CLAVISTER®

NetWall

THE MOST ROBUST NEXT-GENERATION FIREWALLS
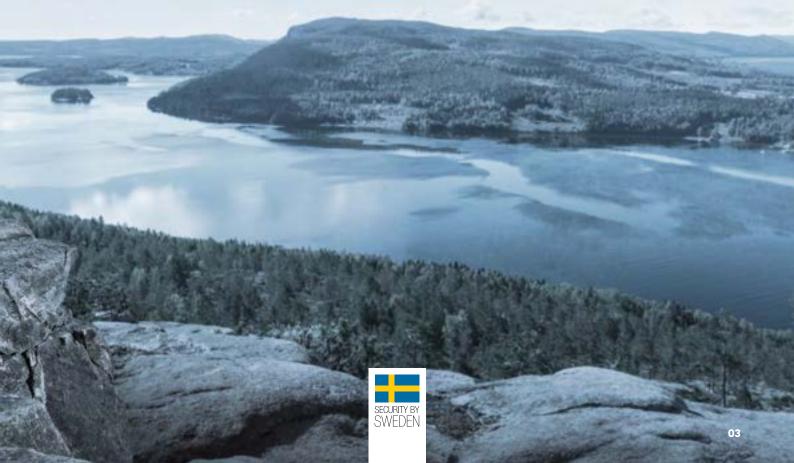
SECURITY BY SWEDEN

TABLE OF CONTENTS

The Most Robust Next-Generation Firewalls

Clavister NetWall is our family of AI-powered Next-Generation Firewalls – designed and developed in Sweden – ideal for cyberprotecting mission-critical infrastructure, including datacentres, remote sites and harsh industrial environments.

SECURITY BY
SWEDEN

SECURITY BY DESIGN

We believe we offer the most robust cybersecurity solutions ever built. We build on 25 years of security track record – the result of a proven secure development lifecycle. The result? Record-few vulnerabilities and unparalleled uptime.

THE SWISS ARMY KNIFE OF ROUTING

With incredibly flexible routing capabilities, Clavister NetWall is designed to support the most complex network setups.
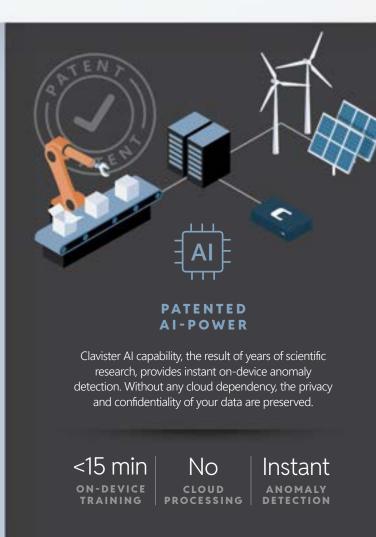
APPLICATION-BASED ROUTING

Efficient routing-decisions made by identification of applications. Allow your mission-critical applications to use the best routes available.

VIRTUAL & DYNAMIC ROUTING

Deploy multiple virtual routers with powerful policy flows. Dynamic routing protocols ensure interoperability with existing network equipment.

ALWAYS-UP PHILOSOPHY

Through a vast range of health monitors, balancing and fail-over methods, your traffic is guaranteed to reach its destination at all times.

PATENTED AI-POWER

Clavister AI capability, the result of years of scientific research, provides instant on-device anomaly detection. Without any cloud dependency, the privacy and confidentiality of your data are preserved.

<15 min	No	Instant
ON-DEVICE TRAINING	CLOUD PROCESSING	ANOMALY DETECTION

SIMPLE SECURE REMOTE WORKING

Clavister OneConnect is our VPN client that offers a simple and easy to use solution for remote access. Connecting securely is as easy as downloading and installing from common marketplaces or distributing using a device management software. Complement with the Clavister IAM solution to benefit from strong authentication and single sign-on capabilities.

