes all that is needed to access the group's resources while also complying with its security policy. The firewall is integrated into the current equipment and is centrally managed.

We should not have any real problems deploying VMware in conjunction with StoneGate

GS Mag: In terms of organisation, what consequences do you foresee arising during deployment of these systems?

Frédéric Le Guillou: We do not anticipate any real problems with this deployment, which is in line with our virtualisation technology implementation strategy put in place over four years ago.
Today, VMware is fully under control and we have used the StoneGate firewall for more than six years under very severe business continuity conditions and with very complex filtering rules.
Recently, we successfully completed a worldwide migration of the StoneGate software solution onto FW-5000 appliances. Implementing the same solution, managed by the same management console, at a data centre and at our subsidiaries' remote sites is already a reality at Cegedim. It allows real productivity gains and fits perfectly into our "follow the sun" support philosophy.

Our secure virtual architecture will allow us to manage our company's global IT integration

GS Mag: What do you expect from this deployment?

Frédéric Le Guillou: The integration of Stonesoft firewalls under VMware offers a decided advantage, as it will allow us to manage Cegedim's worldwide IT integration with more flexibility.
One of the ways in which Cegedim grows is by acquisition and last year the company bought out its chief competitor. Integrating the two worldwide IT infrastructures is a long, complex process, mainly because of the need to unify security practices. With a virtual solution that includes the group firewall solution, we can implement a uniform security policy less expensively. The integration process becomes more fluid.

From a business standpoint, the solution is particularly advantageous because it allows us to expand our hosting services and offer a customer a dedicated comprehensive solution (virtual network and server resources). This solution is similar to that of a virtual data centre that can be managed by our customers. ■ ■ ■

SECURE VIRTUALISATION WITH STONEGATE VIRTUAL SOLUTIONS

Interview with Frédéric Ramage, Thales

THALES

Frédéric Ramage is responsible for new project and new technology integration at Thales' Elancourt Service Centre. His company began to virtualise its production environments in 2006 in an effort to reduce its deployment costs, among other things. To secure his virtual environment, Frédéric Ramage opted for the StoneGate Virtual solution, which meets his requirements in terms of unencrypted flow analysis, licensing costs and load balancing.

Global Security Mag: Can you tell us about Thales and your roles and responsibilities at the company?

Frédéric Ramage: Thales is a world leader in mission-critical systems. I am part of Thales' "mission-critical information systems" activity, which provides consulting, integration and facilities management services to its customers in the industrial, financial, transport and public administration sectors.
I am responsible for new project and new technology integration at Thales' Elancourt Service Centre.

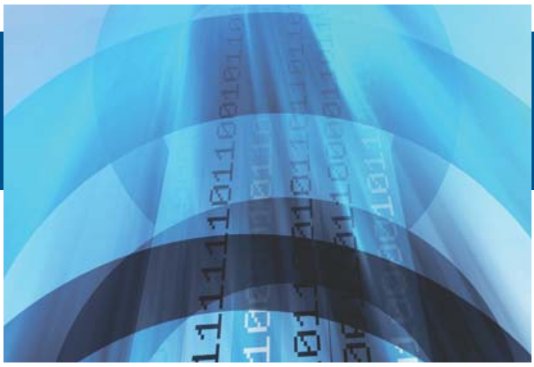
GS Mag: What were the circumstances that prompted you to choose a virtualised architecture?

Frédéric Ramage: As for many services companies, keeping costs down is an ongoing challenge. In 2006, Thales began to virtualise its production environments. This provides an excellent solution for deploying our services and keeping them in operating condition under very competitive terms.

In fact, virtualising a portion of the information system gives us a great deal of flexibility, enabling us to adjust each environment's capacity less expensively based on requirements. It is very easy for us to add new servers and new firewalls. In addition, facilities infrastructure costs (energy, cooling, etc.) are optimised.

GS Mag: What made you choose virtualisation?

Frédéric Ramage: At present, virtualisation is widely used at Thales.
Our architecture required a small investment with the possibility of significant growth. At the same time, we



had to be able to pool our environment in order to accommodate other customers within this physical platform. The target environment was an excellent candidate for virtualisation because it required few resources (processor, memory, IO).

GS Mag: What were your requirements in terms of securing these infrastructures and why did you opt for the Stonesoft solution?

