



Clavister Virtual Security Gateway Product Data Sheet

- Protect Virtual Servers
- Runs Within the Virtual Environments
- Secure Inter-Communication
- Achieve Auditing and Regulatory Compliance
- No Security Policy Compromises for Virtual Environments
- Highly Scalable
- Lower CAPEX
- Simplified Administration and Maintenance
- Green IT
- Highly Resource Optimized
- Optimized for the Unique Conditions found only in Virtual Environments

Introducing Clavister Virtual Security Gateway

More and more organizations are focusing on virtualization and reaping the benefits of cost reduction, higher utilization of hardware, less power consumption and an optimized environment, not to mentioned benefits such as ease of deployment and improved service availability. But there is one thing that does not come for free with virtualization and that is security. Virtualization puts new and demanding requirements on security, and therefore requires a virtualized security solution especially designed for virtual environments

Clavister is proud to introduce a leading virtual security solution for Data Centers/Hosting Providers, Telecom Operators and leading organizations. The Clavister Virtual Security Gateway Series joins the rank of the award-winning Clavister Security Gateway Series offering the same powerful Unified Treat Management (UTM) services as its hardware appliance and software appliance siblings. However, the main difference is that the Clavister Virtual Security Gateway Series runs inside the virtual environment as an integrated part and can therefore be managed as any other virtualized applications.

Security in virtualized environments must be easy to configure, maintain and deploy and requires special considerations regarding resource utilization and cater for the exceptional dynamic nature of virtualized environments where virtual machines are routinely moved around. This is especially true for Managed Security Service Providers (MSSP) and Data Centers who need an effective way to provision new services to customers.

Virtualization Market

The virtualization market has experience a strong growth rate in the last couple of years. Yankee Group stated in August 2007 that "9 of 10 enterprises have virtualization by 2007" and Gartner predicted in April 2008 that "virtualization would be part of nearly every aspect of IT by 2015".

This scenario shows a clear trend; more and more organizations move to virtualized environments. This creates new and challenging security threats in the virtualized environment that needs to be addressed. So far, the virtualization market has focused its effort on deployment, maintenance and provisioning of virtual servers.

With the introduction of Clavister Virtual Security Gateway, network security professionals now have the right solution to provision security in a virtual environment, without sacrificing any functionality.

"This new release allows us to add state-of-the-art virtual security appliance offerings to our product portfolio."

Kurt Glazemakers, VP Engineering
European Business Unit, Terremark
Worldwide, Inc.

"Virtualization, as with any emerging technology, will be the target of new security threats."

Neil MacDonald, Vice President and
Gartner Fellow

"Clavister offers one of the most compelling virtual security solutions for virtualized environments."

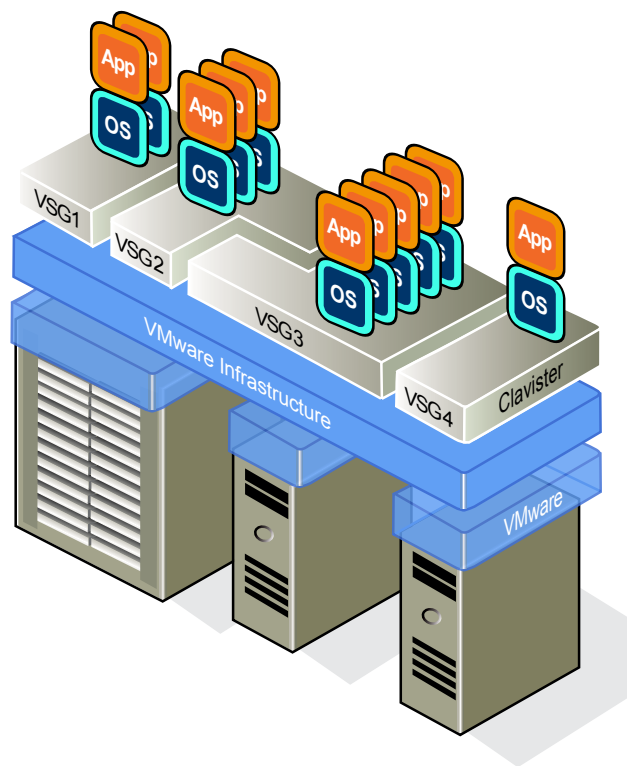
Jorina van Rensburg, CEO Condyn,
South Africa

Challenges in Virtualized Network Security

Traditional network security relies on physical segmentation of networks and servers, where physical firewalls or security gateways form effective filters between different servers and applications.

In a virtual environment, however, a large amount of servers may be deployed within the boundaries of a virtual infrastructure. As a result, communication between servers does not necessarily need to leave the virtual infrastructure and pass through the external physical security systems.

Using traditional, non-virtualized security solutions in conjunction with a virtualized environment in many ways defeats the benefits with virtualization, such as cost-savings and ease of administration. It is clear that organizations need to adopt a virtualized security solution especially designed for virtual infrastructures, especially since the virtual environment is a very dynamic environment, where servers are added, removed and change place frequently. This means that the traditional security solution cannot offer the same level of security as security solutions which operate within the virtual environment.



Security in virtualized environments must be easy to configure, maintain and deploy and requires special considerations regarding resource utilization. Given the dynamic nature of the virtualized environment, where virtualized applications can be restarted and moved, it is mandatory that the virtualized security solution operates within the virtualized environment. This is also a requirement for enabling protection between virtualized servers. Without securing the inter-communication between virtualized applications, it is not possible to achieve regulatory compliance, which is often a requirement for many solutions.