SUPPORTED PLATFORMS

Windows
chromeOS
Android
macOS
iPadOS
iOS

HIGHLY RESILIENT

We appreciate the mission-criticality of your network. That is why Clavister NetWall is built to provide the highest level of resiliency. Through our state-of-the-art high availability capability, seamless switch-over to a secondary device happens within milliseconds, without any interruption of traffic. Extensive health checks, not only on the Clavister NetWall device itself but also on links, routes, gateways and even third-party hosts, cater for prompt resolution in case of degradation.
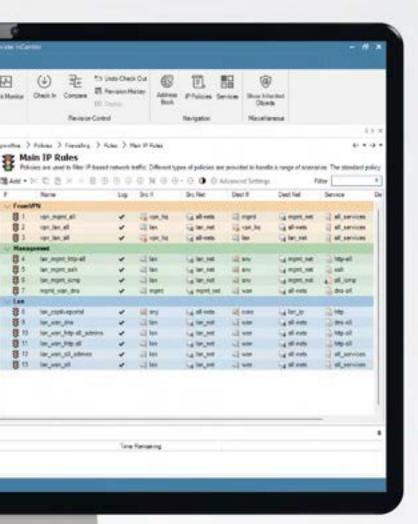
7+ Years

AVERAGE NUMBER OF YEARS OF UNINTERRUPTED PROTECTION

ACTIONABLE SECURITY ANALYTICS

All Clavister NetWall products come with powerful security analytics capabilities. A single pane of glass console provides clear, actionable, and comprehensive evaluation of your organisation's cybersecurity readiness. Through a blend of sophisticated algorithms and real-time insights, the system pinpoints vulnerabilities, prioritises risks, and offers tailored recommendations to keep your business secure.

CENTRAL MANAGEMENT AND CONTROL

The Clavister InControl centralised management console, included in all Clavister NetWall licensing plans, makes managing Clavister NetWall firewalls easy and efficient, even for large networks.

Its intuitive interface simplifies administration through features like zero-touch deployment, shared policy sets, and scheduled firmware updates to simplify day-to-day tasks.

With tools for firewall configuration, troubleshooting, firewall backups, and remote access, Clavister InControl is designed to save time and reduce complexity while keeping your network running smoothly.

Through a granular role and permission structure, Clavister InControl integrates well with your security policy framework.

Full	Zero Touch	Batch
REVISION CONTROL	DEPLOYMENT	FIRMWARE UPGRADES

TRAFFIC MANAGEMENT

The advanced traffic management capability in Clavister NetWall ensures optimised bandwidth usage, enabling smoother network performance even during peak loads. With granular control and intelligent traffic prioritisation, businesses can secure critical applications while maintaining consistent service quality across their infrastructure.

NetWall

DEEP APPLICATION AWARENESS

In-depth recognition, inspection and control of several thousands of applications allows for the most powerful and granular enforcement of application policies.

SELECTED APPLICATION-BASED CAPABILITIES

Inspection of, and policies for, granular application attributes.

Ensure consistent quality-of-service with effective bandwidth management.

Block or limit undesired or risky applications.

Extensive logging for analytics and auditing.

Apply routing decisions to achieve local internet break-out scenarios.

4,500+
IDENTIFIED APPLICATIONS AND PROTOCOLS

ALWAYS-UP VPN

Clavister NetWall delivers reliable and secure site-to-site VPN capabilities, designed to connect remote locations seamlessly. Built on industry-standard encryption protocols, it ensures excellent interoperability with other VPN solutions, providing secure data transmission across networks. With Clavister's robust IPsec implementation, businesses can count on high performance, ease of configuration, and strong protection for their critical communications. Whether connecting branch offices or integrating with partner networks, Clavister NetWall simplifies secure connectivity while maintaining top-tier security and reliability.

FLEXIBLE DEPLOYMENT OPTIONS

Clavister NetWall is available in a number of models ranging from small desktop versions to large datacenter appliances. Clavister NetWall is also available on virtualized versions for deployment in public and private cloud environments. Turn key appliances to fit all your needs.

ORACLE CLOUD

Azure

Google Cloud

aws

openstack

KVM

Microsoft Hyper-V

vmware vSphere

THREAT PREVENTION

Clavister NetWall employs a wide array of sophisticated threat prevention capabilities, all seamlessly integrated with each other, working in concert to provide the most efficient mitigation for a vast range of cyber-attacks.

