

Feature Brief



Policy-Based Server Load Balancing

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.

Server Load Balancing

Clavister Security Gateway comes with an integrated Server Load Balancing feature, which turns it into an intelligent, high-availability load-balancing device for any company's server farms, no matter if they are public Web servers or internal applications.

The Server Load Balancing (SLB) feature included in the Clavister Security Gateway is closely integrated with the Clavister Security Gateway core functionality, which is activated/deactivated as a part of a policy set, thus making it highly flexible and configurable.

Server Load Balancing in Clavister Security Gateway has the following key features:

- Load Distribution
- Server Monitoring

Load Distribution

The Load Distribution feature is responsible for distributing packets to destination servers/applications according to the chosen distribution method and distribution algorithm.

Distribution Modes

The mode of distribution controls the way connections are established between the client and the server. There are three distinct distribution modes - Per-State Distribution, IP Address Stickiness, and Network Stickiness.

Per-State Distribution

This model can record state of every distribution. Based on this state information is possible to transfer complete session to the same server. The Per-State Distribution model guarantees reliable data transmission.

IP Address Stickiness

In this mode, all connections from a specific client will be sent to the same server. This is particularly important for SSL services such as HTTPS, which require a consistent connection to the same host.

Network Stickiness

Essentially the same as IP Stickiness, but the difference is that a netmask is applied to determined the uniqueness of an IP address.

Algorithms

The Server Load Balancing feature in Clavister Security Gateway use different algorithms to ensure optimal traffic throughput. The goal of these algorithms is to intelligently distribute load and maximize the utilization of all servers within a cluster. Clavister Security Gateway support two algorithms - Round-Robin and Connection-Rate.

Round-Robin Algorithm

The Round-Robin algorithm redirects the network connections to a different server in a round-robin manner. It treats all real servers as equal regardless of number of connections or response time. This algorithm is suitable when the real server of cluster have equal processing capabilities.

Connection-Rate Algorithm

The Connection-Rate algorithm redirects a connection to the server with the least number of connections in a predefined timespan. New connections are saved in an array that tracks how many connection was made each second. The array is updated each second. This algorithm is suitable in a heterogeneous server environments, where real servers or cluster have different processing capabilities.

Server Monitoring

Performing various checks to determine the health of servers and applications is one of the most important benefits of the Server Load Balancing feature. Clavister Security Gateway can perform certain network-level checks at different OSI layer, which makes server monitoring both flexible and powerful.

When a server/application fails, it is removed from the active server/application lists and traffic is not routed to it until the server or application is restored.

ICMP Ping

Clavister Security Gateway pings the real server IP address. A ping is used to check whether the server is available. This is also known as "heartbeat".

TCP Connection

Clavister Security Gateway attempts to connect or bind to configured ports where applications are running. For example, if the server runs a Web application on port 80, Clavister Security Gateway attempts to establish a connection or attempts to bind to that port. The Clavister Security Gateway sends a TCP SYN request to port 80 on each physical server and checks for a TCP SYN/ACK in return. If the connection or bind fails, Clavister Security Gateway marks the port 80 to be down on that server.

