clavister

Clavister W20



Next-generation firewall with excellent scalability, performance and functionality

FEATURES AT-A-GLANCE

- Cost-effective next-generation firewall for larger remote/branch office or for entry-level enterprise solutions, housed in a sleek 1U 19" rack appliance, delivering up 6 Gbps of firewall performance (plaintext throughput)
- Next-generation firewall services, including Clavister True Application Control, Clavister Content Security Services and User Identity Awareness
- Powerful stateful firewall with deep-packet inspection gives you a high level of security
- Flexible, dynamic routing and connectivity with support for link aggregation
- Built-in support for both IPsec and SSL VPN offers easy to use remote connectivity
- Centralized Security Management System included free-of-charge in the Clavister Security Subscription package
- High-end network infrastructure, such as traffic management, High Availability (HA), server load balancing and WAN load balancing, are all included with Clavister Subscriptions
- The perfect solution for remote offices, branch offices and entry-level enterprises

The Clavister W20 is a set of beautifully designed next-generation security appliances, targeted towards remote/branch offices and as entry-level enterprise security gateways. The Clavister W20 delivers next-generation firewall security at a break-through price point, offering advanced routing flexibility and comprehensive features without compromising security.

The Clavister W20 is an ideal solution for any organization that need premium network security in a cost-effective package.

Next-Generation Firewall Services

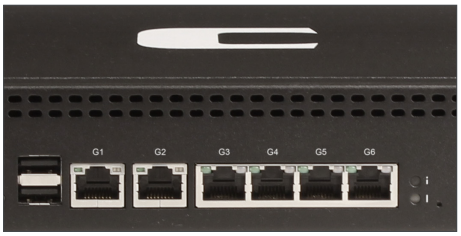
True Application Control

Clavister W20 fully supports True Application Control – one of our next-generation firewall security services.

Enabling True Application Control will help you to manage applications used in your network more safely. With added security you lower your overall risk exposure and as a result, costly security incidents and downtime can be avoided. It also gives you valuable insight in which applications are used by which user, and can therefore prioritize business critical application and increase your overall business productivity.

True Application Control not only recognize more application and data, it understands how these application behave and can act immediately on malicious behavior.

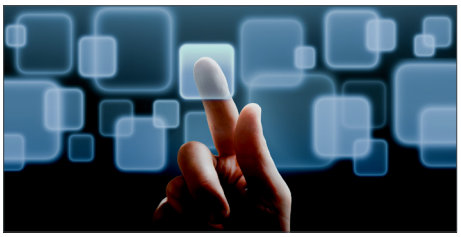
With its unique support for Deep Application Content Control (DACC) technology, our application control can perform in-depth analysis and control of application content with higher degree of control. DACC enables you to understand and visualize Skype IDs, SQL queries, Facebook chat text, VoIP call information and much more.



Connectivity Choices

The Clavister W20 is equipped with six 1GbE (RJ45) connectors. Thanks to the flexible routing capabilities of the Clavister W20, any port can be fully configured. This means you can configure access to management interfaces on a shared port or dedicate one specifically for the purpose. You can also choose to dedicate any selected port as the High Availability (HA) synchronization port in clustered High Availability configurations.

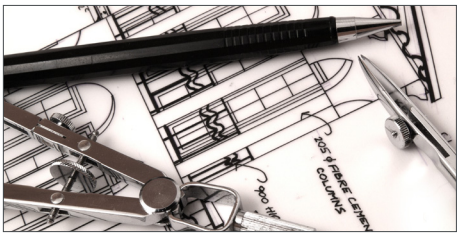
Clavister W20 also support link aggregation, which means that you have the added benefit of maximizing throughput and increase the resilience of your system.



RADIUS Relayer – Pinpoint Security

Clavister W20 includes support for RADIUS Relayer, which can provide user information and DHCP IP provisioning for RADIUS-based authenticated users.

For example, when a user roams over from a cellular network to an Enterprise Wi-Fi network for data access. This is useful as it allows for granular user and group-based policing of traffic and controlling access to network resources.