BOTNET

To conduct large-scale cyberattacks, including Distributed Denial-of-Service (DDoS) attacks and massive spread of malware, hackers typically make use of a botnet – a network of compromised computers or devices. Clavister NetWall mitigates these types of attacks by detecting and blocking botnet Command and Control communication.

UNFRIENDLY STATES

Many cyberthreats originate from countries infamous for hosting threat actors or computing resources designated for attacks. Using the geo-fencing capabilities of Clavister NetWall will dramatically reduce the window of attack origin.

PHISHING

Rogue actors frequently attempts to deceive users into sharing sensitive information, such as passwords, credit card numbers or other personal data. This is typically done through fraudulent emails, text messages or fake websites. Clavister NetWall blocks senders of phishing attempts and prevents users from accessing illegitimate websites.

VULNERABILITIES AND EXPLOITS

Hackers commonly abuse poorly written software – both on an application and operating system level – to gain unauthorised access to systems, or to simply cause disruptions. Clavister NetWall detects and automatically blocks attempts to exploit known vulnerabilities.

DENIAL-OF-SERVICE (DoS)

A DoS cyberattack aims at disrupting the normal functioning of a network by overwhelming it with a flood of malicious traffic. The goal is to make the targeted resource unavailable, causing downtime, inconvenience, and/or financial loss. Clavister NetWall reduces the impact of DoS attacks using a combination of mitigation technologies.

VIRUSES AND OTHER MALWARE

Malware, such as viruses, worms, ransomware and trojans, pose a constant threat to all organisations and can be extremely costly to address once they have gained foothold and begun spreading within a network. Clavister NetWall restricts access to websites known for hosting malware, and can furthermore detect malware in transit to reduce the risk of infection.

ILLEGAL AND INAPPROPRIATE CONTENT

Accessing illegal or inappropriate content can be harmful not only from a cybersecurity stand-point but also as a potential violation of business policies. Clavister NetWall provides the safeguards to restrict what type of content users can access.

DIMENSIONS & POWER

Form Factor	Desktop / Wall Mounted
Dimensions (H x W x D)	34 x 131 x 180 mm (1.34 x 5.16 x 7.09 in)
Rack Mountable	Yes (Optional)
DIN-rail Mountable	Yes (Optional)
Maximum Power Consumption	9.2 Watt
Power Supply (AC)	100-240 VAC, 50-60 Hz
Power Supply (DC)	-
Redundant Power Supplies	-
Hot-swappable Power Supplies	-

INTERFACES & MODULES

Ethernet Interfaces	4 x 1 GbE RJ45
Power-over-Ethernet Interfaces	-
Ethernet Bypass Interfaces	-
Console Port	1 x COM RJ45
Number of Expansion Slots	-

OPERATING ENVIRONMENT & CERTIFICATIONS

Safety	CE, UL
EMC	FCC, CE, VCCI
Operating & Storage Humidity	0 % to 95 % (Non-condensing)
Operating Temperature	5°C to 35°C (41°F to 95°F)

SYSTEM PERFORMANCE & CAPACITY

	NETWALL 110	NETWALL 140
Firewall Throughput[1] (1518 / 512 / 64 byte, UDP)	1 / 1 / 0.38 Gbps	4 / 3 / 0.38 Gbps
Firewall Throughput[1] (Packets per Second)	742 Kpps	742 Kpps
Concurrent Connections	128,000	256,000
New Connections/Second (TCP)	42,000	42,000
IPsec VPN Throughput[2] (1420 / 512 / 64 byte, UDP)	100 / 100 / 73 Mbps	250 / 250 / 73 Mbps
IPsec VPN Throughput[2] (Software Only) (1420 / 512 / 64 byte, UDP)	-	-
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	50	100
OneConnect VPN Throughput (TCP)	100 Mbps	250 Mbps
OneConnect VPN Tunnels	50	100
VLANs	128	128
Virtual Routers	10	20

OPTIONAL RACK MOUNT KIT

RACK-100S

OPTIONAL DIN MOUNT KIT

DIN-100S

[1] Firewall Throughput tested according to RFC2544   [2] IPsec VPN performance test uses AES-CGM-128 ICV16

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document is subject to change without prior notification.

