clavister
FeatureSpotlight

Clavister True Application Control

Optimize network for business applications

Top Features

- Monitor, Block or Traffic Shape applications based on Layer 7 recognition, not ports
- High recognition rate: ability to identify protocols from layer 2 to 7 in the OSI model
- Deep Application Content Control (DACC) extracting meta-data and decodes actions launched inside applications.
- Decode messages from more than 2,300 applications and 2,400 meta data tags (comparable to 11,5 million signatures using old-school IPS engines)
- High-performance, non-intrusive SSL Inspection for Application Control
- Advanced DPI engine to identify and control advanced and evasive applications, not just simple Web applications
- User-friendly, Wiki-style configuration
- High performance – value for money

Introduction

Clavister Application Control (AC) provides an effective way to identify and manage how applications are used in the network regardless of port and protocol used.

The need to control how applications behave in the network regardless of ports and protocol grows exponentially when more applications runs over the same Web-ports (80/443, HTTP/HTTPS) and evades normal port based firewall policies.

Future-safe technology

The highly advanced DPI engine in our products stands out in a crowded market of next-generation firewalls based on IPS engines as it offer a deeper level of inspection and goes far beyond those old-fashioned regexp signatures.

Thanks to sophisticated protocol plug-ins and the unique engines inside Clavister Application Control (AC) and Clavister Deep Application Content Control (DACC) our products decode messages from more than 2,300 applications and extract more than 2,400 meta data tags. This translates into a future-proof solution with monitoring and control capabilities for millions of combinations of Web 2.0 applications, widgets, actions launched inside applications and similar.

High performance recognition of encrypted applications

With Clavister SSL Inspection for Application Control you can even recognize applications that are encrypted (HTTPS). The tight integration of SSL Inspection for Application Control enables recognition of encrypted applications without any performance degradation or issues with certificate intrusions.

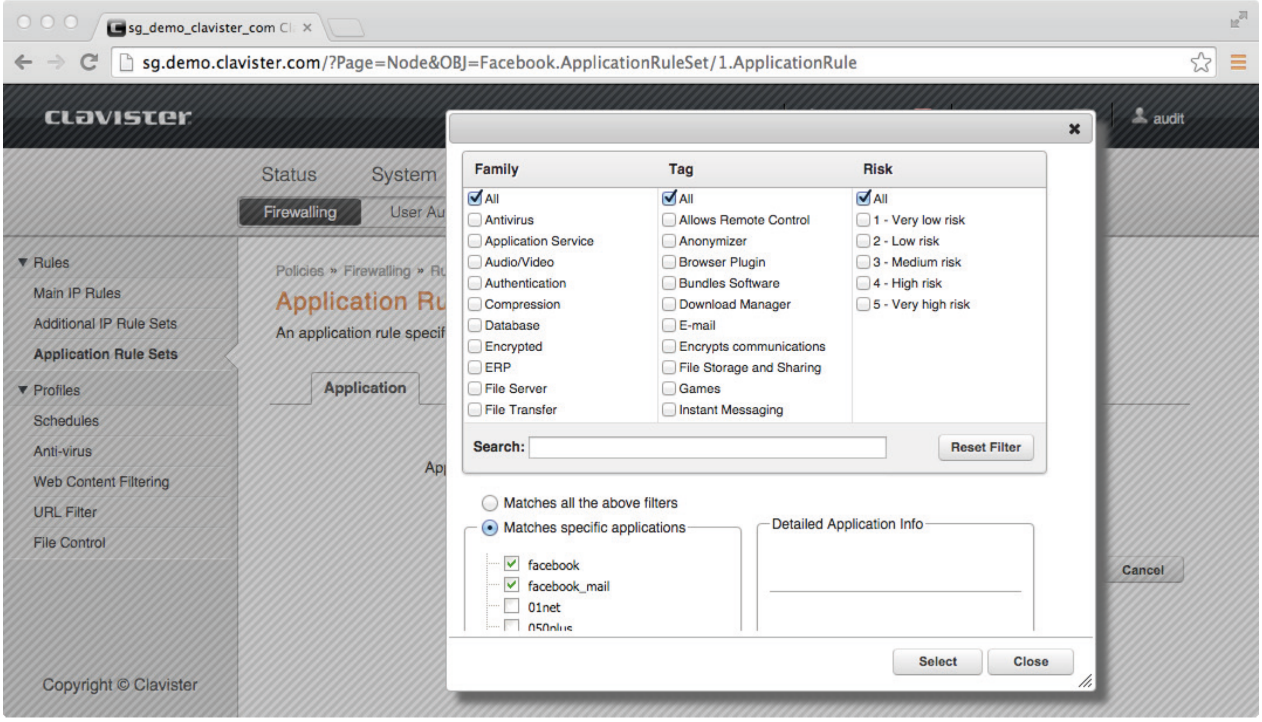
By identifying the encrypted applications without having to initiate a so called man-in-the-middle attack where all sessions has to be decrypted and re-encrypted the recognition can be done at very high speed but also avoid issues with invalid certificates. This, non intrusive approach, also enables recognition to work on thick applications where the certificate validation is done more rigid than in web-browser based applications.

