

# Feature Brief



## Threshold Rules

### 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](http://www.clavister.com).

## Overview

More and more organizations depend on Internet today in their day to day business. Email, Web, and Web-based business applications are pervasive and mission-critical. Unfortunately, the Internet is also the main vehicle for threats such as viruses, worms, and Trojan horses. Security has become one of the main topics for the IT/IS department to tackle. For the IT/IS department it is important to be able to observe and react to signs of abnormal traffic activity. For example, an internal host could become infected with a virus and start making repeated connections to external IP addresses, or an external source trying to open excessive number of connections.

Add to this the general Quality of Service (QoS) issues, with constant fight for to maintain bandwidth for all branches and offices.

Threshold Rules is an important part of traffic management and can help IT/IS department to curb security threats and a higher level of Quality of Service.

## Threshold Rules

Threshold Rules enables you not only to detect abnormal connection activity, but also to react to it. A Threshold Rule is like a normal policy-based rule and supports all types of connections, such as TCP, UDP, and ICMP. The following text will detail how you can configure Threshold Rules to support your needs.

As with other rules in Clavister Security Gateway, you name the Threshold Rule and you specify an address filter. A Threshold Rule can also be associated with a specific Service, such as HTTP or FTP. This can be useful if you want to create separate Threshold Rules for specific service. You can also configure the Threshold Rule to be active in accordance with a predefined schedule. This gives you all the power to create Threshold Rules that exactly match your requirements.

### Action

Each rule can have associated with it one or more Actions, which specify how to handle different threshold conditions. You select whether the rule should perform an Audit action when the specified threshold is exceeded or if the rule should perform a Protect action. If you select Audit, the rule will leave the connection intact but log the event. If you select Protect, the triggering connection will be dropped. If you want to log this connection attempt, you need to check the "Generate Log Message" checkbox.

It is possible to set multiple Actions for a given rule. This allows you to set an Audit for a given threshold but also to add a Protected for a higher threshold value.

If you can not determine the threshold value beforehand, it is recommended to use an Audit Action.

---

**NOTE: Some Advanced Settings known as `BeforeRules` settings can exempt certain types of connections for remote management from examination by the rule sets, including Threshold Rules. For more information on Advanced Settings, please read "Clavister CorePlus™ Administration Guide"**

---

### Threshold Type

It is possible to configure if the threshold is applied separately to connections from different IP addresses, or if it applied to all connections matching the rules as a group.

You can configure it to be Host Based, which means that the threshold should be applied separately to connection from different IP addresses. You can also configure it to be Network Based, which applies to all connection matching the rules as a group.

### Threshold

The Threshold parameter specifies how the measurement techniques are to be applied. You can choose between Maximum Number of Connections per Host/Network or Maximum New Connections per Second, also on a per host/network basis. When the number of connections per second threshold is reached, the specified action will trigger.

This feature can be very useful in order to limit the impact of Peer-to-Peer (P2P) usage in large networks, which can use a lot of a company resources. It can also mitigate the impact from viruses or worms that might try to create a DoS attack against a network by setting up many connections.

### Log Settings

It is also possible to configure whether the triggered Action should be logged or not. You can also specify if you want to override the Event Severity level and set a different Event Severity level. For information on Severity levels and log format, please consult "Clavister Log Reference Guide".

## Blacklist

When a Protected action is used it is possible to automatically add the offending source to a Blacklist of IP addresses or networks. If you have specified a Host-based Threshold Type it will blacklist a single host when triggered. If you have specified a Network-based Threshold Type it will blacklist source network associated with the Threshold Rule.

You also specify how long the host or network should be blacklisted. The host or network will be blacklisted for the specified number of seconds and then removed from the black-list.

If the Threshold Rule is associated with a specific Service you can specify that only that Service should be blacklisted.

It is also possible to choose whether established connections from the offending source should be left unaffected or if they should be dropped. Check the "Exempt Established Connection from Blacklisting" checkbox to allow established connections to be left unaffected.

The Blacklist is also used by the Intrusion Detection and Prevention (IDP) module, which also adds hosts or networks to the list. It should be noted that the Blacklist is maintained even if the Clavister Security Gateway is shut down or rebooted.

## Increasing Security

### Managing Attacks

One important aspect of the Threshold Rules feature is the ability to detect abnormal connection activities. This can be used to detect denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks. A DoS or DDoS attack is an attempt to make a computer resource unavailable to its intended users. Perpetrators of these attacks typically target sites or services hosted on high-profile Web server. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by:

- forcing the targeted computer or computers to reset, or deplete its resources such that it can no longer provide its intended service; and/or,
- obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Configuring Threshold Rules to monitor unusual or abnormal connection activities works both for incoming traffic as well as outgoing traffic. It might be the case of an worm-infected internal net that causes an abnormal number of connections to be opened.