Frédéric Ramage: Our requirements were simple:
secure our platform with stateful firewalls and be able to analyse unencrypted flows (http);
hold down costs: the licensing mechanism of StoneGate Virtual Solutions lends itself to this since it is done annually, without any bandwidth limitation or other options that have a financial impact on the "natural" evolution of the architectures;
have a simple, efficient load balancer: this functionality is built into the Stonesoft solution, making it possible to balance the load on a server farm and ensure high availability.

The new ESX Server drivers should result in better performance

GS Mag: What problems did you encounter when deploying your security solution?

Frédéric Ramage: First of all, we discovered a limitation with the VMware servers: a virtual machine under ESX Server 3.5 supports only four network interfaces, which fell short of our interconnection requirements. We had to adapt our architecture to this constraint. (However, it appears that an extension to six interfaces is scheduled for late 2008).
We also found that network performance on a virtual server is poor (300Mbit/s maximum speed per interface) compared with the capacities of physical firewalls on the market. This may be due to the fact that the use of virtual network cards consumes CPU time by running operations that are normally executed by ASICs on the network cards of physical firewalls. In addition, using virtual switches on an ESX is a limiting factor because of its CPU consumption. However, the new ESX Server drivers (Enhanced VMXnet) should result in better performance.

The integration of virtual IPS is a big plus

GS Mag: Having used Stonesoft solutions for six months now, what lessons have you learned?

Frédéric Ramage: Firewall virtualisation within a VMware ESX Server architecture is still new but promising. We have not had any major problems.
Segmentation of administration rights is necessary to ensure satisfactory business security, whereas, by default, on an ESX server, the administrator can do anything.
I think that Stonesoft has developed an innovative solution and must keep making improvements to what is increasingly the core of our environments.
The integration of virtual IPS is a big plus. Deploying and moving a sensor from one environment to another becomes very easy with virtualisation (template, virtual network connections, etc.). It is a significant step forward!

GS Mag: What improvements would you like to see in Stonesoft products?

Frédéric Ramage: Version 4.3 of the SMC, as well as the engines in 4.2.4 (to date), have brought many improvements. I think that A-A clustering and tagging must be officially supported in the near future, even if they run perfectly*.

A full test period is needed before moving to production

GS Mag: What advice would you give your fellow information systems security managers to help them deploy virtualised architectures?

Frédéric Ramage: That's a hard question…
Virtualisation is both a godsend and a trap. I think that, before virtualising, you really need to know your information system fully and have clear objectives.

A period of testing, benchmarking and qualification of the future architecture is necessary before moving to production. Because virtualisation has so much potential, you must carefully consider the possibilities it offers.
If you have no experience, getting outside advice can help you avoid the usual errors and deploy more quickly. ■ ■ ■

***Editor's note:** This and other functionality has been supported since late summer when Stonesoft received its VMware Virtual Appliance certification.

STONESOFT
AT A GLANCE

StoneGate SSL VPN

Secure mobile and remote access at any time, with any device

StoneGate Secure Mobile Connectivity Solution with SSL VPN offers flexible, secure and cost-effective remote access to enterprise information, applications and networking resources. Moreover, the solution provides Network Access Control (NAC) where it is most needed, for mobile network access originating from unidentified devices.