Managing application control policies

Simple yet powerful configuration

Applying Clavister Application Control policies are as easy to define as regular level 3 policies.

For layer 3 policies it is often easy to decide what port/protocol to allow or block but when it comes to applications it is sometimes a bit more complicated to understand what is productive and what is not, what applications may introduce risk and similar. To assist and simplify building proper application control policies the configuration interface has been designed as a Wiki style portal. The Wiki stye portal enables filtering and selection of applications based on Application-Family, Characteristics/Behavior descriptive Tags and Risk Rating.



Family	Tag	Risk
☑ All	☑ All	☑ All
□ Antivirus	□ Allows Remote Control	□ 1 - Very low risk
□ Application Service	□ Anonymizer	□ 2 - Low risk
□ Audio/Video	□ Browser Plugin	□ 3 - Medium risk
□ Authentication	□ Bundles Software	□ 4 - High risk
□ Compression	□ Download Manager	□ 5 - Very high risk
□ Database	□ E-mail	
□ Encrypted	□ Encrypts communications	
□ ERP	□ File Storage and Sharing	
□ File Server	□ Games	
□ File Transfer	□ Instant Messaging	

Search: Reset Filter

○ Matches all the above filters

● Matches specific applications

☑ facebook
☑ facebook_mail
□ 01net
□ 050plus

Detailed Application Info

Select Close

This approach helps you define policies that are effective and optimize your network for security and productivity without having to understand the exact behavior of every application that exists on the Internet.

Flexible configuration to meet your business needs

To further enhance the usability of Clavister Application Control we have integrated it following the same super-flexible approach as with all other features. This means that it is easy to combine Application Control with User Awareness, Time Schedules, Interfaces, IP addresses and similar. Naturally you can apply actions such as allow / monitor, block or traffic shape on any policy you define. The flexible and powerful configuration makes it easy to tailor your policies to fit your specific business needs rather than having to compromise due to lack of configurability of your firewall.

One of the strong points of Clavister application Control is the ability to monitor application usage in your network. Some applications can disturb the network traffic by using too much resource or they can attract malicious traffic patterns or viruses.

Monitor, analyze, take action

As an example, an administrator notices that there is an increase in traffic going back and forth between the Internet and the internal network. Before taking any steps to curb this, the administrator enables Clavister Application Control. Studying the log files reveals that the offending application is a BitTorrent application originating from an IP address on the internal network. This information enables the administrator to act accordingly, either by blocking or applying traffic management to BitTorrent, but limit it to only 2 Mbps.

For applications that have a tendency to starve network traffic resources, you can apply traffic management to these applications. This gives you the ability to allocate the right amount of resources without having network congestion caused by applications.

