clavister
SolutionSeries

Clavister – True Next-Generation Firewall

Intelligent and Robust Security With Next Generation Technologies

SOLUTION AT-A-GLANCE

- Clavister True NGFW combines the best of two worlds by offering a mature and proven Enterprise Firewall with well-integrated Next Generation Technologies. No compromises and no need to add more boxes to your network.
- Clavister True NGFW offers advanced Deep Application Content Control (DACC) that makes it possible for you to control how applications are being used in a pro-active and "zero-day" manner.
- No compromises when using Clavister True NGFW in real networks as features are well integrated and not just designed to tick-off checkboxes in a datasheet.
- Clavister True NGFW saves money as it has a minimal TCO but also reduce wasted productivity & bandwidth at the same time as it avoids costly security breaches.

KEY FEATURES

- Mature & Proven Enterprise Firewalling
- Deep Application Content Control
- User Identity Awareness and Control
- Flexible Configuration and Scalability
- Actionable Intelligence

Executive Summary

The CEO just left your room, your ears are ringing and your head is buzzing from what he just told you.

A report from a 3rd party security assessment had shown him more than 20 areas of weaknesses and a handful of potential breaches.

Not only have you had massive potential data leakage of confidential information, your network is also under attack by an advanced persistent threats (APTs) and with capability to encrypt valuable files as a part of a ransom scheme.

This might sound like a horror story but the bitter reality is that this is far from a worst-case scenario or even unlikely to happen. In fact, this happens to someone almost every hour, 365 days per year.

At the same time as internet offers many fantastic things for the enterprises and its users, the networks has grown increasingly complex with trends and technologies like cloud services, mobile work forces, BYOD, virtualized datacenters, social media, web-apps and more.

Not only have the network become more complex, dynamic and diversified, threats too have evolved and the worst case scenario of a security breach is a lot more serious than a defaced website.

Up until recently networks were relatively flat and basically made up of a LAN, WAN, DMZ with very little mobility in place. All the security you needed in those days was to deploy edge and core firewalls, install antivirus on the computers and that was it.

No matter how good, legacy firewalls fails to protect you as all applications communicates of the same http and https ports. Opening up your network for accessing internet means that you are opening up for almost every

application in the world to talk transparently through your firewall, without you even knowing about it and even less controlling it.

In this solution brief we help identify the challenges, the issues with the different products and technologies available on the market and how Clavister True NGFW does a better job when it comes to controlling security in a fast moving and dynamic network, without adding more "boxes" to manage.

Challenges in a dynamic and app-centric network

New technologies does not only come with benefits but also introduce new challenges. BYOD, Cloud, etc make it more difficult to define the boundaries of the network, where the enforcement points are and to understand/control how applications are being used, by whom and what information is being transferred.

Administrators are challenged to provide applications and services in a more dynamic way but still maintain best-in-class security so that the brand and business is not put at risk.

The borderless network

One of the aspect that create cause for concern in the modern network is that it has evolved from small and well contained segments to a borderless network that is dynamic by nature and constantly changing.

Users access information from a plethora of devices from any location in the world. At the same time as your critical applications and information is scattered across your own network but also across the internet (cloud services).

Threats growing exponentially

Hackers are no longer only students in dorm-rooms looking to show off their skills to their friends by defacing websites. There is a new breed of hackers that are highly skilled and motivated cyber criminals looking for financial gain and/or damage to brand and business by launching targeted attacks.

The treats today has become more sophisticated, increased in frequency and consequences more devastating.

Legacy SPI Firewalls and the App-centric network

The classic concepts of network segmentation and stringent access control still apply as the cornerstones in security best practices and SPI firewalls is, and will always be, a crucial part of implementing these boundaries.

However, in today's app era there are more things needed in order to manage and control a secure network.

As almost every single application today are running over the same ports as your normal web-browsing (port 80, 443, etc), the legacy Stateful Packet Inspection firewalls fails to see any difference between for instance Skype and someone browsing internet. Allowing your users to access internet means you are opening up for them to use almost all applications.

The need to control how applications are being used in your network goes far beyond combatting unproductive usage of social media and extends to far more serious issues such as to avoid applications from being a threat vector or a gaping hole for data leakage.

Consequently the mobility and app era demands new security products to help you:

- Manage risks from attacks (Infected web-applications, multi-staged attacks)
- Avoid data leakage through applications (Dropbox, megashare, skype, IMs)
- Reduce risk for unproductive use of e.g. social media (Facebook, Twitter, Instagram)
- Decrease risk for downloads of copyrighted materials (P2P/Torrent, File-sharing)
- Avoid bandwidth starvation due to usage of unproductive download apps (P2P & Streaming video)
- Establish clear accountability (Who did what using which application from what device and location)

Extract from Gartner recommendations and analysis

- "The stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats"

Extract from NSS Labs Recommendation to old-generation firewall users

- Firewall users should consider including NGFW technology on the short list during the next refresh cycle.