Figure 1 below illustrates how this connectivity pattern can look like. Over some time the network opens a varying number of connections, but at some point in time there is a surge of new connections opened. This will trigger the Threshold Rule actions and restore the network to normal conditions.

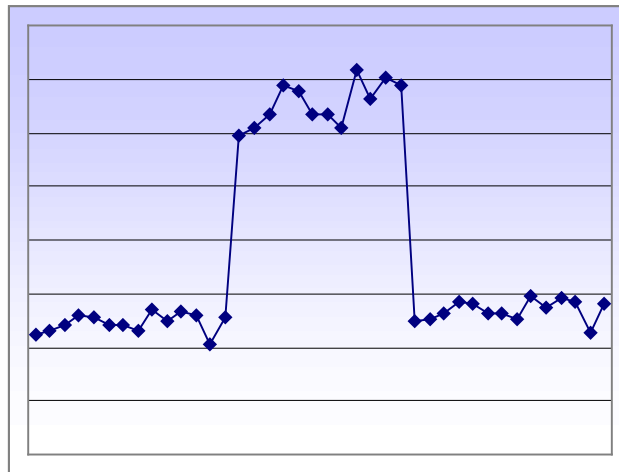


Figure 1: Abnormal connectivity pattern

This is one example on how Threshold Rules can help protect your network against DoS or DDoS attacks in an efficient way. Below is another example on how to use rate limiting on services to managing attacks.

## Rate Limiting Services

Another possibility to manage attacks is to configure a rate limit on services. Figure 2 below illustrates a possible traffic pattern, where the blue illustrates ICMP traffic and the grey illustrates typical regular day-to-day business traffic. At some point in time there is an attack with a dramatic increase in ICMP traffic, which consumes the headroom for regular traffic. Eventually the system is brought to a stand still and the attack has succeeded.

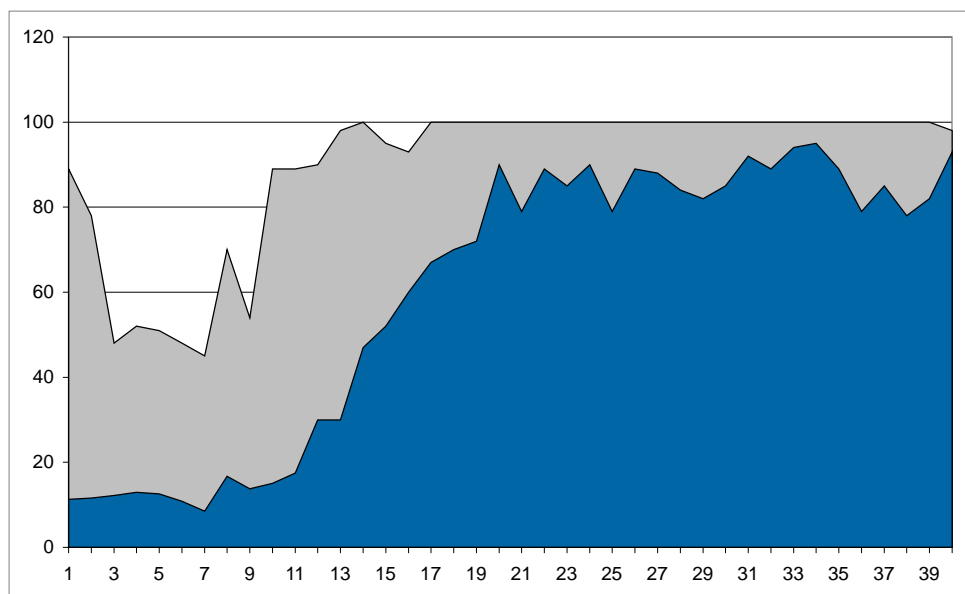
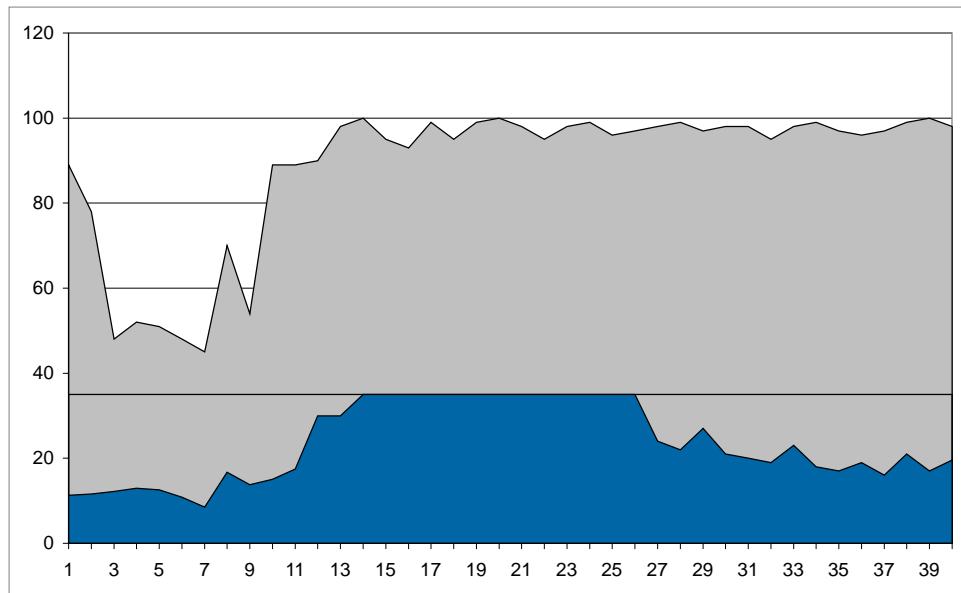