Advanced Routing

The Clavister W20 provide an advanced routing engine, including Policy-Based Routing, with seamless route failover. This allow for Dynamic Policy-Based Routing where traffic can be routed based on dynamic events, such as User Identity, latency, HTTP Get responses, etc.

This enable you to create truly flexible and sophisticated policies that reflect the true requirements of your network.

Clavister SSL Inspection for Application Control provides a high performance and non-intrusive way to identify and control even SSL encrypted applications.

True Application Control is included in the Clavister Security Subscription (CSS) service.

Content Security Services

Having a regular firewall is not enough to prevent attacks from happening on your network. As attacks become more severe and the threat landscape becomes more dynamic, additional measures need to be in place to protect your network. Clavister offers best-of-breed content security services, including Intrusion Detection and Prevention System, network-centric Anti-Virus from Kaspersky Labs, and Web Content Filtering to add an additional security layer to your firewall. These content security services protect your network from advanced threats your firewall alone cannot stop. The Content Security Services are included in the Clavister Security Subscription (CSS) service.

User Identity Awareness

User Identity Awareness (UIA) provides granular visibility of user identity, and enables you to control network access at the user level. The User Identity Awareness together with our True Application Control functionality will provide you with an extremely powerful and versatile tool for granular visibility and control of “who-does-what-and-when” in your networks. You will have the ability to pinpoint user access to applications across both wired and wireless networks regardless of connecting device.

True Security Values

Clavister Subscriptions

We believe our customers should have choices. We also believe you should have it all. Therefore we offer you a choice between our comprehensive Clavister Product Subscription (CPS), or our all-inclusive, full service option, Clavister Security Subscription (CSS).

Clavister Product Subscription

The Clavister Product Subscription contains a high number of product service, such as software updates, centralized management support and flexible service plans.

CPS includes a hardware replacement service to offer you the best possible protection in case a hardware failure should occur. Finally to ensure you get the best out of your Clavister security gateway, we provide you with around-the-clock support from our award-winning technical support team – your dedicated resource with highly skilled engineers that help you out in case of need. The Clavister Product Subscription keeps your Clavister updated, online and ready for business twenty-four-seven.

Clavister Security Subscription

Clavister Security Subscription is a complete, all inclusive suite of product services. It contains all the services you get with Clavister Product Subscription, but extends the service offering by including a full set of next-generation firewall services, such as Clavister True Application Control, Web Content Filtering, Anti-Virus and Intrusion Detection and Prevention (IDP).

CSS offers best-in-class content services, which protect you from the more advanced types of malware and exploits. It grants you access to the latest software and signature updates keeping your infrastructure up to date and increasingly more stable and secure.

All Clavister Subscriptions are available in 12, 24, 36, 48 and 60 months service terms, offering you maximum security and flexibility.

For more information about Clavister Subscriptions, see the separate **Clavister Subscriptions** brochure.

True Flexibility – Get more performance when you need it

Clavister W20 is available in two models, each addressing specific customer requirements. Should your performance needs increase, Clavister offers you the flexibility to upgrade to a more powerful Clavister W20 without having to invest in new hardware. Just simply order the upgrade to your preferred Clavister W20 model and install the new license file. It is as simple as that.

This makes Clavister W20 a low risk choice in dynamic business environments where requirements can change overnight. Clavister provides you the performance when you need it, avoiding high up front investment costs to your security infrastructure or having to worry about costly upgrades.

Uptime Technologies

Clavister W20 comes with powerful features to ensure that your network infrastructure is online and ready for work. Features like High Availability (HA) is fully supported, as well as Fast Route Failover technologies and link aggregation, which ensures that your business is not affected by network downtime caused by link failure or hardware problem. It also support flood protection technologies to increase uptime in case your network is subjected to a Denial-of-Service (DoS) attack.

Powerful Firewall

The Clavister W20 is a next-generation firewall, but it also has all the traditional security features, such as stateful firewall with deep-packet inspection, and it is powered by our own in-house developed network security operating system, the Clavister cOS Core. As well as providing all traditional firewall functions, such as port blocking and proxy server, all Clavister firewall solutions incorporate next-generation firewall features to detect and block sophisticated application-level attacks. This means higher level of security, higher traffic throughput and minimal use of system resources.