This is especially true for Managed Security Service Providers (MSSP) and Data Centers who need an effective way to provision new services to customers. Clavister, as a VMware Technology Alliance Partner, has worked hard to ensure that the Clavister Virtual Security Gateway Series is uniquely positioned as being very efficient on resource utilization and easy to manage in a virtual environment.

Resource Management

Virtualization is about managing your resources more efficiently. Dedicated servers may not utilize all its resource the most optimal way, whereas it is possible to consolidate many servers in a virtual environment and get the best possible resource utilization. The requirement for a virtual network security product must therefore be very efficient and require a minimum of resource, such as small footprint and memory requirement without sacrificing the level of security provided.

VMware Technology Alliance Partner

Clavister is a VMware Technology Alliance Partner and we are working closely with VMware to ensure the highest possible technology match for Clavister Virtual Security Gateway.



Clavister Virtual Security Gateway

Clavister Virtual Security Gateway Series comes with all the features of the Clavister Security Gateway Series, including:

- Stateful Firewall
- Deep Packet Inspection
- VPN
- Intrusion Detection & Prevention (IDP)
- Web Content Filtering
- Anti-Virus
- Anti-Spam
- SIP/VoIP Support
- Virtualization Technologies
- Gigabit Traffic Management
- User Authentication
- Server Load Balancing
- Route Load Balancing
- High Availability Clustering

For more information about Clavister Security Gateway, please visit:
www.clavister.com/products

Clavister Virtual Security Gateway – Resource Efficient

Clavister Virtual Security Gateway requires just 128 Megabyte of RAM and less than 32 Megabyte of hard disk space, which makes it one of the most efficient virtual network security products on the market and the ideal choice for Data Centers and Managed Security Service Providers (MSSP) who wish to provide security services to hundreds or thousands of customers.

Green IT

The promise of a greener IT environment and a huge reduction in energy cost can be achieved with right-sizing your IT environment and dynamic management of computer capacity across a pool of servers. Energy costs saving by 80 percent is not uncommon in virtualized environments. This makes the Clavister Virtual Security the obvious choice for customers who want to save energy and the environment.

Clavister Virtual Security Gateway

The new Clavister Virtual Security Gateway Series requires Clavister CorePlus™ 9.10 or higher and VMware ESXi 3 or higher.

Features and Benefits

Protect Virtual Servers. You can easily separate virtual machines from each other to eliminate the possibility of an intruder gaining easy access to several machines.

Secure Inter-Communication. Utilize VPN encryption to secure communication between virtual machines.

Achieve Auditing and Regulatory Compliance. Since the Clavister Virtual Security Gateway is inside the virtual environment, security auditing can be achieved and thereby meeting regulatory compliance requirements.

No Security Policy Compromises for Virtual Environments. Share your standard set of policies among your hardware appliances, software appliances and virtual appliances. This makes it much easier to enforce a cohesive security policy across all your Clavister network security gateways.

Scalability. Administrators can now extend security by simply deploying new Clavister Virtual Security Gateways as they go. This could be done simply by drag-and-drop or scripted using the built-in Command-Line Interface (CLI).

Lower CAPEX. Virtualization enables new business models where CAPEX is minimized.

Simplified Administration and Maintenance. Security components inherit all manageability features from the virtual environment, such as fail-over, provisioning, etc. This gives the solution a much easier administration and maintenance.

Minimized Downtime. Less hardware combined with highly efficient disaster recovery and redundancy tools, such as VMmotion from VMware, reduces downtime and improves the overall service performance of the security solution.

Clavister Virtual Security Gateway Series Specifications

| | Clavister VSG21 | Clavister VSG110 | Clavister VSG510 | Clavister VSG1010 |
|------------------------------|--|------------------|------------------|-------------------|
| Performance | | | | |
| Plaintext Throughput (Mbps)* | 50 | 200 | 500 | 1000 |
| VPN Throughput (Mbps)* | 50 | 200 | 500 | 1000 |
| Concurrent Connections* | 4000 | 16000 | 64000 | 256000 |
| Concurrent VPN Tunnels | 25 | 200 | 700 | 1000 |
| Ethernet Interfaces | Up to 3 | Up to 5 | Up to 7 | Up to 10 |
| Virtual Interfaces (VLAN) | 4 | 64 | 128 | 512 |
| Hardware | | | | |
| Form Factor | Virtual | Virtual | Virtual | Virtual |
| Warranty | All products in the Clavister Virtual Security Gateway Series come with a ninety (90) days Software Subscription covering all major and minor software releases counting from the Start Date. Start Date means the earlier of Product registration or ninety (90) days following shipment from Clavister. | | | |

Specifications subject to change without further notice.

* Specification is hardware (host) dependent.

NOTE: For product license options and support options, please visit: www.clavister.com or contact your local Clavister Sales Representative.

About Clavister

Since 1997, Clavister has been delivering leading network security solutions, providing commercial advantage to tens of thousands of businesses worldwide. The Clavister family of unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control.

Clavister has pioneered virtual network security, and this along with its portfolio of hardware and software appliances gives customers the ultimate choice. Clavister products are backed by Clavister's award-winning support, maintenance and education program.

Headquartered in Sweden, Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Contact Information

General Information
info@clavister.com

Sales Information
sales@clavister.com

Technical Support
support@clavister.com

Ordering Information
order@clavister.com

Partner Information
partner@clavister.com



WE ARE NETWORK SECURITY

Clavister AB, Torggatan 10, SE-891 33 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com | Email: info@clavister.com