09

300

DIMENSIONS & POWER

Form Factor	Desktop
Dimensions (H x W x D)	44 x 270 x 160 mm (1.73 x 10.62 x 6.29 in)
Rack Mountable	Yes (Included)
DIN-rail Mountable	-
Maximum Power Consumption	19.5 Watt
Power Supply (AC)	100-240 VAC, 50-60 Hz
Power Supply (DC)	-
Redundant Power Supplies	-
Hot-swappable Power Supplies	-

INTERFACES & MODULES

Ethernet Interfaces	6 x 1 GbE RJ45, 2 x 1 GbE SFP
Power-over-Ethernet Interfaces	-
Ethernet Bypass Interfaces	-
Console Port	1 x COM RJ45
Number of Expansion Slots	-

OPERATING ENVIRONMENT & CERTIFICATIONS

Safety	CE, UL
EMC	FCC, CE, VCCI
Operating & Storage Humidity	0 % to 95 % (Non-condensing)
Operating Temperature	5°C to 35°C (41°F to 95°F)

SYSTEM PERFORMANCE & CAPACITY	NETWALL 310	NETWALL 340
Firewall Throughput[1] (1518 / 512 / 64 byte, UDP)	4 / 3.6 / 0.47 Gbps	8 / 3.6 / 0.47 Gbps
Firewall Throughput[1] (Packets per Second)	923 Kpps	923 Kpps
Concurrent Connections	500,000	1,000,000
New Connections/Second (TCP)	82,000	82,000
IPsec VPN Throughput[2] (1420 / 512 / 64 byte, UDP)	1 / 1 / 0.2 Gbps	2 / 1.4 / 0.2 Gbps
IPsec VPN Throughput[2] (Software Only) (1420 / 512 / 64 byte, UDP)	-	-
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	500	1,000
OneConnect VPN Throughput (TCP)	250 Mbps	500 Mbps
OneConnect VPN Tunnels	500	1,000
VLANs	256	512
Virtual Routers	20	50

[1] Firewall Throughput tested according to RFC2544   [2] IPsec VPN performance test uses AES-CGM-128 ICV16

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document is subject to change without prior notification.

10

DIMENSIONS & POWER

Form Factor	Rack Mounted / Desktop
Dimensions *(H x W x D)*	44 x 251 x 250 mm (1.73 x 9.88 x 9.84 in)
Rack Mountable	Yes (Simple Kit Included)
DIN-rail Mountable	-
Maximum Power Consumption	20.7 Watt
Power Supply *(AC)*	100-240 VAC, 50-60 Hz
Power Supply *(DC)*	-
Redundant Power Supplies	Yes (Optional)
Hot-swappable Power Supplies	Yes

INTERFACES & MODULES

Ethernet Interfaces	6 x 1 GbE RJ45, 2 x 10 GbE SPF+
Power-over-Ethernet Interfaces	Yes *(Enable PoE+ on two onboard RJ45 ports using optional PSU)*
Ethernet Bypass Interfaces	-
Console Port	1 x COM RJ45
Number of Expansion Slots	-

OPERATING ENVIRONMENT & CERTIFICATIONS

Safety	CE, UL
EMC	FCC, CE, VCCI
Operating & Storage Humidity	0 % to 95 % (Non-condensing)
Operating Temperature	5°C to 35° C (41°F to 95°F)

SYSTEM PERFORMANCE & CAPACITY

	NETWALL 510	NETWALL 550
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	10 / 5.7 / 0.72 Gbps	15 / 5.7 / 0.72 Gbps
Firewall Throughput[1] *(Packets per Second)*	1.3 Mpps	1.3 Mpps
Concurrent Connections	1,000,000	2,000,000
New Connections/Second *(TCP)*	92,000	92,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	3 / 1.8 / 0.3 Gbps	5 / 1.8 / 0.3 Gbps
IPsec VPN Throughput[2] *(Software Only) (1420 / 512 / 64 byte, UDP)*	-	-
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	1,000	2,000
OneConnect VPN Throughput *(TCP)*	500 Mbps	700 Mbps
OneConnect VPN Tunnels	1,000	2,000
VLANs	512	1,024
Virtual Routers	50	100

OPTIONAL PREMIUM RACK MOUNT KIT

Upgrade your NetWall 500 Series with this premium rack mount kit, that includes mounting for PSUs.