Performance

Clavister W20 provides next-generation security services across all points of your network without sacrificing performance throughput. Purpose-built hardware running on our highly efficient network security operating system ensures that the firewall performance throughput is one of the highest in the industry, making sure that your Clavister firewall will not be a bottleneck in your network infrastructure.

Simplicity

We strive to make things easy to understand and easy to use. This includes everything from hardware design to security management. We build highly customizable enterprise-grade firewalls, and despite the inherent complexity, we make an effort of making it easy to use. For example, our highly acclaimed centralized security management system, Clavister InControl uses color-coded attribute groups to provide a clear overview over dependencies that the firewall rules have to each other, making human errors less likely to occur. By combining policies and services into one, firewall policy management can be simplified and more easy to use. This results in fewer policy rules, making it easier to manage and less likely to cause a security breach.

All-Inclusive Security Management

For any network, security management is one of the more important aspects. It has to be intuitive, efficient and easy to use for large enterprises, with multiple firewalls at multiple sites, and even in geographical disperse areas, keeping your security management consistent and cohesive, and up to date is a non-trivial task. All these security management systems are included with our Clavister cOS Core products – free of charge.

Clavister InControl - Centralized Security Management

Clavister InControl offers a comprehensive centralized management solution that will assist and help administrators perform their daily tasks faster, easier and in a more streamlined way. Its intuitive user interface and support for task-driven workflow management guides administrators through complex and repetitive tasks, thereby alleviating the burden of managing large installations. With support for triple-AAA (Authentication, Authorization and Audit) the integrity and configurations managed by the Clavister InControl system is kept under strict control. This level of control makes it easy to use delegated manage-

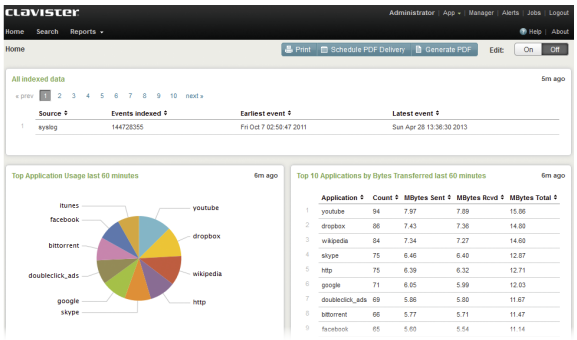
ment, allowing specific teams and personnel to access only designated parts of the system.

Clavister InControl can be extended to collaborate with a vast number of other management system with the use of Clavister InControl Software Development Kit (SDK). The Clavister InControl SDK enables organizations to integrate and extend existing system management tools with Clavister InControl management. For example, optimized provisioning systems, integrated help desk functionality.



Splunk for Clavister

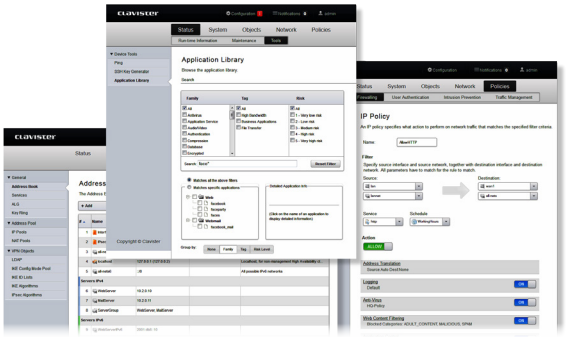
Splunk for Clavister is a comprehensive Web-based reporting system that offers enterprise-level reporting with tight integration with all Clavister cOS Core-based products. Splunk supports real-time data analysis, with Key Performance Indicators (KPI), graphs, tables and long-term trending, scaling from a single Clavister security gateway to large data centers.



Splunk for Clavister enables you to visualize your Clavister security solution, including pinpointing problem areas, thwarted attacks and other security issues, and then turn them into business-level reports. You can also take advantage of the built-in scheduling and distribution features to make sure the right people get the right reports on time.

