

Feature Brief



Clavister Web Content Filtering

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

CLAVISTER®

Protecting Values

Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

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

Overview

For many organizations, Internet access can be a mixed blessing, or sometimes even pose a serious problem. The Internet is usually regarded as a productivity enhancement - employees can access information from anywhere, work can be done in a more freely manner and with the right information at their disposal. But sometimes it can also be counter-productive. Apart from any security issues, the Internet can also be a source of non-productivity. Many organization points to legal liability, productivity, and bandwidth usage as concerns that arise when employees view inappropriate Web sites, shop online incessantly, or download and play DivX files throughout the day. Monthly sales numbers are down but employee surfing is up.

Some organizations are also looking at Web Content Filtering by a lack of perceived control, especially in the wake of new regulations like HIPAA and Sarbanes-Oxley, which are meant to protect customer privacy and oversee financial dealings. For school's this issue also tether on moral and ethical obligations that parents feel the school has, such as preventing children from accessing pornographic or racist Web sites from school computers. It is not realistic to expect teaching staff to supervise all computer use, especially if computers are accessible during breaks. Any organization faced with this situation should consider Web Content Filtering, but also think through organization policies. Avoid letting fear provoke hasty decisions.

Clavister Extended Unified Threat Management

Clavister Web Content Filtering (WCF) is part of the Clavister Extended Unified Threat Management (xUTM) solution that provides best-in-breed Intrusion Detection & Prevention (IDP), Web Content Filtering (WCF), Anti-Virus and Anti-Phishing. The converged security solution provides your IT department with a comprehensive toolbox which is easy to use, low on maintenance and scales as you grow. All components in the Clavister xUTM solution are built to lower your maintenance effort, and increase the productivity within your company.

Clavister Service Provisioning Network

The Clavister Service Provisioning Network (CSPN) is a global network of secure and high-performance servers managed by Clavister that ensures fast, accurate and safe delivery of Intrusion Detection & Prevention (IDP) and Clavister Anti-Virus signatures, as well as content classification databases for the managed Web Content Filtering (WCF) services. The CSPN is the backbone in Clavister Zero-Day Protection (CZDP).

Clavister Web Content Filtering

Web traffic is one of the biggest sources for security issues and misuse of the Internet. Inappropriate surfing habits can expose a network to many security threats, as well as legal and regulatory liabilities. Productivity and Internet bandwidth can also be impaired. Clavister Web Content Filtering provides three mechanisms for filtering out Web content that is deemed inappropriate for an organization or group of users. The supported filtering mechanisms are:

- Active Content Handling
- Static Content Filtering
- Dynamic Content Filter

These filtering mechanisms address different types of problem and offers solution to the most common problem. All three mechanisms can be used together to form a very effective solution. Each of these mechanisms will be presented below.

Active Content Handling

Some Web content can contain malicious code designed to harm the workstation or the network from where the user is surfing. Often, such code is embedded into various types of objects or files which are embedded into Web pages.

Clavister Web Content Filtering includes support for removing or blocking the following types of objects from Web page content:

- ActiveX objects, including Flash objects
- Java applets
- Javascript/VBScript code
- Cookies
- Invalidly formatted UTF-8 characters, since invalid URL formatting can be used to attack Web servers

You can configure which types of object to remove individually by configuring the corresponding HTTP Application Layer Gateway (ALG).

Static Content Filtering

Clavister Web Content Filtering can also block or permit certain Web pages based on configured lists of URL's which are called URL Blacklists and URL Whitelists. This type of filtering is also known as Static Content Filtering. The main benefit with Static Content Filtering is that it is an excellent tool to target specific Web sites, and make the decision as to whether they should be blocked or allowed.

Filtering Ordering

Static Content Filtering takes place before Dynamic Content Filtering. This makes it possible to manually make exceptions from the automatic dynamic classification process. For example, where goods have to be purchased from a particular online store, Dynamic Content Filtering might be configured to prevent access to shopping sites by blocking the "Shopping" category. By entering the online store's URL into the HTTP Application Layer Gateway's URL Whitelist, access to that URL is always allowed, taking precedence over Dynamic Content Filtering.