RACK-500S

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

11

Clavister

NetWall

6000

DIMENSIONS & POWER

Form Factor	Rack Mounted
Dimensions *(H x W x D)*	44 x 438 x 508 mm (1.73 x 17.24 x 20.00 in)
Rack Mountable	Yes (Included)
DIN-rail Mountable	-
Maximum Power Consumption	140.3 Watt
Power Supply *(AC)*	100-240 VAC, 50-60 Hz
Power Supply *(DC)*	48 VDC (Optional)
Redundant Power Supplies	Yes (Optional)
Hot-swappable Power Supplies	Yes

INTERFACES & MODULES

Ethernet Interfaces	8 x 1 GbE RJ45, 2 x 10 GbE SFP+
Power-over-Ethernet Interfaces	Yes *(Using optional Expansion Module)*
Ethernet Bypass Interfaces	-
Console Port	1 x COM RJ45
Number of Expansion Slots	Two (2)

OPERATING ENVIRONMENT & CERTIFICATIONS

Safety	CE, UL, TUV
EMC	FCC, CE, VCCI
Operating & Storage Humidity	0 % to 95 % (Non-condensing)
Operating Temperature	0°C to 40°C (32°F to 104°F)

SYSTEM PERFORMANCE & CAPACITY

	NETWALL 6200	NETWALL 6600
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	20 / 20 / 2.58 Gbps	50 / 20 / 2.58 Gbps
Firewall Throughput[1] *(Packets per Second)*	4.7 Mpps	4.7 Mpps
Concurrent Connections	5,000,000	8,000,000
New Connections/Second *(TCP)*	300,000	300,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	5 / 5 / 0.78 Gbps	15 / 6 / 0.78 Gbps
IPsec VPN Throughput[2] *(Software Only) (1420 / 512 / 64 byte, UDP)*	1.12 / 0.82 / 0.20 Gbps	1.12 / 0.82 / 0.20 Gbps
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	2,500	5,000
OneConnect VPN Throughput *(TCP)*	2 Gbps	3.5 Gbps
OneConnect VPN Tunnels	2,500	5,000
VLANs	4,096	4,096
Virtual Routers	250	500

EXPANSION MODULES

8 x 1 GbE RJ45 Copper	8 x 1 GbE RJ45 SFP	PoE, 8 x 1 GbE RJ45 Copper	4 x 10 GbE SFP+	IPsec Accelerator & 4 x 10 GbE SFP+	2 x 25 GbE SFP28	2 x 40 GbE QSFP
	No Transceivers Incl	*Incl External 48V PoE PSU*	*No Transceivers Incl.*	*No Transceivers Incl.*	*No Transceivers Incl*	*No Transceivers Incl.*
CM-NET84	CM-NET85	CM-POE86	CM-NET143	CM-SEC144	CM-NET220	CM-NET420

[1] Firewall Throughput tested according to RFC2544   [2] IPsec VPN performance test uses AES-CGM-128 ICV16

DIMENSIONS & POWER

Form Factor	DIN-rail Mounted
Dimensions (H x W x D)	150 x 66 x 127 mm (5.9 x 2.6 x 5 in)
Rack Mountable	-
DIN-rail Mountable	Yes (Included)
Maximum Power Consumption	20 Watt
Power Supply (AC)	-
Power Supply (DC)	9 to 36V DC (Typical 12/24V)
Redundant Power Supplies	Yes (Optional)
Hot-swappable Power Supplies	Yes