Other Management Options

In addition to our centralized management solution, we also provide the Clavister Web Management system, an easy-to-use Web-based security management solution that works for smaller installations with just a few firewalls. Each product also supports our comprehensive command-line interface (CLI), enabling you to script common tasks.



CLAVISTER SECURITY GATEWAY SERIES HIGHLIGHTS

Next-Generation Firewall Security

By integrating world-class Next-Generation Firewall functionality, such as our Clavister True Application Control, Intrusion Detection and Prevention (IDP), Anti-Virus, Anti-Spam and Web Content Filtering with a stateful firewall with deep packet inspection, IPsec and SSL VPN connectivity, we are able to protect your organization against everything from network layer attacks to application layer threats, and even viruses and worms. While you have full control of who does what, when and with what.

Clavister cOS Core

Clavister cOS Core is our in-house developed, high-performance security network operating system. Every line of code is carefully crafted to ensure that it delivers maximum performance at all times. We take pride in delivering a product that we have full control over, rather than a mashup of open-source components.

Flexibility and Adaptability

Not all networks are created equally. Vast differences in network topology and configuration require a network security gateway to be able to accommodate all these differences. Our security gateways gives you the freedom to set routing policies with extreme granularity. A large number of parameters can be used to construct policies and rules to meet even the most demanding network installation.

Big on Performance - Low on Maintenance

All Clavister security gateways share a common trait: they all support Clavister Service Provisioning Network (CSPN). This secure, high-speed network ensures that all Clavister Security Subscription services are kept updated and current from newly emerging threats. This gives system administrators the freedom to concentrate on running their network without having to worry about having the latest security patches installed.

License Scalability

One important aspect of our products is scalability. Our licensing model offers you the ability to start with your performance needs today and upgrade your product incrementally as your organization grows. You also have the choice of two subscriptions models: the Clavister Security Subscription, our all-inclusive subscription, or the regular Clavister Product Subscription.

Low Total Cost of Ownership

Our goal is to provide a complete security solution that is more cost efficient than our competitors. Clavister security gateways, with their unique set of integrated security features, world-class service and support, and their powerful administration system, enables you to spend less time managing your security environment and keep your network defenses up to date, and thereby lower your network security infrastructure TCO significantly.

Performance* and Capacity	Clavister W20	Clavister W20 Pro
Firewall Performance (plaintext throughput)	4 Gbps	6 Gbps
IPsec VPN Performance (large packets)	1 Gbps	1,5 Gbps
Maximum Concurrent Connections	500,000	750,000
Maximum Concurrent IPsec VPN Tunnels	500	1,000
Maximum Concurrent L2TP/PPTP/SSL VPN Tunnels	500	1,000
Maximum Number of Users	Unrestricted	Unrestricted
Maximum Number of Routing Tables (Virtual Routers)	25	50

Connectivity	Clavister W20	Clavister W20 Pro
Ethernet Interfaces	6 x 1GbE (RJ45)	
Interfaces for Management / High Availability (HA)	Yes, any Ethernet interface can be configured for Management/High Availability (HA)	
Configurable Internal / External / DMZ Ports	Yes	Yes
Local Console Port	Virtual Console[1] - Micro USB	
Link Aggregation IEEE 802.1AX-2008 (Static/LACP)	Yes	Yes
Maximum Number of VLAN Interfaces IEEE 802.1Q	256	512
Support for High Availability (HA)**	Yes	Yes
Service-VLAN Interfaces IEEE 802.1ad (Q-in-Q)	Yes	Yes

[1] The Virtual Console Port requires a system driver to be installed on the workstation to get access to the device local console.

