

Security Gateway Series



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

CLAVISTER™

Control Freaks

CLAVISTER™

Clavister SSP™ – Security Services Platform

Clavister makes what we believe to be the best Security Services Platform in the world. Customers (mainly security integrators, enterprises and service providers) use it as a firewall, a virtual private networking (VPN) terminator, an intrusion prevention system, a traffic shaper, a virus blocker, a content filter and/or any combination of the above.

Our customers use our products at the heart of their security infrastructures, taking advantage of the unique combination of super-granular control and seamless scalability that we offer.

Key features

Modularity – This allows you to provision (and pay for) only the functionality you need including firewall, VPN termination, IDP, anti-virus, traffic shaping, authentication and web content filtering.

Seamless scalability – Our xPansion™ Lines licensing philosophy means we offer a single, identical platform that is applied to all sizes of requirement.

There are no time-consuming upgrades and service pack installations to be done (as is common with many other vendors). Any upgrades that are required (to handle newly emerging threats, for example) are handled automatically online from a central management station.

Clavister CorePlus™ kernel – At the heart of Clavister SSP lies an in-house developed, high-performance kernel with an invisible attack surface and air-tight component integration. We write every line of code ourselves to ensure that it all works perfectly together at staggeringly high performance levels.

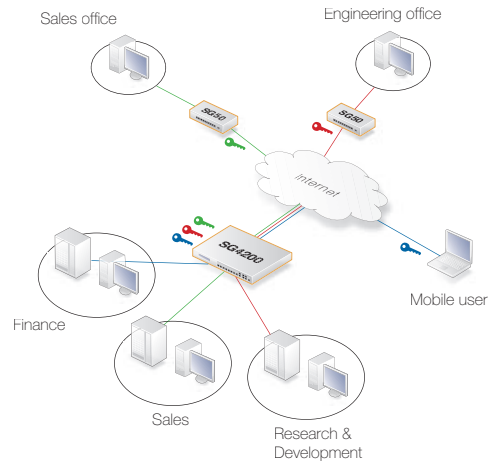
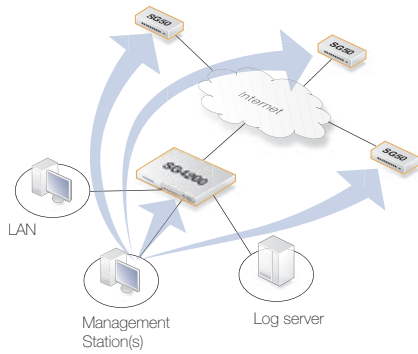
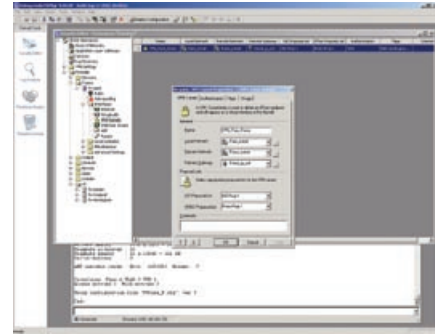
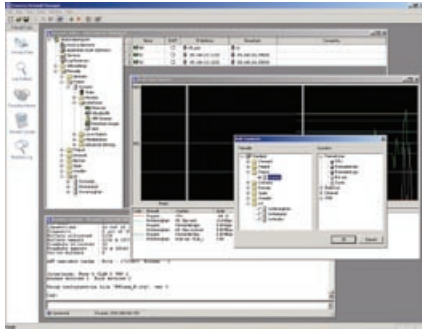
This stands in direct contrast to most security products on the market which piece solutions together from several different sources.

Based on Clavister Service Oriented Security (SOS)™ – Our goal is to allow customers the benefit of granularity and provide the greatest freedom to configure and optimize their security solution to exactly meet their specific needs. Our SOS design philosophy means that, where possible, we avoid integrating third-party code.

SG 50



System Performance and Capacity	51	53	55	57
Plaintext Throughput (Mbps)	50	75	100	200
AES/3DES Throughput (Mbps)	20/20	20/20	40/40	40/40
Concurrent Connections	4,000	8,000	16,000	32,000
Concurrent VPN Tunnels	25	50	100	200
Ethernet Interfaces	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX
Virtual Interfaces (VLAN)	4	8	32	64
Virtual Systems & Virtual Routers	5	5	5	5
Mode of Operation				
Layer 2 mode (transparent mode)			Yes	
Layer 3 mode (route mode)			Yes	
Policy-based NAT/PAT			Yes	
Policy-based Server Load Balancing			Yes	
Virtual IP			Yes	
Firewall				
Network Attack Detection/Prevention			Yes	
DoS and DDoS Detection/Prevention			Yes	
VPN – Virtual Private Networking				
AES, 3DES, DES, Twofish, Blowfish, CAST-128 Authentication			Yes	
X.509 Certificates, Pre-Shared Keys			SHA-1, MD5	
Self-Signed Certificates			Yes	
IPSec NAT Traversal (NAT-T)			Yes	
VPN Tunnel Keep-alive			Yes	
L2TP and PPTP Client / Server (LNS/PNS)			Yes	
Application Layer Gateways				
FTP			Yes	
H.323			Yes	
HTTP			Yes	
SMTP *			Yes	
Content Security				
Intrusion Detection & Prevention			Yes	
Web Content Filtering			Yes	
Antivirus *			Yes	
Bandwidth Management				
Policy-based Bandwidth Management			Yes	
Guaranteed / Maximum Bandwidth			Yes	
Dynamic Bandwidth Balancing			Yes	
Addressing and Routing				
Static IP			Yes	
Policy-based Routing (PBR)			Yes	
OSPF			Yes	
Proxy ARP (Transparent Mode)			Yes	
DHCP Client, Server and Relay			Yes	
PPPoE			Yes	
GRE			Yes	
Multicast - IGMP			Yes	
Logging / Monitoring				
Clavister Firewall Logger			Yes	
Real-time Log Viewer			Yes	
Graphical Log Analyzer			Yes	
Real-time Performance Monitoring			Yes	
SNMP Polling			Yes	
Management				
Local Console			RS232	
Command-line based Remote Management			Yes	
Graphical Enterprise Remote Management			Yes	
User Authentication				
External RADIUS User Database			Yes, multiple servers	
CHAP, PAP			Yes	
VPN IKE XAuth			Yes	
High Availability				
Firewall and VPN state Synchronization	No	No	No	Yes
Dead Link, Gateway & Interface Detection	Yes	Yes	Yes	Yes
Route Failover, Interface Failover	Yes	Yes	Yes	Yes
Average Failover time	-	-	-	< 800 ms



All Clavister Security Gateways include a Centralized, enterprise security management system used for configuration and monitoring of multiple devices.

Clavister products are ideal components in any VPN solution.

About Clavister

Clavister is a leading developer of high-performance IT/IP security. The products, based on unique technology, include carrier-class firewalls and VPN solutions. They have been awarded preferred choice by international press and are in use today by thousands of satisfied customers. In short; In a world where people depend on information,

Clavister provides complete security solutions more cost-efficient than any competitor, always with Your business in mind.

Clavister was founded 1997 in Sweden. Its R&D and headquarters is situated in Örnsköldsvik, Sweden and its solutions are marketed and sold through sales offices, distributors and resellers in Europe and Asia. Clavister also offers its technology to OEM manufacturers.

Clavister SSP™ Security Services Platform

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

CLAVISTER™

Control Freaks