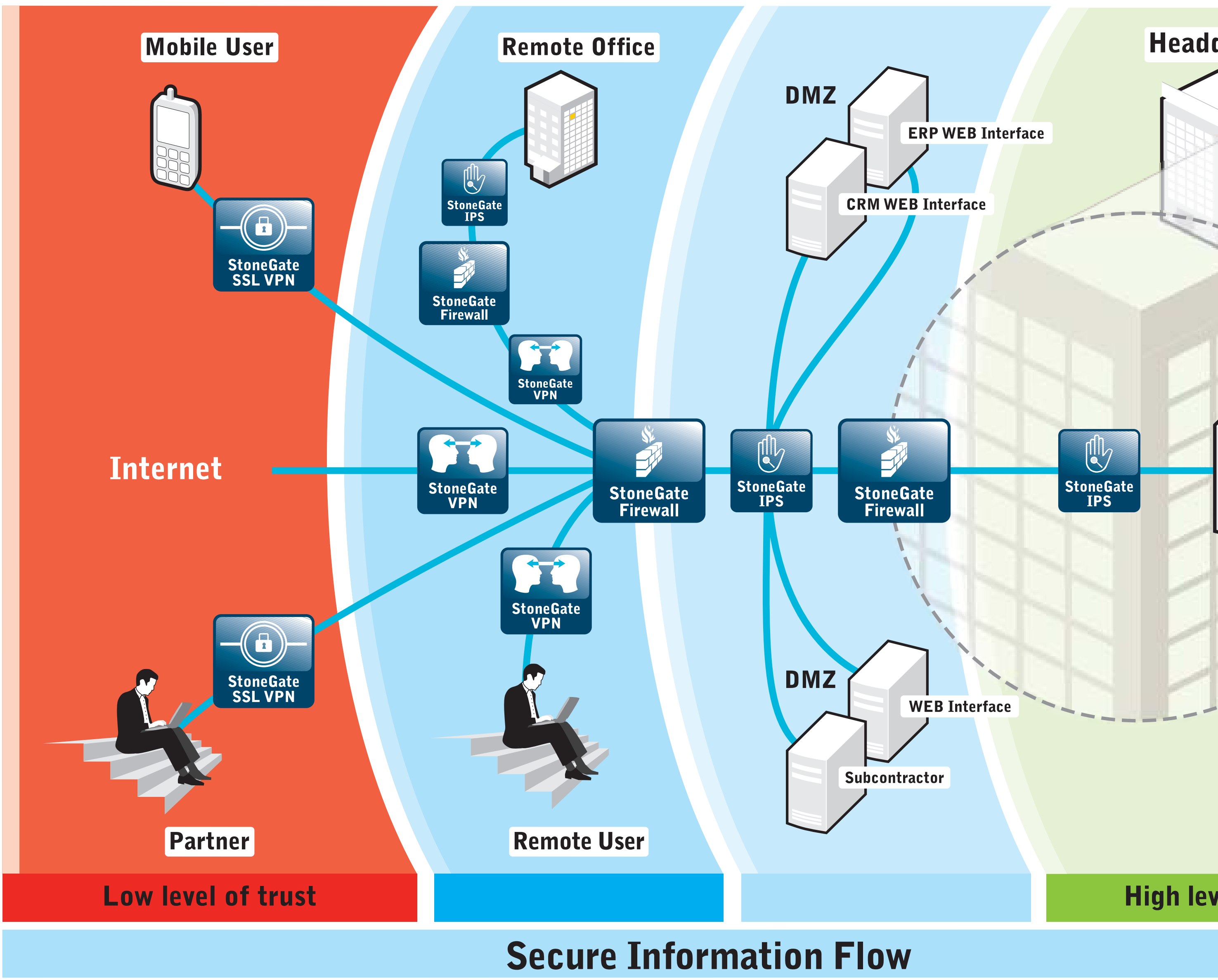
The key benefits of StoneGate SSL VPN include modular and reliable end-to-end security with strong encryption, solid authentication, granular access control and comprehensive trace removal.

StoneGate IPS

Comprehensive protection against malware and DoS attacks

Integrated with StoneGate Firewall/VPN, StoneGate IPS complements perimeter defense by protecting the inside of your network. StoneGate IPS protects vulnerable applications, operating systems and back-end databases by stopping worms, spyware, peer-to-peer, web applications, denial of service (DOS) and other malicious attacks.

The unique StoneGate transparent access control module unifies IPS and firewall functionalities, providing attack prevention and transparent firewall access control without the need to change existing network configurations.

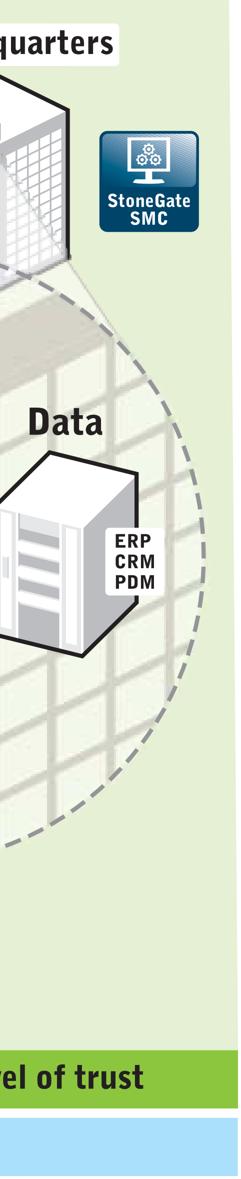


StoneGate Management Center

Easy and cost efficient management and configuration

StoneGate Management Center (SMC) delivers an innovative, holistic approach for role-based administration through a single, centralised management system. StoneGate Management Center allows you to:

- Benefit from advanced features such as remote upgrades, alarm centre management and sophisticated reporting
- Create a disaster recovery site, ensuring continuous access to management and log resources
- Reduce incident handling times, simplify everyday administration and lower the total cost of ownership (TOC)



StoneGate Firewall/VPN

Enhanced network security and business continuity

StoneGate Firewall/VPN creates a protective perimeter around your company, prevents attacks and secures the information flow with Virtual Private Network (VPN).