Product Specific Specification	
Form Factor / Rack Mountable	1U 19" rack mount / Yes
Dimensions (height x width x depth)	44 mm x 430 mm x 205 mm (17.3 in x 169.3 in x 80.7 in)
Hardware Weight / Package Weight	2 kg (4.41 lb) / 2.7 kg (5.95 lb)
Regulatory and Safety Standards	
Safety / EMC	CE, CB / FCC class A, CE class A
Power Specifications	
Power Supply (AC) / PSU Rated Power (W)	100-240 VAC, 50-60 Hz, 0.3 A / 12 W
Average Power Consumption / Redundant PSU	12 W/43 BTU / No
Appliance Input	100-240VAC
Environmental	
Cooling / Humidity	Single built-in fan module / 0% to 95% non-condensing
Operational Temperature	5° to 45° C (41° to 113° F)
Vibration (operating) / Shock (operating)	0.41 Grms2 (3-500 Hz) / 30 G
Warranty	All Clavister Wolf Series products include a two (2) years standard RMA warranty.

*** Performance based on Clavister cOS Core 11.00.**

**** When using High Availability clusters, the hardware settings for each interface must be identical on both cluster nodes (bus, slot and port)**

Where to Buy Clavister

For more information about where to buy Clavister products, visit www.clavister.com/partners. Additional resources and customer testimonials can be found at www.clavister.com/resources.

Product Features

Firewall	
Stateful Firewall / Deep Packet Inspection	Yes / Yes
IP Policies	ALLOW, DROP and REJECT
Multiple IP Rule Sets	Yes
User- and Group-Based Policies	Yes
Scheduled Policies	Yes
DoS and DDoS Detection and Prevention	Yes
Threshold Rules (Connection Count and Rate Limits)	Yes
IP Blacklisting / Whitelisting	Yes / Yes
TCP Sequence Number Tracking	Yes
FQDN Address Filter in IP Policies	Yes
IP Geolocation Filter in IP Policies	Yes
Ingress Filtering / IP Spoofing Protection	
Access Rules	Yes
Strict Reverse Path Forwarding (RPF)	Yes
Feasible RPF by using Interface Equivalence	Yes
Address and Port Translation	
Policy-Based	Yes
Dynamic NAT (Source)	Yes
Symmetric NAT	Yes
NAT Pools	Yes
Static Source Translation	Yes
Static Destination Translation (Virtual IP/Port Forward)	Yes
NAT Hairpinning	Yes
Server Load Balancing (SLB)	
SLB Distribution Methods	Round-Robin, Connection-Rate
SLB Monitoring Methods	ICMP Echo, Custom TCP Port, HTTP Request/Response
SLB Server Stickiness	State, IP Address, Network
Mode of Operations	
Transparent Mode (Layer 2)	Yes
Routing Mode (Layer 3)	Yes
Mixed Transparent and Routing Mode	Yes
Routing	
Static Routing	Yes
Policy-Based Routing (PBR)	Yes
Scheduled Policy-Based Routing	Yes
Virtual Routing	Yes
Multiple Routing Tables	Yes
Loopback Interfaces	Yes
Route Load Balancing (Equal-Cost Multipath)	Yes
Route Failover	Yes
Route Monitoring Methods	ARP, ICMP Echo, Custom TCP Port, HTTP Request/Response
Source-Based Routing	Yes
Path MTU Discovery	Yes
Dynamic Routing	
Policy-Based Dynamic Routes	Yes
OSPFv2 Routing Process (RFC2328)	Yes, multiple
OSPFv2 RFC1583 Compatibility Mode	Yes
OSPFv2 over VPN	Yes
Multicast	
Multicast Forwarding	Yes
IGMPv2 Compatibility Mode (RFC2236)	Yes
IGMPv3 (RFC3376)	Yes
IGMP Proxy Mode	Yes
IGMP Snoop Mode	Yes
Transparent Mode (L2 Bridge Mode)	
Policy-Based	Yes
MPLS Pass-through	Yes
DHCP Pass-through	Yes
Layer 2 Pass-through of Non-IP Protocols	Yes
Spanning Tree BPDU Relaying	Normal (STP), Rapid (RSTP), Multiple (MSTP), Per VLAN Spanning Tree Plus (PVST+)
IP Address Assignment	
Per Interface Address Assignment	Yes
Static	Yes