The Clavister True Next Generation Firewall solution

To help secure the dynamic and app-centric networks we have taken the best from Enterprise Firewalling (SPI), Unified Threat Management (UTM) and Next Generation Firewalls (NGFW) and created the Clavister True Next Generation Firewall.

Clavister True Next Generation Firewall uniquely combines the robustness and flexibility from Enterprise Firewalls, the versatility from Unified Threat Management and Application Control from Next Generation Firewalls.

With Clavister True NGFW you get the best-of-the-best without the compromises you have in each respective product type. As an example, Clavister True NGFW gives you the versatility from UTM without the poor integration and flexibility that makes them difficult to run in networks more complex and Deep Application Content Control to manage how applications are used and replaces your legacy firewall rather than just add another device to complement it.

Features such as Deep Application Content Control, User Awareness, Devices Awareness, Flexible configuration & Scalability makes the Clavister True NGFW the ideal choice for enterprise and mid-segment customers.

- **Mature and Proven Enterprise Firewall**

  Stability, performance and flexibility comes as a result of good design and has made Clavisters technology the #1 choice in more than 200.000 networks over the last 17 years.
- **Clavister Deep Application Content Control (DACC)**

  Protocol Decoders, Heuristic Analysis, Future Flow Association and other advanced techniques makes it possible to control how applications are being used in a zero-day manner and high accuracy.
- **User Awareness and Control**

  Multiple techniques to transparently authenticate and identify users combined with careful integration into the core functionality makes it easy to define policies that combine application, user, ip, time, network or even type of devices. As a consequence you can easily see who did what and when and establish an unquestionable accountability.
- **Flexible Configuration and Scalability**

  All features in Clavister True NGFW is designed from ground up and every line of code carefully implemented to make sure you can configure them any way you like or need. No compromises are needed, after all, no two networks are alike. Additionally the same software that runs inside our physical appliances comes as a virtual appliance that helps you secure your virtual datacenter or even cloud applications.
- **Actionable Intelligence**

  While most other vendors have report tools that simply just prints the log records sorted in different ways but doesn't help you understand what is really going on or what the problems are, Clavister Actionable Intelligence extended these classic firewall/network reports with infographics reports and dashboards. This helps you to quickly analyze and understand where your risks and gaps are, what's going on in your network and assists you in making good decisions on how to address your problems and weak spots.

Benefits & Conclusion

Your organization are going through changes and you need to balance security and efficient communication.

Clavister True NGFW helps you maintain a flexible and dynamic organization that benefits from all the new technologies without having to compromise security, add more devices or costs. In fact, Clavister actually helps your organization become more efficient by eliminating risk of unproductive usage of applications, lowering the administrative workload and improve service for your mission critical applications.

No other product on the market offers the same unique combination of mature and proven enterprise firewalling with tightly integrated next generation technologies. A combination that allows you to secure and control the network without adding more boxes but instead replacing and consolidating them.

Feature	Benefit
Mature Enterprise Firewalling	**Superior TCO, Less administration and enhanced security** No need to add more devices as Clavister True NGFW has a rock-solid enterprise firewall combined with well integrated next gen technologies.
True Deep Application Content Control	**Improved security** thanks to zero-day awareness of sub-features / sub apps. **Works in real networks** as you can identify how applications are being used, not just what application or url it is. **More accurate control** as engine is built on best-in-class DPI technology, not just IPS with app signatures, it has less false positive/negatives. **Clear accountability** as you can identify who did what, when and what information was transferred.

Feature	Benefit
User Awareness	**Improved security** as you can tailor access to what is only needed for a specific user or group, no more one-size-fits-all. **Clear accountability** as you will know exactly who did what and when without having to dig through many systems to locate who was using which IP address and when. **Decrease in risky behaviour** among your users as they understand that they are being held accountable for inappropriate usage of corporate resources. **Reports that makes sense** and are easy to read
Flexible Configuration & Scalability	**Designed for real networks and requires no compromises** rather than a product that looks good in the datasheet but doesn't work in the real world. **Simplified administration and improved security** as the same software that runs inside the physical appliances can run in your virtual datacenter or cloud environment; it even uses the same central management and reporting tools.
Actionable Intelligence	**C-Level Reporting made easy by Infographics reports.** **Improved Security** since "reports" focus on giving you valuable and useful information rather than than just print-outs of log data sorted in different ways. **More efficient network** as you understand how to optimize your policies and decrease wasteful bandwidth usage. **More efficient workforce** as you can optimize policies for internet usage and avoid unproductive behaviours.

Choose Clavister True NGFW today, start saving valuable time on security administration and boost your business productivity.

Where to Buy Clavister

For more information about where to buy Clavister products, visit **www.clavister.com/partners**. Additional resources and customer testimonials can be found at **www.clavister.com/resources**.

About Clavister
Clavister is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against current and new threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the 2012 Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

clavister®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com

Copyright © 2014 Clavister AB. All rights reserved. The Clavister logo and all Clavister product names and slogans are trademarks or registered trademarks of Clavister AB. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Information in this document is subject to change without prior notification.