

# Feature Brief



Clavister Anti-Spam  
September 2007

**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 and service-oriented framework for providing best-in-class security solutions. Clavister SSP™ comprises of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Its combination of precise control, fine-granular administration, and seamless scalability makes 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 telecom operator.

### Clavister Network Security Elements

The physical building blocks installed in the network. The major network security element products are the Clavister Security Gateway; pre-packaged solutions in either turn-key appliance format for easy deployment or software-only format for your preferred hardware platform.

### Clavister Lifecycle Systems™

The Clavister Lifecycle Systems™ is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, configuration, and integration, monitoring, reporting, and analysis/optimization/troubleshooting.

### 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.

Clavister SSP™ provides a secure environment for your business; 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](http://www.clavister.com).

## Overview

Organizations today are inundated with unsolicited bulk email, phishing campaigns, and other forms of spam attacks. These attacks constitute big business for e-marketers, hackers, and criminal organizations. Spam attacks are more than just annoying emails that fill up your mail box. It can also contain harmful and malicious code that can infect an entire network in seconds.

Wall Street Journal (WSJ) quoted in August 2003 analysis group Radicati Group, Palo Alto, CA which stated that "Spam accounts for 45% of all emails, or 15 billion messages every day, and costs business world-wide a total of \$20 billion a year in lost productivity and technology expenses. The firm predicts the number of daily spams will rise to more than 50 billion by 2007, and costs will reach almost \$200 billion per year." There is even fear that email might become useless in a near future because of all spam. To label spam as a mere irritation is a gross understatement.

Clavister's introduction of anti-spam functionality adds a new and important tool for administrators to curb spam attacks. Based on Domain Name Server (DNS) Blacklists (DNSBL), Clavister Anti-Spam is easy to use and effectively manages incoming emails.

## Anti-Spam

Clavister Anti-Spam supports the DNSBL, sometimes also referred to as DNS Blocklist. There are several trustworthy sites on the Internet that are working to curb spamming. These sites publish lists of IP addresses linked to spamming. Such a list is called a DNSBL. The sites themselves do nothing with these addresses, but provide them as a service for others to use. Clavister Anti-Spam utilizes these lists to block spam from these known IP addresses.

---

**NOTE: Clavister does not maintain its own blacklist; instead Clavister is querying public DNSBL's to obtain these lists. The administrator can configure which lists to query.**

---

When a Clavister Security Gateway receives a mail it is passed through the SMTP Application Layer Gateway (ALG). If Anti-Spam has been configured it will check against all configured DNSBL's to verify that the mail has not been sent from a source known for spamming.

The following steps are executed when the mail has been passed to the DNSBL control:

1. The IP address from the client is extracted from the mail. For example, IP address 192.168.42.23. This IP address is then reversed, which yields 23.42.168.192.
2. The domain name of the DNSBL is then appended. For example, `spammers.example.net` will be 23.42.168.192.spammers.example.net.
3. Perform a lookup using the compound name in the DNS, using it as a domain name. The lookup will use the DNS 'A' record for this query. This will return either an address, indicating that the client is listed; or an `NXDOMAIN`, a "No such domain" code, indicating that the client is not listed.
4. Optionally, if the client is listed, look up the name as a text record using the "TXT" record. Most DNSBL's publish information about why a client is listed as TXT records.
5. When all DNS queries has been resolved or failed, the accumulated sum is matched against the configured threshold values. The result value is sent to the SMTP-ALG which decides what to do with the mail based upon the result value.

## Weight-Point Calculation

Clavister Anti-Spam supports a weight-point system to aggregate all query replies. A weight value is added to the sum for each DNSBL reply for a given IP address lookup. The result is then compared to the configured thresholds. All values are configurable.

If a DNSBL fails, for example if the query times out, the thresholds needs to be modified, since it will be harder to reach the necessary points for the threshold. This can result in false positives. If a query is considered failed, the weight-point value will be subtracted from the thresholds when comparing against the result from the IP address lookup.

It is important to use several DNSBL's and assign weight-points to them, to minimize false-positives or false-negatives. You will base your decision on a much larger set of sources rather than relying on a single source.

## Spam Threshold

Clavister Anti-Spam utilizes a Spam Threshold, which defines when a mail should be tagged with the spam message. Such mails will be delivered to the client with the attached spam message and, if enabled, a TXT records from the DNSBL's. The Spam Threshold may be set lower or equal to the Drop Threshold. If the Spam Threshold and the Drop Threshold is equal, the Drop Threshold has precedence.

## Drop Threshold

Like the Spam Threshold, the Drop Threshold defines when a mail should be dropped, either because it is deemed to be spam or contain malicious code. It is also possible to configure an administrative mail address where dropped mail is sent to instead of the original receiver. The Drop Threshold may be set higher or equal to the Spam Threshold. If the Drop Threshold and the Spam Threshold is set equal, the Drop Threshold has precedence.

## Email Sender Verification

Spamming programs can cause the source address in the SMTP protocol header to differ from the SMTP data load header so that they do not match. An option in the SMTP ALG can verify this and act accordingly.

## Logging

Clavister Anti-Spam will log all emails that are either dropped or tagged, including the source mail and IP address, as well as the destination mail address. The log entry will also contain the weighted-point score and the reason, if provided by the list.

If a DNS Blacklist stops responding for some reason, the events are logged. This allows administrators to take appropriate action, for example, to replace the DNSBL with another or recalculate the thresholds. If all DNS Blacklists stop responding the Anti-Spam functionality will be rendered useless and all mail will be accepted. These events are logged with high severity so that administrators can take appropriate action.

---

**NOTE: The logging is done within the scope of the SMTP-ALG.**

---

## Clavister PinPoint™ Support

The Clavister Anti-Spam function is also supported with Clavister PinPoint™. Various statistics can be obtained from the DNSBL object for use in e.g. PinPoint:

- Hits on specific DNS Blacklist
- Total number of mail in the DNS Blacklist object
- Number of accepted mail
- Number of spam-tagged mail
- Number of dropped mail
- Specific DNS Blacklist active or failing

Statistics are persistent through reconfigurations and can be cleared via the CLI command.

## Conclusion

This Feature Brief describes Clavister Anti-Spam 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.

## Clavister Anti-Spam Key Benefits

- Support for multiple and user definable DNS Blacklists
- Enables you to use any or all of your favorite spam list servers, both commercial and free versions, or a mix of both for optimal performance, resiliency and cost efficiency
- Adds a second level of spam verification or even replace dedicated spam verification servers
- Increases the overall network security by limiting spam from being the source of malware
- Increases productivity by removing unwanted spam
- Rapid deployment as no additional hardware or software needs to be installed
- Weight-Point Calculation improves accuracy by reducing both false-positives and false-negatives
- Clavister PinPoint™ compatibility and support which allows you to get a quick overview of the current spam situation

## 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](mailto: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](http://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-anti-spam-a001