DHCP Client	Ethernet, VLAN, Link-Aggregation
PPPoE Client	Ethernet, VLAN, Link-Aggregation
PPTP/L2TP Client	Yes
Network Services	
DHCP Server	Yes, multiple
DHCP Server Custom Options	Yes
DHCP Relay	Yes, multiple
IP Pool	Yes
Proxy ARP	Yes
Dynamic DNS Services	DynDNS.org, Dyns.cx, CJB.net, Peanut Hull
Custom HTTP Poster	Yes
Bandwidth Management	
Policy-Based Bandwidth Management	Yes
Scheduled Policies	Yes
Bandwidth Guarantees / Limits / Prioritization	Yes / Yes / Yes
DSCP- / ToS-Based	Yes
Bandwidth Management per Group	Yes
Dynamic Bandwidth Balancing between Groups	Yes
Packet Rate Limits	Yes
DSCP Forwarding	Yes
DSCP Copy to Outer Header	VLAN, IPsec
Application Control	
Recognizable Applications	< 2,000
Recognition of SSL Based Applications	Yes
Application Content Control	2,400
Policy-Based	Yes
Policy Matching on Application	Yes
Policy Matching on Application Content (Metadata)	Yes
Policy Actions	Audit, DROP, Bandwidth Management
Intrusion Detection and Prevention	
Policy-Based	Yes
Signature Selection per Policy	Yes
Policy Actions	Audit, DROP, Bandwidth Management
Stateful Pattern Matching	Yes
Protocol and Rate Anomaly Detection	Yes
Insertion and Evasion Protection	Yes
Dynamic IP Blacklisting	Yes
Automatic Signature Updates	Yes
Content Security	
Policy-Based	Yes
Protocol Validation	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, TFTP, SIP, H.323, PPTP, TLS/SSL
Web Content Filtering	
HTTP / HTTPS	Yes / Yes
Audit / Blocking Mode	Yes / Yes
Classification Categories	32
URL Whitelisting / Blacklisting	Yes / Yes
Customizable Restriction Pages	Yes
Cloud-Based URL Classification Source	Yes
SafeSearch Enforcement	Google, Yahoo, Bing
User-Agent Filter	Yes
Anti-Virus	
Supported Protocols	HTTP, HTTPS, FTP, SMTP, POP3, IMAP
Stream-Based Scanning	Yes
File Type Whitelisting	Yes
Scanning of Files in Archives (ZIP/GZIP)	Yes
Nested Archives Support (ZIP/GZIP)	Yes, up to 10 levels
Automatic Updates	Yes
Anti-Spam	
Supported Protocols	SMTP, POP3, IMAP
Anti-Spam Detection Mechanisms	Yes
Reply Address Domain Verification	SMTP, POP3, IMAP
Malicious Link Protection	SMTP, POP3, IMAP
Distributed Checksum Clearinghouses (DCC)	SMTP, POP3, IMAP
DNS Blacklisting	SMTP, POP3, IMAP
Anti-Spam Actions	