StoneGate Firewall/VPN allows you to gain granular control of your network with Quality of Service (QoS) and Bandwidth Management.

Multi-Link Technology

StoneGate Multi-Link technology tackles the problem of unreliable WAN connections by adding real VPN tunnel load balancing and fault tolerance via transparent automatic failover to always-on or backup VPN tunnels. With Multi-Link, VPN connections can become as reliable and even more secure than traditional private WAN connections. Transparent automatic failover means that user connections are maintained even if one or more WAN connections are lost. Multi-Link improves VPN performance significantly because it always chooses the fastest path for users' connections. By providing faster speed, lower latency and greater reliability, Multi-Link helps companies meet their requirements in terms of centralising business applications, thin client architectures, VoIP infrastructures, etc.

The five key points of Stonesoft's solution

✓ European manufacturer whose integrated network security and business continuity solutions have been EAL4+-certified since 2002.

✓ Three ranges of security and high availability solutions for corporate networks: StoneGate Firewall & VPN (VPN and firewall), StoneGate IPS (intrusion prevention system) and StoneGate VPN-SSL (mobile VPN connections). These solutions are built around a common core, StoneGate Management Center (administration platform).

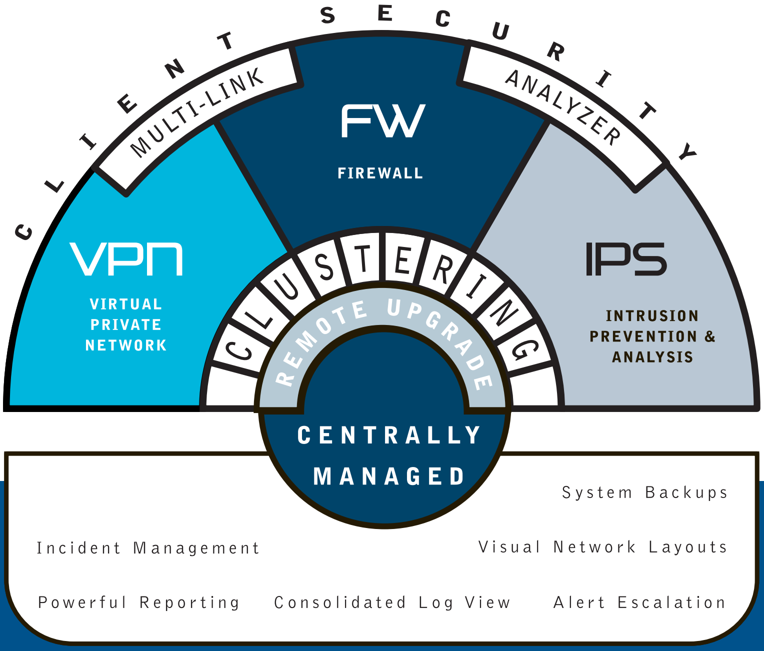
✓ A solution available as an Appliance and as software. These solutions are also integrated into virtual environments, with the same level of functionality.

✓ One of the only solutions capable of securing a network infrastructure throughout the client-server communication chain via its clustering, server load balancing and WAN connection mechanisms. In addition, its exclusive Multi-Link VPN ™ mechanism allows users to create a fully redundant multi-site architecture that protects against session outages in the event of operator failure.

✓ A highly-developed console for managing and operating the StoneGate engines which includes a wide range of features perfectly suited to distributed environments, data centres and/or MSSP.

STONESOFT

THE CORE OF THE STONEGATE ARCHITECTURE



The StoneGate Management Center (SMC) allows centralised administration of all StoneGate equipment (FW/IPS/VPN/VPN-SSL) via a single graphical interface. The SMC manages both physical and virtual engines with complete transparency in order to consolidate all the security nodes of an architecture.