Load Distribution Scenario

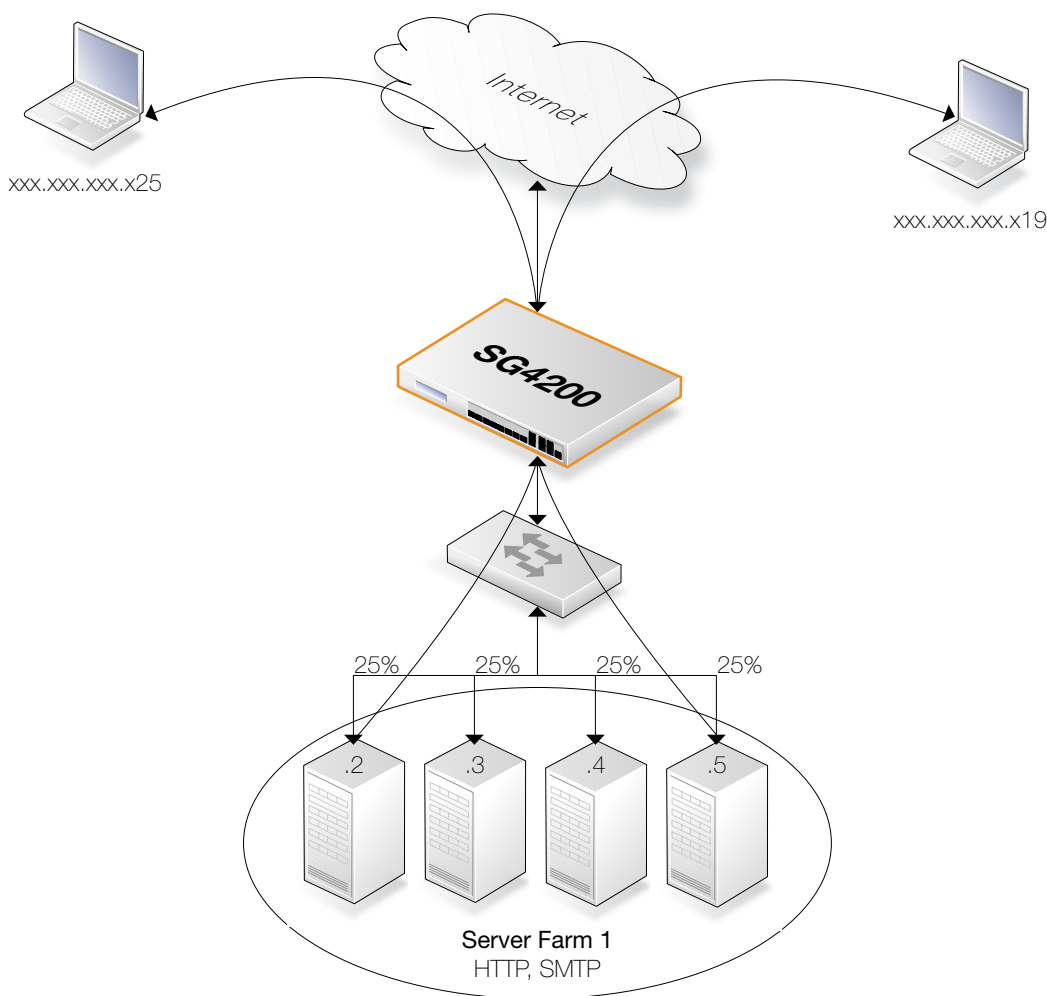


Figure 1: Server Load Balancing

Server Load Balancing is very commonly used for distributing HTTP traffic across a farm of Web servers to achieve higher performance, shorter response times and increased resiliency.

As most Web applications are session based, it is required that the clients connects to the same physical Web server during their entire session.

By configuring the Clavister Security Gateway to run Server Load Balancing with IP Address Stickiness distribution mode, it is possible to achieve powerful load balancing, and at the same time assure that the client will be routed to the same physical server during the entire session.

Questions and Answers

When does Server Load Balancing in Clavister Security Gateway make sense?

Clavister Security Gateway with Server Load Balancing is the answer to three key issues when it comes to server clustering; Availability, Scalability and Simplified Administration.

Availability

- Q:** How does Server Load Balancing provide increased availability?
- A:** Clavister Security Gateway provides increase availability by adding redundancy and eliminating single point of failures. It adds the possibility to guarantee availability to critical systems and services.
- Q:** What happens if the Clavister Security Gateway itself stops functioning for some reason?
- A:** Clavister Security Gateway is built for resilient solutions and provides the capability to have redundant gateways which automatically takes over the role as active gateway in the rare case of hardware failure.
- Q:** How many servers can you add to a cluster provisioned by the Clavister Security Gateway?
- A:** Clavister Security Gateway is built to function even in the extreme scenarios and there is no exact limit to how many servers you can place in a server farm, however there are of course practical limits, such as financial limits.
- Q:** What happens if a server or application in the cluster ceases to work?
- A:** If a server or application provisioned by Clavister Security Gateway ceases to work the Health Monitoring mechanism detects the problem and automatically stops routing traffic to the malfunctioning host and balances the load to the other servers.

Scalability

- Q:** In what way does Server Load Balancing provide scalability?
- A:** Clavister Security Gateway increase scalability by allowing the administrator to easily add more servers to a cluster and to expand with the growing need for performance and availability.
- Q:** What value does this scalability provide to our company?
- A:** By enabling your company to easily expand the server farm you can balance the need for performance against current financial means. This type of scalability also makes it possible to purchase less expensive main-stream servers instead of expensive cutting- edge technology servers in order to stay ahead.

Simplified Administration

- Q:** Administration is a time-consuming task for us since service availability must be guaranteed at all times, does the Clavister Security Gateway help us simplifying this task?
- A:** Yes, as there are no single points of failure you can easily disable one or more servers to perform maintenance whilst providing the critical service without any interruptions.

Conclusion

This Feature Brief describes Policy-Based Server Load Balancing 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.

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-policy-based_server_load_balancing (0801)`