Clavister Web Content Filtering

Clavister SSP™ Security Services Platform

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

clavister™

Control Freaks

- Improved security
- Increased productivity
- Lowered bandwidth costs
- Enforce regulatory compliance
- Award-winning ratings database
- Cost effective per-device services
- URL database is updated every hour
- Minimal administration
- Available in all Clavister SSP products
- High Performance
- Redundant database server network

Manage your internet resources

Effective information flows has become a strategic asset for all organizations as they face increased market competition, restricted budgets and general cut-backs. In many cases the Internet is a key business enabler, a critical part of your infrastructure or even the tool that gives you competitive edge.

Web traffic is also one of the biggest origin for security issues and misuse of company time and resources. Inappropriate surfing habits can expose your network to many security threats as well as legal and regulatory liability. Also, as a consequence, productivity and Internet bandwidth will be impaired.

Clavister SSP™ provides various mechanisms for making sure that your IT infrastructure is secure and that it is being used in a way that is appropriate at your organization:

- Dynamic Content Filtering is a powerful feature that enables you to allow or block access to web sites depending on the category they have been classified as. Dynamic content filtering requires a minimum of administration effort and has a very high accuracy.
- Static Content Filtering provides means for manually classifying web sites. This is also known as URL blacklisting and URL whitelisting.
- Finally, Active Content Handling can be used to "scrub" web pages from content that can be harmful, including ActiveX objects, Java Applets and so forth.

Features and Benefits

Increase Productivity
The Clavister Web Content Filtering feature makes it possible for you to enforce appropriate surfing policies. This means that you can block non-business related browsing and by doing so also increase the productivity of your employees.

Increase security
By blocking pages which contains for instance pornographic content, gambling, violence and similar you also block the access to sources where you are most likely to find malicious content such as viruses, worms and spyware.

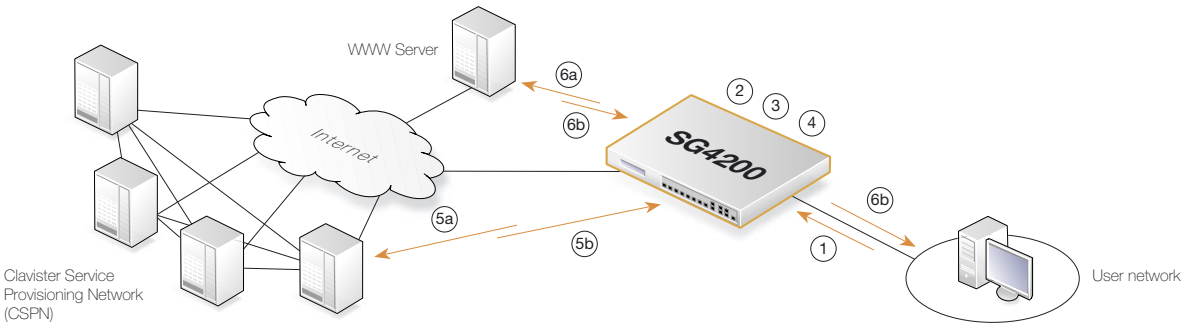
Protects against Phisihing attacks
A special task force discovers internet material that is used as a part of a phishing attack and makes sure that such material is categorized and included in the next hourly database update

High Performance
Through a proprietary connection between the Clavister devices and the global server, we limit the latency and increases the performance.

The Clavister devices also contain a local cache which stores the most commonly requested pages, this drastically decreases the number of queries that needs to be done.

if that wasn't enough, we have chosen to place the categorization servers only on high speed connections on the internet.

The basics of Clavister Web Content Filtering



1. URL Request
An employee or user requests a URL.

2. Cache lookup
The URL is picked up by the Clavister Security Gateway and compared against the entries in the local cache.

2.1 URL Found in Cache
If the URL is found in the cache it is immediately matched against the policy specified for the user and an action is taken (3).

2.2 URL Not Found in Cache
If the URL is not found in the cache, a request is sent to the categorization server within the Clavister Service Provisioning Network™- CSPN (5a). The URL is then compared to the CSPN database and a category is sent back to the Clavister Security Gateway (5b).

3. Policy lookup
When the category for the URL requested is identified the policy specified for the user is enforced and an action is taken (4)

4. Action
Depending on the category of the URL which was requested and the policies you have defined an action is taken.

4.1 URL Allowed
If the URL belongs to a category which is allowed, the user may continue and the request is sent to the server hosting the URL (6a) and the content is sent back to the user (6b).

4.2 URL Blocked
If the category of the URL is not allowed the user get different responses depending on the policy you have defined for him or her.