Enhance security by Whitelisting applications

Application Control is often used in order to monitor the application traffic in a network but it can also be used as a powerful security feature to lower the attack footprint and avoid data leakage.

With Clavister AC you can build policies that ensure for instance that the only application that is allowed to talk on a specific port and IP address is MySQL/SQL Commands. All other known or unknown application will be blocked, including traffic from unproductive applications, malwares or malware communication to command and control servers.

Application rule sets

It is also possible to configure filters on application rule sets, support for lists of users and user groups, block and allow applications, and to apply traffic management functionality on applications. This enables you to make extremely efficient application rules, for example:

```
allow ‘facebook’ for group ‘marketing’
drop ‘facebook’
allow ‘http’
```

This rule enables the Facebook application but only for members of the group “Marketing”. All other users are denied, but any Web site is allowed.

Logging and reporting

One of the key components in Clavister Application Control is the Clavister InControl Logging Agent (ILA) which is used for collecting application statistics. The statistics can then be processed, analyzed and presented in Clavister InControl using a wide range of display options, including online analytical processing (OLAP) functionality.

Clavister InControl enables you to view not only collected application control information, but all collected information, including IDP, AV and WCF information. This gives you a correlated view of collected information, which can be analyzed and distributed in various formats.

Using the associated meta data it is possible to refine policies for greater accuracy. For example, for generic HTTP traffic you can specify URL, user agent, Web server, cookies and more than 60 additional meta data tags.

Questions and Answers

Clavister security Gateway with True Application Control is the answer to the challenge of optimizing the network for running business productive and safe applications, regardless of port or protocol being used an key issues when it comes to optimizing the network for running productive application traffic.

Q: Does Clavister AC work on encrypted applications

A: Yes, Clavister SSL Inspection for Application Control enables recognition of applications also for encrypted applications.

Q: Does the Clavister SSL Inspection for Application Control slow down my network and create issues with modified certificates?

A: No, the powerful DPI engine used for our Application Control feature enables this detection without having to conduct a man-in-the-middle attack and decrypt / re-encrypt all traffic. Clavister SSL Inspection for Application Control enables recognition of encrypted applications without any performance degradation or issues with certificate tampering/intrusions.

Q: Recognition of more than 2,300 applications is a lot but some vendors claims hundreds of thousands. What is the real difference?

A: Yes, 2,300 applications is a lot of applications depending on what you actually count as an application. Some vendor reports hundreds of thousands of applications when it in fact might just be a lot of URLs or widgets/sub-applications inside a real application.

Thank to the capabilities of the Clavister DACC feature that decodes and extracts more than 2,400 meta-data tags you do not only get the power to control or monitor millions of these so called widgets or sub-applications but you do it for both known and unknown ones using powerful policies. Clavister AC and DACC has an advanced and proactive technology that recognize more applications than almost any other product and does not need to rely on hundreds of thousands of signatures that becomes outdated almost before they are released.

True Application Control Key Benefits

- **Improved security** – Lower the attack footprint by ensuring that only allowed application traffic is flowing through the firewall. Traffic from unwanted or unknown applications can be recognized on a per-application basis and stopped at the firewall regardless of port and protocol being used.
- **Reduced risk for data leakage** – Avoid data leakage by blocking traffic from unwanted applications that try to evade the firewall by using the same ports and protocols as business applications.
- **Improve performance and remove bottlenecks before they happen** – Optimize network for business applications and free up bandwidth and resources by limiting and blocking traffic from unproductive or unwanted applications.
- **Reduce waste of resources and productivity** – Limit and control usage of corporate resources to productive applications. Avoid wasting bandwidth and work force productivity by managing access to social media, P2P and other.
- **Insight and Situation Awareness** – Transparently identify the applications being used in your network to identify security risks, potential performance bottlenecks or simply to optimize capacity to be aligned with business goals.

For more information about Clavister products and services, please visit us at: www.clavister.com.

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/support/resources.

About Clavister
Clavister (NASDAQ: CLAV) 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 threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the 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