INTERFACES & MODULES

Ethernet Interfaces	4 x 2,5 GbE RJ45, 2 x 1 GbE SFP
Power-over-Ethernet Interfaces	-
Ethernet Bypass Interfaces	2 x 2,5 GbE RJ45
Console Port	1 x COM RJ45
Number of Expansion Slots	-

OPERATING ENVIRONMENT & CERTIFICATIONS

Safety	CE, FCC
EMC	FCC, CE
Operating & Storage Humidity	10 % to 95 %
Operating Temperature	-40°C to 70°C (-40°F to +158°F)

SYSTEM PERFORMANCE & CAPACITY

Firewall Throughput[1] (1518 / 512 / 64 byte, UDP)	10 / 7 / 1.1 Gbps
Firewall Throughput[1] (Packets per Second)	1.6 Mpps
Concurrent Connections	256,000
New Connections/Second (TCP)	85,000
IPsec VPN Throughput[2] (1420 / 512 / 64 byte, UDP)	0.25 / 0.25 / 0.2 Gbps
IPsec VPN Throughput[2] (Software Only) (1420 / 512 / 64 byte, UDP)	-
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	100
OneConnect VPN Throughput (TCP)	250 Mbps
OneConnect VPN Tunnels	100
VLANs	256
Virtual Routers	20

[1] Firewall Throughput tested according to RFC2544   [2] IPsec VPN performance test uses AES-CGM-128 ICV16

Virtual

INTERFACES & MODULES	
Ethernet interfaces	Up to 10

SYSTEM PERF. & CAPACITY	100V	500V	1000V	2000V	4000V	6000V	12000V
Firewall Throughput[1]	100 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps	6 Gbps	12 Gbps
Concurrent Connections	16,000	64,000	128,000	256,000	512,000	1,000,000	1,000,000
IPsec VPN Throughput *(1420 / 512 / 64 byte, UDP)*	100 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps	6 Gbps	12 Gbps
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	50	250	500	500	1,000	1,500	1,500
OneConnect VPN Tunnels	50	250	500	500	1,000	1,500	1,500
VLANs	1024	1024	1024	1024	1024	1024	1024
Virtual Routers	25	25	50	50	100	100	125

VIRTUALIZATION SPECIFICATIONS							
Supported Hypervisors	VMware vSphere, KVM (ARM & Intel), Microsoft Hyper-V						
Intel AES-NI Crypto Acceleration	Yes						
Intel DPDK and SR-IOV Support	Yes						
Recommended Available Storage	1 GB						
Minimum Recommended RAM	512 MB	512 MB	512 MB	1 GB	2 GB	4 GB	4 GB

NO. OF VCPU SUPPORTED	32-BIT IMG (x86)	64-BIT IMG (x86_64)	64-BIT IMG (ARMv8)	COMMENT
1 vCPU	●	●	●	*32-bit image:* The image will run in interrupt mode *64-bit image:* The image can run in either interrupt mode or polling mode
2 vCPU		●	●	The image will run in polling mode
3 vCPU		●		The image will run in polling mode and use one vCPU for interface offloading
4 vCPU		●	●	The image will run in polling mode and use one vCPU for AI Processing

[1] Actual performance depends on host/server-hardware, hypervisor and similar

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

14

Support Offering

Our multi-tiered model, Standard and Priority Support, provides tailored service levels to meet your needs. From technical assistance to 24/7 emergency support, we ensure reliable solutions for your business.

STANDARD SUPPORT

Included, without extra cost, for all customers with an active Licensing Plan.

Technical Support
via helpdesk at my.clavister.com

Technical Documentation
including Knowledge Base

Standard Availability
08:00-17:00 CET
(Swedish office hours)

English and Swedish
as supported languages

PRIORITY SUPPORT

Available for customers with an active subscription and a Priority Support Agreement.

STANDARD SUPPORT

+

Emergency Availability 24/7/365
When production network is down or is severely degraded in performance, functionality or management

Callback Option
Callback request via support ticket

SupportOps
10 h/year included

SUPPORT OPS

SupportOps is a personalised complement to Standard Support, designed to address specific needs efficiently. Whether you need help with configuration, design advice, or resolving an issue, our experts provide hands-on assistance. Sessions are scheduled promptly and are available to all partners and customers, regardless of support tier, at an hourly rate.