The optional response options are:

a) an administrator customizable block page with no possibility to continue

b) an administrator customizable page with a policy guidance message and a possibility to continue

c) an administrator customizable page with the possibility to send the URL for re-categorization

Feature List

Active Content Filtering
- Object Removal
- Active X
- Flash
- Java applets
- JScript / VBScript
- Cookies
- Invalid UTF-8 Characters

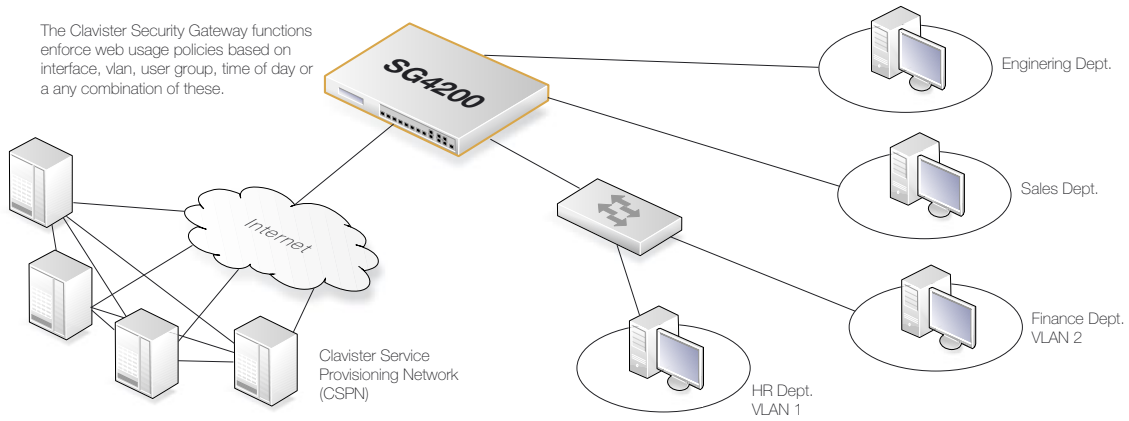
Static Content Filtering
- White -/Blacklists
- Use of wildcards

Dynamic Content Filtering
- Managed Service
- Per Device Service Licensing
- Internal URL Cache
- Audit mode
- Blocking mode
- Override options
- Re-classification options
- Customizable block pages
- Hourly CSPN database update
- 31 Content Categories
- Block access to P2P, Phishing and Spyware sites

For the enterprise

The Clavister Web Content Filtering Service offers enterprises an easy way to secure and control access to inappropriate web sites that may expose businesses to material which could jeopardize network security and consume costly bandwidth.

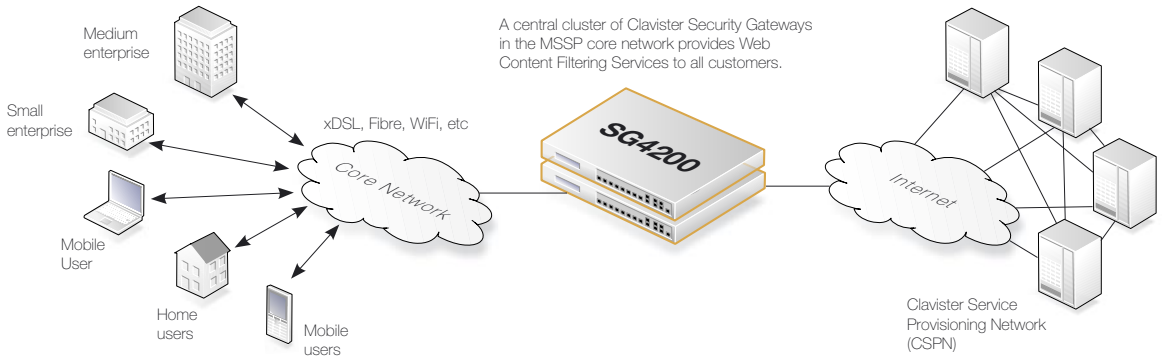
The Web Content Filtering feature is provided to the enterprise as a managed service which means that all you need to do is configure your surfing policies, all the server and database maintenance is taken care of by Clavister. Thus giving you as the enterprise a solution where you would only be taking part of the benefits but none of the costly maintenance and administration.



For the Service Provider

In the strive towards increased efficiency and productivity, especially in competitive markets, more and more customers turn to their service providers for a one-stop, out-sourced IT solution. One sector where this is especially true is the Small and Medium Enterprises (SME) as they often do not have in-house resources for managing complex IT environments, nor should they.

Clavister SSP™ and the Web Content Filtering feature is designed to function both on its own as a solution inside a customer network and as a managed service provided by an MSSP. A Service Provider can easily setup a central cluster with the Clavister SSP™ and offer filtering and/or auditing as a managed solution.



Clavister SSP™ Security Services Platform
firewall • VPN termination • intrusion prevention • anti-virus
content filtering • traffic shaping • authentication

clavister™
Control Freaks

Part number: CLA-WCF-DTS rev A01