Support for Wildcards

Both URL Blacklist and URL Whitelist support wildcard matching of URL's. This makes the Static Content Filtering very powerful and flexible. This wildcard matching is also applicable to the path following the URL host name which means that filtering can be controlled at both file and directory level.

Below are some URL Blacklist examples used for blocking:

```
*.example.com/*
```

This is an effective blacklist configuration. This will block all hosts in the `example.com` domain and all Web pages served by those hosts.

```
www.example.com/*
```

This is also an effective blacklist configuration. This will block the `www.example.com` Web site and all Web pages served by that site.

```
*/*.gif
```

This is also an effective blacklist configuration. This will block all files with the file extension `.gif`.

```
www.example.com
```

This is a less effective blacklist configuration. This will only block the first request to the Web site, which is probably not what the administrator had in mind. For example, surfing to `www.example.com/index.html` will not be blocked.

```
*example.com/*
```

This one is also a less effective blacklist configuration. This will also cause `www.myexample.com` to be blocked since it blocks all sites ending with `example.com`.

Dynamic Content Filtering

Clavister Web Content Filtering also supports Dynamic Content Filtering of Web traffic. This function allows administrators to permit or block access to Web pages based on the content of those Web pages. This functionality is fully automated and it is not necessary to manually specify which URL addresses to block or allow. Instead, Clavister maintains a global infrastructure of databases containing massive numbers of current Web site URL addresses, grouped into a variety of categories such as shopping, news, sport, adult-oriented, etc. For a complete list of categories, please see Table 1 below. These databases are updated every hour with new, categorized URL addresses while at the same time older, invalid URL addresses are dropped. The database content is global, covering Web sites in many different languages and which are hosted in several countries around the world.

Categorizing Pages and Not Sites

The Dynamic Content Filtering categorizes Web pages and not sites. In other words, a Web site may contain particular pages that should be blocked without blocking the entire site. Clavister Web Content Filtering provides blocking down to the page level so that users may still access parts of Web sites that are not blocked by the filtering policy.

Content Filtering Categories

This section lists all the categories used with Dynamic Content Filtering. For detailed information and examples of each category, please read the Clavister CorePlus™ Administration Guide.

1: Adult Content	17: www-Email Sites
2: News	18: Violence/Undesirable
3: Job Search	19: Malicious
4: Gambling	20: Search Sites
5: Travel/Tourism	21: Health Sites
6: Shopping	22: Clubs and Societies
7: Entertainment	23: Music Downloads
8: Chatrooms	24: Business Oriented
9: Dating Sites	25: Government Blocking List
10: Game Sites	26: Educational
11: Investment Sites	27: Advertising
12: E-Banking	28: Drugs/Alcohol
13: Crime/Terrorism	29: Computing/IT
14: Personal Beliefs/Cults	30: Swimsuit/Lingerie/Models
15: Politics	31: Spam
16: Sports	32: Non-Managed

Table 1: Web Content Filtering Categories

NOTE: The Non-Managed category contains unclassified sites and sites that do not fit one of the other categories. These sites will be placed in this category. It is unusual to block this category since this could result in URL addresses, mostly harmless, being blocked.

Web Content Filtering At Work

When a user requests access to a Web site the Clavister Security Gateway queries all configured databases to retrieve the category of the requested site. The user is then granted or denied access to the site based on the filtering policy in place for that category. If access is denied, a Web page will be presented to the user explaining that the requested site has been blocked. This means that the block page can be customized with organization logotypes and messages that explain the organization's Internet policy. The Web page presented to the user can be customized to your needs by uploading a package of HTML pages to the system. To make the lookup process as fast as possible a local cache of recently accessed URL addresses is maintained on the Clavister Security Gateway. Caching can be highly efficient since a given user community, for example a group of university students, often surfs to a limited range of Web sites.

If the requested Web page URL is not present in the CSPN databases, then the Web page content at the URL will automatically be downloaded to Clavister's central data warehouse and automatically analyzed using a combination of techniques including neural networks and pattern matching. Once categorized, the URL is distributed to the global databases and the Clavister Security Gateways can access the category for the URL. This minimizes the administrative effort of maintaining the Dynamic Content Filtering.