Strip Malicious Links	SMTP, POP3, IMAP
Tag Subject and Headers	SMTP, POP3, IMAP
Send to Quarantine E-mail Address	SMTP
E-mail Rate Limiting	SMTP
File Integrity	
Supported Protocols	HTTP, HTTPS, FTP, SMTP, POP3, IMAP
File Type Whitelisting / Blacklisting	Yes / Yes
File Extension and MIME Type Verification	Yes
Application Layer Gateway	
HTTP / HTTPS (Content Security)	Yes
FTP (Content Security, NAT / SAT)	Yes
TFTP (NAT / SAT)	Yes
SIP (NAT / SAT)	Yes
H.323 / H.323 Gatekeeper (NAT / SAT)	Yes
SMTP (Content Security)	Yes
POP3 (Content Security)	Yes
IMAP (Content Security)	Yes, using Email Control Profile
SSL / TLS (Offloading)	Yes
PPTP (Passthrough, NAT / SAT)	Yes
IPsec VPN	
Internet Key Exchange	IKEv1, IKEv2
IKEv1 Phase 1	Main Mode, Aggressive Mode
IKEv1 Phase 2	Quick Mode
IPsec Modes	Tunnel, Transport (IKEv1 only)
IKE Encryption	AES, 3DES, DES, Blowfish, Twofish, Cast-128
IPsec Encryption	AES, 3DES, DES, Blowfish, Twofish, Cast-128, NULL
AES Key Size	128, 192, 256
IKE/IPsec Authentication	SHA-1, SHA-256, SHA-512, MD-5, AES-XCBC (IKEv2 only)
Perfect Forward Secrecy (DH Groups)	1, 2, 5, 14, 15, 16, 17, 18
IKE Config Mode	Yes
IKE DSCP Assignment	Static
Dead Peer Detection (DPD)	Yes
Pre-Shared Keys (PSK)	Yes
X.509 Certificates	Yes
XAuth (IKEv1)	Yes, Client and Server
EAP (IKEv2)	Yes, Server (RADIUS only)
PKI Certificate Requests	PKCS#1, PKCS#3, PKCS#7, PKCS#10
Self-Signed Certificates	Yes
Certificate Authority Issued Certificates	Yes, VeriSign, Entrust etc.
Certificate Revocation List (CRL) Protocols	LDAP, HTTP
CRL Fail-Mode Behavior	Conditional, Enforced
IKE Identity	IP, FQDN, E-mail, X.500 Distinguished-Name
Security Association Granularity	Net, Host, Port
Replay Attack Prevention	Yes
Policy-Based Routing	Yes
Virtual Routing	Yes
Roaming Client Tunnels	Yes
NAT Traversal (NAT-T)	Yes
IPsec Dial-on-Demand	Yes
IPsec Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Redundant VPN Tunnels	Yes
IPsec Passthrough	Yes
SSL VPN	
TLS/SSL VPN	Yes
One-Time Client Installation	Yes
Browser Independent	Yes
VPN Policy Selection Through	Firewall Rule Set, Routing and Policy-Based Routing
Split Tunneling	Yes
SSL VPN IP Provisioning	IP Pool, Static
L2TP VPN	
L2TPv2 Client (LAC)	Yes
L2TPv2 Server (LNS)	Yes
L2TPv3 Client (LAC)	Yes
L2TPv3 Server (LNS)	Yes
L2TP over IPsec	Yes

L2TP Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
L2TP Client Dial-on-Demand	Yes
L2TPv2 Server IP Provisioning	IP Pool, Static
Other Tunnels	
PPPoE Client (RFC2516)	Yes
Unnumbered PPPoE	Yes
PPPoE Client Dial-on-Demand	Yes
PPTP Client (PAC)	Yes
PPTP Client Dial-on-Demand	Yes
PPTP Server (PNS)	Yes
PPTP Server IP Provisioning	IP Pool, Static
MPPE Encryption (PPTP/L2TP)	RC4-40, RC4-56, RC4-128
Generic Router Encapsulation (RFC2784, RFC2890)	Yes
6in4 Tunneling (RFC4213)	Yes
Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
User Authentication	
Local User Database	Yes, multiple
RADIUS Authentication	Yes, multiple servers
RADIUS Accounting	Yes, multiple servers
LDAP Authentication	Yes, multiple servers
RADIUS Authentication Protocols	PAP, CHAP, MS-CHAPv1, MS-CHAPv2
XAUTH IKE/IPsec Authentication	Yes
Web-Based HTTP/HTTPS Authentication	Yes
Configurable HTTP/HTTPS Front-End	Yes
L2TP/PPTP/SSL VPN Authentication	Yes
Single Sign-On	
Device-Based Authentication (MAC Address)	Yes
ARP Authentication	Yes
RADIUS Relay	Yes
Active Directory Integration	Microsoft Windows Server 2003, 2008 R2, 2012
Client-less Deployment	Yes
Client Support	iOS, Android, Windows, OSX, Linux
Security Management	
Centralized Management	Clavister InControl[1]
Web User Interface (WebUI)	HTTP and HTTPS
SSH / SCP Management	Yes / Yes
Command Line Interface (CLI)	Yes
REST API	User Authentication
Management Authentication	Local User Database, RADIUS
Remote Fail-Safe Configuration	Yes
Local Console (RS-232)	Yes
Traffic Simulation (CLI)	ICMP, TCP, UDP
Scripting	CLI, WebUI
Packet Capture (PCAP)	Yes
System Upgrade	SSH / WebUI / Clavister InControl. From version 9.00.01 and later.
System and Configuration Backup	SSH / WebUI / Clavister InControl
SNTP Time Sync	Yes
Monitoring	
Syslog	Yes, multiple servers
Clavister Log	Yes, multiple servers
Real-Time Log	WebUI, Clavister InControl
Mail Alerting	Yes
Log Settings per Policy	Yes
Log Export via WebUI	Yes
SNMPv2c Polling / SNMPv2c Traps	Yes / Yes
SNMPv3	Yes
Real-Time Monitor Alerts (Log Action)	Yes
Real-Time Performance Monitoring	WebUI, Clavister InControl
Hardware Key Metrics Monitoring	CPU Load, CPU Temperature, Voltage, Memory, Fan, etc.
NOTE: Several third-party log monitoring plug-ins are available for Clavister firewalls. These monitoring plug-ins are either commercially available or via open source.	
IPv6	
IPv6 Ready Certification	Core Protocols, Phase-2 Router
Neighbor Discovery	Yes
Proxy Neighbor Discovery	Yes
IPv6 Path MTU Discovery	Yes