The StoneGate Management Center module offers all administration functions as a standard feature:

- Network mapping
- Standardisation of deployments
- Statistical log analysis
- Online updates
- Incident management
- Reporting and Audits

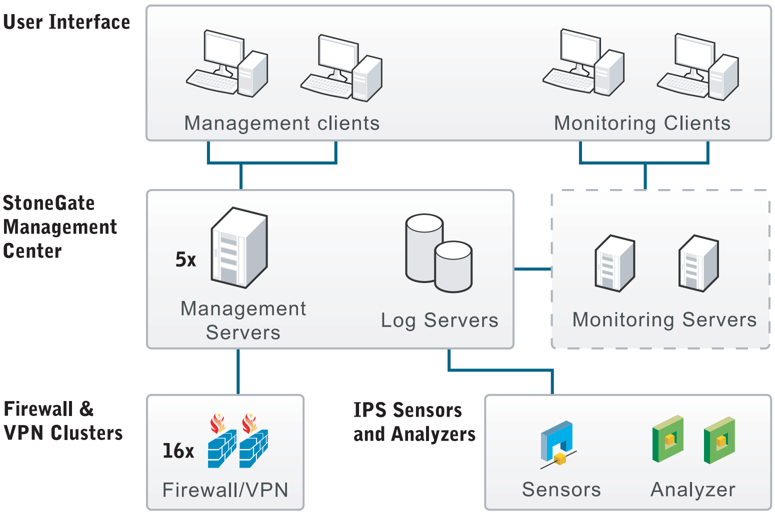
The StoneGate Management Center is the focal point of the security solution.

For obvious performance, reliability and security reasons, Stonesoft has opted for a three-tier management architecture. This means that the Management, Log and Alert servers are dedicated. This allows the FW/VPN/IPS filtering equipment to focus on its own specific tasks. For example, log processing does not degrade the performance of the Firewall.

In terms of security, companies are generally forced to use different administration tools for each product. They sacrifice their ability to use "unified management" tools for products that are not designed to be managed together. The result is higher training costs and a loss of security due to the team's inability to administer the entire security environment.

StoneGate products are designed from the ground up to be integrated into a common management system. StoneGate Management Center provides the ability to effectively manage the entire solution by using common configuration objects, concepts, templates, log, audit and alert systems, as well as all other administration tools.

Unified security and network configurations and "end-to-end" availability help reduce the solution's complexity and improve the level of security. This results in time and cost savings in everyday operational tasks.



FUNCTIONALITY AT A GLANCE

CENTRALISED MANAGEMENT

- "Define-once, use-everywhere" network elements
- Failsafe remote upgrade
- Audit trail of admin actions
- Rule base analysis tool
- Rule base templates and sub-rule bases for improved efficiency and performance
- Easy system backup and restore
- Role-based system administration
- Drag-and-drop routing
- Visual network layout for status monitoring and equipment configurations
- All communications are encrypted and authenticated
- Overview of connectivity, node and security status
- Configure and modify multiple elements at a time
- Security incident handling and documentation tool

CENTRALISED LOG MANAGEMENT

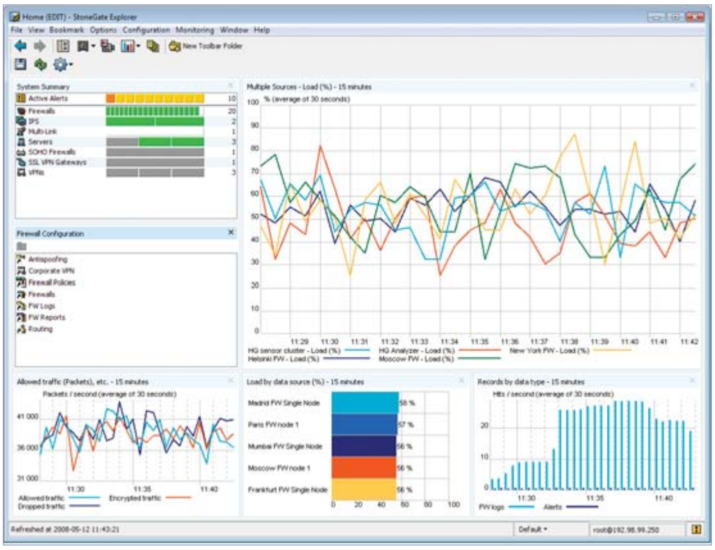
- Fast log browser that consolidates all the logs and alert information in a single view
- Support for multiple log servers
- Advanced log filtering for browsing, exporting and pruning
- Scheduled log data export and manipulation
- High performance log server