Allowing Override

Sometimes, Dynamic Content Filtering may prevent users carrying out legitimate tasks. Consider a stock broker dealing with online gaming companies. In his daily work, he might need to browse gambling Web sites to conduct company assessments. If the corporate policy blocks gambling Web sites, he will not be able to do his job.

For this reason, Clavister CorePlus™ supports a feature called Allow Override. With this feature enabled, the content filtering component will present a warning to the user that he is about to enter a Web site that is restricted according to the corporate policy, and that his visit to the Web site will be logged. This page is known as the restricted site notice. The user is then free to continue to the URL, or cancel the request to prevent being logged.

By enabling this functionality, only users that have a valid reason to visit inappropriate sites will normally do so. Other will avoid those sites due to the obvious risk of exposing their surfing habits.

Reclassification of Blocked Sites

Since the process of classifying unknown Web sites is automated, there is always a small risk that some sites are given an incorrect classification. Clavister CorePlus™ provides a mechanism for allowing users to manually propose a new classification of sites. This mechanism can be enabled on a per-HTTP Application Layer Gateway level. This means that you can choose to enable this functionality for regular users or for a selected user group only.

If reclassification is enabled and a user requests a Web page which is disallowed, the block Web page will include a dropdown list containing all available categories. If the user believes the requested Web site is wrongly classified, he can select a more appropriate category from the dropdown list and submit that as a proposal.

The URL to the requested Web site as well as the proposed category will then be sent to Clavister's central data warehouse for manual inspection. That inspection may result in the Web site being reclassified, either according to the category proposed or to a category which is felt to be correct.

Silent Mode

One very useful Web Content Filtering feature is to run the function in Silent Mode. This means that you configure the Web Content Filtering to audit and categorize Web pages but none of the Web pages are blocked. This gives administrators a clear picture of how Internet resources are used within an organization.

For System Integrators, this can even be turned into an offered service. A System Integrator can offer to run the Clavister Web Content Filtering free of charge for a predefined number of days. At the end of the free run, they present a detailed report using Clavister InSight™. The report will detail time spend and bandwidth used for different users in different categories. The System Integrator can then work with the organization to calculate how the Web Content Filtering can improve the organization and make it more efficient. It would also be easy to calculate the Return of Investment (ROI) for the Clavister Web Content Filtering.

Subscribing to the Clavister Web Content Filtering Service

The Web Content Filtering feature is purchased as a renewable subscription. The Web Content Filtering subscription includes regular updates of the content classification databases during the subscription period with signatures of the latest content classification updates.

To subscribe to the Web Content Filtering service, please contact your local Clavister Sales Representative, or visit us at: www.clavister.com for more information.

Clavister InSight™ Support

Clavister InSight™ offers excellent support for creating Web Content Filtering reports. It is easy to build reports that show individuals surf habits. It is also a great tool for optimizing Web Content Filtering. Configure your Web Content Filtering settings to be lenient to start with. Use the weekly or month Clavister InSight™ to monitor the surfing behavior. If there is a tendency to spend a lot of time on certain categories you can opt to block that category. This way you will base your blocking strategy on facts rather than assumptions.

Conclusion

This Feature Brief describes Web Content Filtering and how to use it with your Clavister SSP™ installation. Below are some key customer benefits:

Clavister SSP™ Key Benefits

- **Robust Security**
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **High Performance**
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Internet Service Provider Networks, Data Centers, and telecom operators.
- **Low Total Cost of Ownership (TCO)**
Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

Web Content Filtering Key Benefits

- Malicious Object Removal
- URL Blacklist and URL Whitelist
- Wildcard Support
- Managed Service
- Per Device Service Licensing
- Internal URL Cache
- Audit and Blocking Mode
- Override Options
- Re-classification Options
- Hourly CSPN database update
- 32 Content Categories
- Block Access to Peer-to-Peer, Phishing and Spyware sites

Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to product-marketing@clavister.com. Please include the title of the document in your email.

About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at www.clavister.com.

Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Part Number: [clavister-fbr-web_content_filtering \(0801\)](#)