ICMPv6	Yes
IPv6 Router Advertisement	Yes
Interfaces	Yes
Ethernet Interfaces	Yes
VLAN Interfaces (802.1q)	Yes
Link Aggregation IEEE 802.1AX-2008 (Static/LACP)	Yes
Static IPv6 Address Assignment	Yes
IPv6 DHCP Client	Yes
IPv6 Router Solicitation	Yes
Stateless Address Autoconfiguration	Yes
Firewall	
IP Policies	ALLOW, DROP and REJECT
Stateful Firewall	Yes
Ingress Filtering	Yes
IPv6 Routing / Policy-Based Routing	Yes / Yes
Content Security	
Policy-Based	Yes
Protocol Validation	HTTP / HTTPS
Web Content Filtering	
HTTP / HTTPS	Yes
Audit / Blocking Mode	Yes / Yes
Classification Categories	32
URL Whitelisting / Blacklisting	Yes / Yes
Customizable Restriction Pages	Yes
SafeSearch Enforcement	Google, Yahoo, Bing
User-Agent Filter	Yes
Anti-Virus	
Supported Protocols	HTTP / HTTPS
Stream-Based Scanning	Yes
File-Type Whitelisting	Yes
Scanning of files in archives	Yes, up to 10 levels of nested archives
Functionality	
DHCPv6 Server	Yes
Application Control	Yes
High Availability	
Active Mode with Passive Backup	Yes
Firewall Connection State Synchronization	Yes
IKE / IPsec State Synchronization	Yes / Yes
User and Accounting State Synchronization	Yes
DHCP Server and Relayer State Synchronization	Yes
Synchronization of Dynamic Routes	Yes
IGMP State Synchronization	Yes
Server Load Balancing (SLB) State Synchronization	Yes
Configuration Synchronization	Yes
Device Failure Detection	Yes
Dead Link / Gateway / Interface Detection	Yes / Yes / Yes
Average Failover Time	< 800 ms

Specifications subject to change without further notice.

CID: 9150-0040-24 (2016/01)

[1] See Clavister InControl datasheet for compatible versions.

COMMON CRITERIA EAL 4+

ICSA labs CERTIFIED FIREWALL - CORPORATE

About Clavister

Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy

www.clavister.com/partners

Contact

www.clavister.com/contact

clavister®

CONNECT . PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden

• **Phone:** +46 (0)660 29 92 00 • **Fax:** +46 (0)660 122 50 • **Web:** www.clavister.com

Copyright © 2015-2016 Clavister AB. All rights reserved. The Clavister logo and all Clavister product names and slogans are trademarks or registered trademarks of Clavister AB. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Information in this document is subject to change without prior notification.