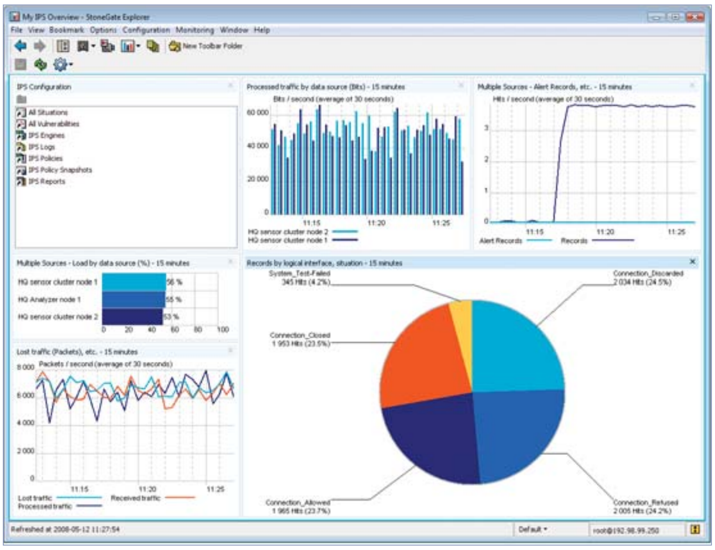
MONITORING AND ALERTS

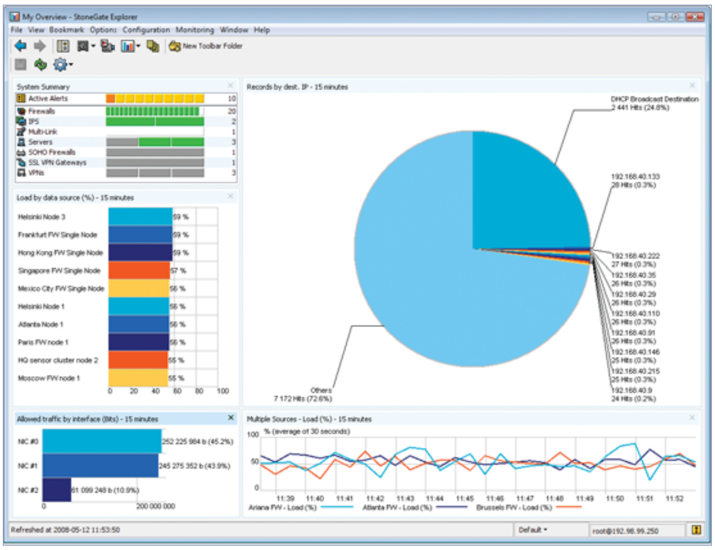
- Graphical, real-time monitoring of traffic and statistics
- Session and blacklist monitoring
- Configurable alert escalation
- Internal test system: auto-recovery system

REPORTING

- Report system and drag-and-drop customisable reports
- Reports exportable in PDF format
- Data selection using filters
- Data shown as charts, tables or both
- Data combined from several servers
- Reports created periodically and/or manually
- Customisable report templates




My IPS Overview - StoneGate Explorer
File View Bookmark Options Configuration Monitoring Window Help
New Toolbar Folder
IPS Configuration
All Situations
All Vulnerabilities
IPS Engines
IPS Logs
IPS Policies
IPS Policy Snapshots
IPS Reports
Processed traffic by data source (Bits) - 15 minutes
Bits / second (average of 30 seconds)
HQ sensor cluster node 2
HQ sensor cluster node 1
Multiple Sources - Alert Records, etc. - 15 minutes
Hits / second (average of 30 seconds)
Alert Records
Records
Multiple Sources - Load by data source (%) - 15 minutes
HQ sensor cluster node 1
HQ Analyzer node 1
HQ sensor cluster node 2
Records by logical interface, situation - 15 minutes
System_Test-Failed 345 Hits (4.2%)
Connection_Discarded 2 034 Hits (24.5%)
Connection_Closed 1 953 Hits (23.5%)
Connection_Allowed 1 965 Hits (23.7%)
Connection_Refused 2 005 Hits (24.2%)
Lost traffic (Packets), etc. - 15 minutes
Packets / second (average of 30 seconds)
Lost traffic
Received traffic
Processed traffic
Refreshed at 2008-05-12 11:27:54
Default
root@192.98.99.250


