

# Feature Brief



## Transparent Mode

### 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).

## Transparent Mode

Layer 2 - Transparent Mode or "stealth-mode" simplifies deployment of Clavister Security Gateway's into existing networks, decreases maintenance and strengthens security.

Transparent Mode helps to ease the administration work as there is no need to reconfigure any equipment when a Clavister Security Gateway is introduced into the network communication flow, configured to operate in Transparent Mode .

Transparent Mode simply makes the Clavister Security Gateway act as a "stealth-gateway" that is easy to deploy, invisible to users and undetectable for intruders.

Transparency in this case refers to the visibility of a Clavister Security Gateway. A gateway is considered transparent to its users if the users do not notice its existence in the packet flow. When adding a transparent gateway into an existing network structure, the Clavister Security Gateway provides the following advantages:

- No reconfiguration required – clients can keep the same network configuration after the gateway has been installed.
- Rapid deployment – Clavister Security Gateway running in Transparent Mode provides hassle and effortless deployment.

- Enhanced security – in Transparent Mode, a Clavister Security Gateway is undetectable for hacker's and intruders thus making it more secure.

Clavister Security Gateways can operate in two modes: **Routing Mode** & **Transparent Mode**. In normal Routing Mode, the gateway acts as a Layer 3 router. If the gateway is placed into a network for the first time, or if there is any topological change within the nodes, the routing configuration must be thoroughly examined to ensure that the routing table of the gateway system is consistent with the current network layout. Reconfiguration of IP settings is also required for existing routers and protected servers. This mode works well when complete control over routing is a desired option.

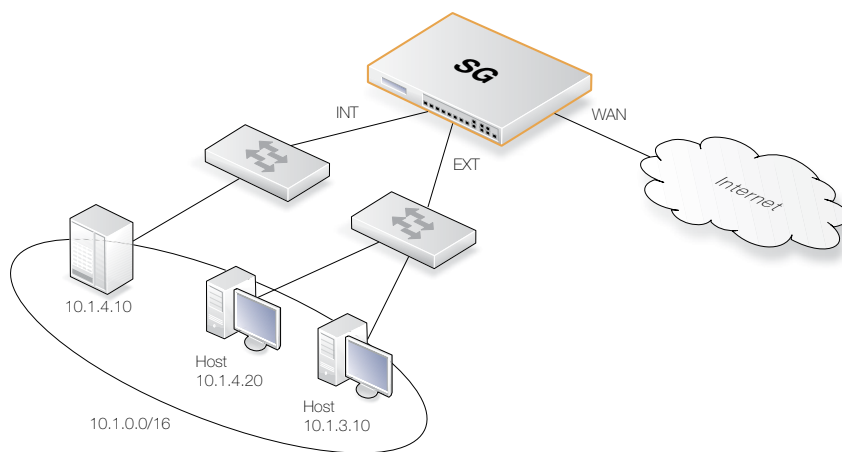
While operating in Transparent Mode, the Clavister Security Gateway acts more like a switch. It screens IP packets traversing the gateway and forwards them transparently to the correct interface without modifying any of the source or destination information. All transparent interfaces are considered to be in the same network, so if one client moves to another interface it can still obtain the same services as before without any routing reconfiguration.

In Transparent Mode the Clavister Security Gateway act similar to Layer 2 switches, thus allowing ARP transactions to pass through the system. By learning from the ARP traffic that passes through the Clavister Security Gateway it understands the relation between the IP address and the physical address of the source and destination. During all the transaction, none of the endpoints will be aware of the Clavister Security Gateway working in between.

## Transparent Mode Scenario

This scenario shows how a Clavister Security Gateway configured to operate in Transparent Mode can be used to separate server resources from the internal network by attaching them to a separate interface without the need of different IP-address ranges.

Servers containing resources that are accessible from the outside could be a security risk if they are placed directly on the internal network. Because of this, such servers are often connected to a separate interface on the firewall, like DMZ.



**Figure 1: Transparent Mode Scenario**

In this scenario all hosts connected to `int` and `dmz` interfaces on the Clavister Security Gateway share the 10.0.0.0/24 address space. As this is configured using Transparent Mode, any IP address can be used for the servers, and there is no need for the hosts on the internal network to know if a resource is on the same network or placed on DMZ. This makes the Clavister Security Gateway transparent in the communication between DMZ and LAN even though the traffic can be restricted using the Clavister Security Gateway's IP rules.

In this case, users on the internal network are allowed to communicate with an HTTP server on the DMZ. Furthermore, the HTTP server on the DMZ is allowed to be reached from the Internet. Additional policies can be added to allow other traffic. An IP address

10.1.4.10 is used as the HTTP server's address in this scenario. We assume that this address has been defined as a local object in the section **Hosts & Networks**, named `dmz_server`.

## Questions and Answers

When does it make sense to use Layer 2 Transparent mode in Clavister Security Gateway?

Transparent mode in Clavister Security Gateway provides several benefits but mainly in the area of simplifying deployment and enhancing security.

- Q:** Simplified deployment sounds nice, but what does it mean in reality?
- A:** A Clavister Security Gateway operating in transparent mode does not require any changes in the network topology. This means you do not need to perform any additional reconfiguration on existing equipment when a new Clavister Security Gateway is introduced into the network.
- Q:** Is it possible to configure Transparent Mode per individual virtual system in Clavister Security Gateway?
- A:** Yes, it is possible since Transparent Mode is integrated in the Clavister Security Gateway code and can be configured in much the same way as routing.
- Q:** I read something about Transparent Mode in combination with VPNs; what does this mean and how can I benefit from it?
- A:** Yes, Clavister Security Gateway can combine Transparent Mode and VPNs, the benefit of this is that you get a much simpler administration of you remote VPN gateways and roaming clients. There is no need to configure or reconfigure any settings for remote networks or similar.
- Q:** In most of Clavister's competitors products you can not have both dynamic and static addresses in Transparent Mode, which causes us lots of problems and is very costly to get around. Does Clavister provide a solution to this?
- A:** Yes, with Clavister Security Gateway it is possible to use both static and dynamic addresses in Transparent Mode.

## Conclusion

This Feature Brief describes Transparent Mode 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.

## Transparent Mode Key Benefits

- Both dynamic and static address translation in Transparent Mode
- Undetectable for hacker's and intruders in Transparent Mode
- Hassle-free and effortless deployment
- IPsec, L2TP and PPTP in Transparent Mode does not need static routes to remote gateways
- Unit administration does not require static routes to management systems
- No reconfiguration required – clients can keep the same network configuration after the Clavister Security Gateway has been installed
- Transparency and routing coexistence - routed destinations can coexist with an otherwise transparent network on the same interface and/or VLAN
- Virtual Transparent Systems - transparency may be individually configured for virtual systems with separate CAM tables
- Full MAC address transparency - units moving from one segment to another, for example wireless roaming, do not need to wait for ARP cache timeouts
- Lossless learning - packets are not dropped while destination discovery is in progress

## 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-transparent\\_mode](#) (0801)