Figure 2: Traffic Pattern without Rate Limited Services

To manage these types of attacks using services, it is possible to set a rate limit on a specific service, in this case ICMP. In Figure 3 below there is a rate limit configured for ICMP, which effectively caps the number of connections at a certain level. The effect is that when the attack starts the number of connections increase but is effectively stopped until the attack has failed.



**Figure 3: Traffic Pattern with Rate Limited Services**

Below is another example on how to use the blacklist feature of Threshold Rules.

## Threshold Rules – A Step-by-Step Example

When configuring Threshold Rules you generally follow the following steps:

1. Decide Rate Limit policies  
How many connections should you allow? Should you protect or only audit offending connections, and should you blacklist the offending connections? These and other questions should be clear before you start to configure your Threshold Rules.
2. Configure Threshold Rules according to the policies specified above  
Use Clavister FineTune to configure the Threshold Rules according to the specified policies.
3. Verify that the Threshold Rules works according to the policies  
It is important that the Threshold Rules work correctly so you need to verify them before going live.

In this example we want to create a Threshold Rule that limit LAN users from accessing any interface/network with more than 5 connections per second. When the rule is triggered we will block offending connections for 30 seconds, but only for the offending service. We will also log all events so we can examine the log files to verify that the rule works correctly. Please follow the instructions below to complete this example.

1. Start your Clavister FineTune application, if it is not already started, and select the Security Editor from the Tools menu.
2. Right-click on the Security Gateway to bring up the contextual menu and select Version Control > Check Out. You can also select the Security Gateway and use Ctrl-O.
3. Expand the Security Gateway by clicking on the + (plus) sign. Expand the Traffic Management folder by clicking on the + (plus) sign.
4. Right-click on the Threshold Rules icon to bring up the contextual menu and select New Threshold Rule.... You can also select the Threshold Rules icon and use Ctrl-N.
5. The Threshold Rule Properties dialog is shown. Select the Threshold Rule tab and enter the following information for our first pipe:

```
Name: LAN_Limit
Source Interface: lan
Source Network: lannet
Destination Interface: any
Destination Network: all-nets
```

6. Select the Service tab and enter the following information:

```
Pre-defined: All
```

7. Select the Rule Action tab and create a new rule action. You create a new rule by clicking on the + (plus) sign. Enter the following information in the Rate Limit Action dialog:

```
Action: Protect
Threshold Type: Host-based
Threshold: 5
Generate Log Message: Yes
Automatically Add to Blacklist: Yes
Time to Block Host/Network: 30
Block only this Service: Yes
```

8. Click OK several times to accept all changes.

You can verify the configuration by surfing to a Web page with lots of advertising, which should generate a lot of connections. Verify in the log that the rate abuse was detected and verify that the browser was blocked for 30 seconds. Remember to disable Pipe Rules after you have verified the configuration.

## Conclusion

This Feature Brief describes Threshold Rules and how to use them 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.

## Threshold Rules Key Benefits

- Configurable measurement techniques
- Support for multiple actions
- Support for both audit and protection
- Flexible Blacklisting functionality
- Increased security by detecting abnormal connection activities

## 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-threshold\\_rules](#) (0801)