My Overview - StoneGate Explorer
File View Bookmark Options Configuration Monitoring Window Help
New Toolbar Folder
System Summary
Active Alerts
Firewalls
IPS
Multi-Link
Servers
SOHO Firewalls
SSL VPN Gateways
VPNs
Records by dest. IP - 15 minutes
DHCP Broadcast Destination 2 441 Hits (24.8%)
Others 7 172 Hits (72.6%)
Load by data source (%) - 15 minutes
Helsinki Node 3
Frankfurt FW Single Node
Hong Kong FW Single Node
Singapore FW Single Node
Mexico City FW Single Node
Helsinki Node 1
Atlanta Node 1
Paris FW node 1
HQ sensor cluster node 2
Moscow FW node 1
Allowed traffic by interface (Bits) - 15 minutes
NIC #0 252 225 984 b (45.2%)
NIC #1 245 275 352 b (43.9%)
NIC #2 61 099 248 b (10.9%)
Multiple Sources - Load (%) - 15 minutes
% (average of 30 seconds)
Ariana FW - Load (%)
Atlanta FW - Load (%)
Brussels FW - Load (%)
Refreshed at 2008-05-12 11:53:50
Default
root@192.98.99.250

STONESOFT VIRTUAL IPS : IN-DEPTH SECURITY FOR VIRTUAL ENVIRONMENTS

IPS has become an essential security feature for detecting malicious or inappropriate traffic. For this reason, Stonesoft has developed StoneGate Virtual IPS, a traffic detection and analysis system that determines the appropriate response. This solution is the only way to ensure full visibility and protection of communications among all virtual machines.

The StoneGate Virtual IPS appliance has all the functionality of a traditional StoneGate IPS appliance.

This virtual appliance provides the ability to filter flows within a virtual infrastructure and generate reports on all flows among virtual machines and on flows out of the ESX server.

StoneGate Virtual IPS is a system that detects and analyses malicious or inappropriate traffic, identifies it clearly and determines the appropriate response.

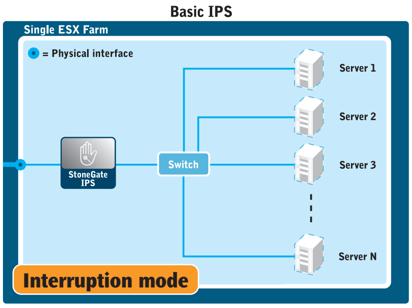
This virtual IPS appliance is extremely important in a virtual environment since it is the only way to ensure full visibility and protection of communications among all virtual machines.

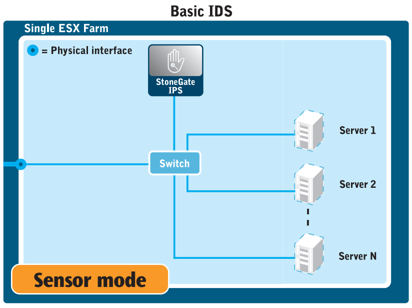
StoneGate Virtual IPS for in-depth security

StoneGate Virtual IPS detects and blocks in real time attacks on flows authorised by the firewall. It also reveals the presence of worms and spyware on the network and P2P applications.

The exclusive StoneGate Virtual IPS technology allows more accurate detection. It is built on multiple contextual methods:

- Signature database (customisable logical expressions)
- Protocol analysis
- Event correlation analysis
- Protocol identification (e.g. P2P on http)
- Advanced port scan detection





StoneGate Virtual IPS can be installed in the virtual architecture in traffic inline mode and/or in detection mode.

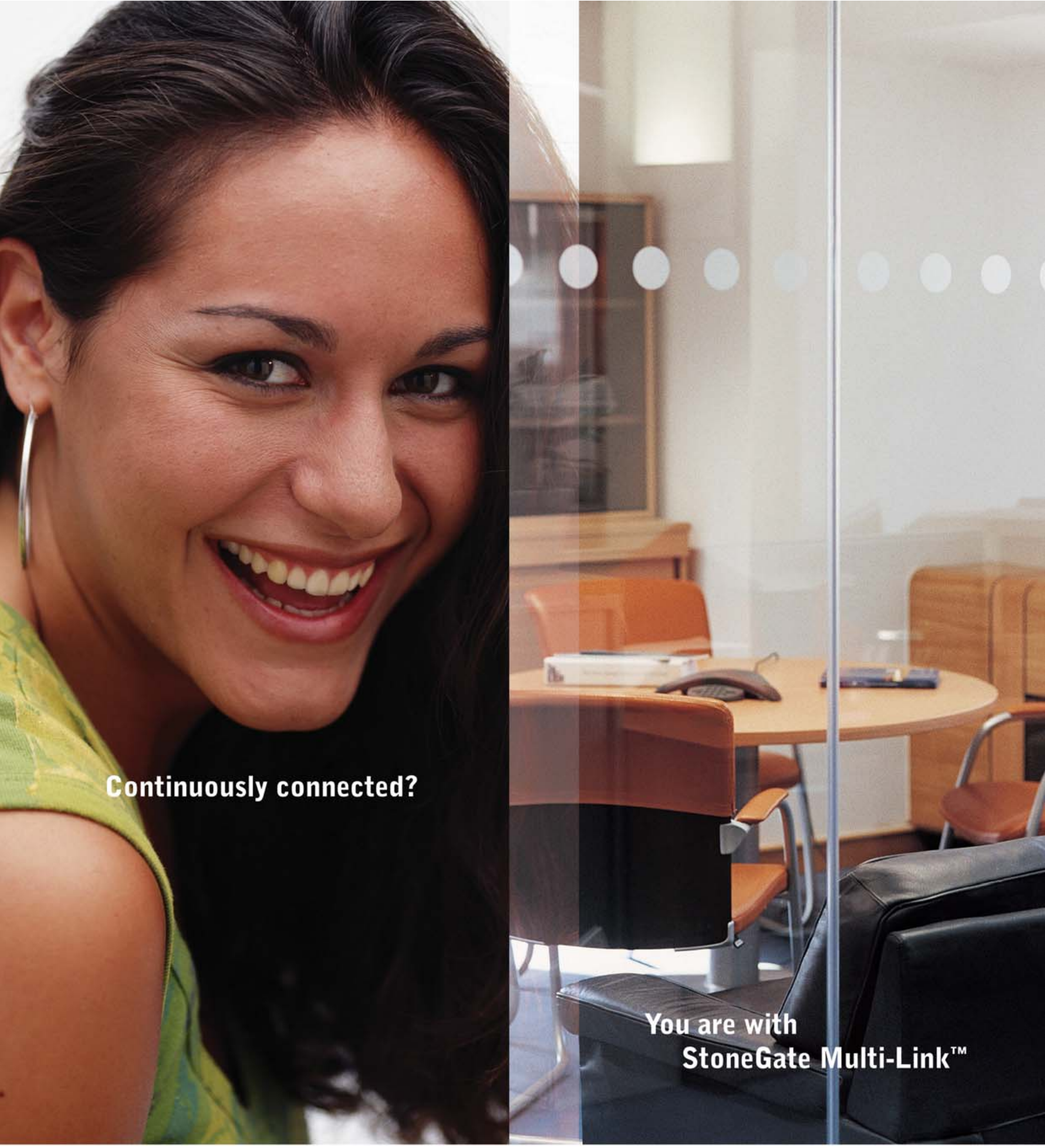
In inline mode, an attack is blocked instantly before it can reach its target. The StoneGate Virtual IPS is placed in front of the virtual machines.

In sensor mode, all traffic is analysed on a virtual switch thanks to the port mirroring function. This switch can also block traffic by delegating this function to another StoneGate IPS and/or FW engine.

StoneGate Virtual IPS also supports Transparent Access Control, which is used to set up level 2 to 7 access rules in addition to the IPS functions. This module offers the ability to segment a network efficiently by easily implementing StoneGate firewall rules. It also prevents unauthorised access between various zones, virtual or otherwise, with different security levels.

FUNCTIONALITY AT A GLANCE

- Protects vulnerable applications against network attacks, including client and server vulnerability on Windows, Linux/Unix and other operating systems.
- Detects spyware, DoS attacks (rate based DoS and non-rate based DoS), port scans, Trojan horses, worms, protocol anomalies and network transactions.
- Includes several inspection methods – protocol validation, malicious activity detection, generic and contextual signatures, denial of service detection, scan detection and event correlation over time and space for detected events.
- Includes thousands of signatures for more than 100 protocols - HTTP, DNS, IMAP, SMB, MSRPC, MYSQL, Oracle, POP3 and many others.
- Includes customisable signatures that use regular expression syntax to ensure greater protection against vulnerability.
- Provides an intelligent event correlation mechanism to reduce and manage false positives and false negatives.
- In inline mode, allows automatic and immediate blocking of anomalies detected or in cases where the security policy is breached.
- Advanced blacklisting and whitelisting capabilities in conjunction with other StoneGate virtual and/or physical components.
- StoneGate Virtual IPS allows implementation of inline mode and/or detection mode within the same virtual appliance.


Continuously connected?
You are with
StoneGate Multi-Link™

STONESOFT

www.stonesoft.com

Secure Information Flow