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document is subject to change without prior notification.

15

Licensing Plans

We offer flexible licensing plans, designed to meet diverse business needs. Each plan unlocks powerful features and tools, ensuring your Clavister NetWall product is optimised for performance, protection, and scalability.

	★ ESSENTIALS	★★ ENHANCED	★★★ PREMIUM
Support and Maintenance			
Standard Support	•	•	•
Software Maintenance	•	•	•
Hardware Replacement	•	•	•
Networking Capabilities			
Routing	•	•	•
Always-Up VPN	•	•	•
Traffic Management	•	•	•
Simple Secure Remote Networking	•	•	•
High Availability	•	•	•
Reverse Proxy		•	•
Management and Analytics			
Centralised Management	•	•	•
Security Analytics	•	•	•
Threat Prevention			
Firewalling	•	•	•
Deep Application Awareness	•	•	•
Geo-fencing	•	•	•
Intrusion Prevention		•	•
Anti Malware		•	•
Web Content Filtering		•	•
IP Reputation		•	•
SSL Inspection			
SSL Inspection with Clavister NetEye			•
Cloud Sandboxing			•

Technical Specifications

FIREWALL

Stateful Firewall / Deep Packet Inspection	Yes / Yes
IP Policies	ALLOW, DROP and REJECT
Security Zones	Yes
Multiple IP Rule-sets	Yes
User- and Group-based Filter in Policies	Yes
Time- and Date-based Scheduled Policies	Yes
DoS and DDoS Detection and Prevention	Yes
Threshold Rules (Connection Count and Rate Limits) for IPv4	Yes
IP Blacklisting / Whitelisting for IPv4	Yes / Yes
TCP Sequence Number Tracking	Yes
FQDN- and Wildcard FQDN Address Filter in IP Policies	Yes
IP Geolocation Filter in IP Policies	Yes
DOS Protection based on IP Geolocation Filter for IPv4	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 for IPv4	
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
Reverse Proxy for IPv4	
Protocol	HTTP, HTTPS
IP Blacklisting	Yes

SERVER LOAD BALANCING (SLB) FOR IPv4

SLB Distribution Methods	Round-Robin, Connection-Rate, Strict, Server Resource-Usage over REST API
SLB Monitoring Methods	ICMP Echo, Custom TCP Port, HTTP Request/Response
SLB Server Stickiness	State, IP Address, Network
SLB Maintenance Mode	Yes
SLB Server Fallback	Yes

CONNECTIVITY

Ethernet Interfaces	1GbE, 2.5GbE, 10GbE, 25GbE, 40GbE
Link Aggregation IEEE 802.1AX-2008 (Static / LACP)	Yes
VLAN Interfaces IEEE 802.1Q	Yes
Service-VLAN Interfaces IEEE 802.1ad (Q-in-Q)	Yes

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

17

MODES 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

Application-based Routing

Routing based on application	Yes

Multicast for IPv4

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+)

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

18

INTERFACE IP ADDRESS ASSIGNMENT

Static IPv4 Address Assignment	Yes
Static IPv6 Address Assignment	Yes
DHCPv4 Client	Ethernet, VLAN, Link-Aggregation
DHCPv6 Client	Ethernet, VLAN, Link-Aggregation
IPv6 Prefix Delegation	Ethernet, VLAN, Link-Aggregation
PPPoE IPv4 Client	Ethernet, VLAN, Link-Aggregation
PPPoE IPv6 Client	Ethernet, VLAN, Link-Aggregation
Stateless IPv6 Address Auto-configuration	Yes
IPv6 Router Solicitation	Yes
PPTP / L2TP IPv4 Client	Yes

SPECIFIC IPv6 PROTOCOL FEATURES

IPv6 Ready Certification	Core Protocols, Phase-2 Router
Neighbor Discovery	Yes
Proxy Neighbor Discovery	Yes
IPv6 Router Advertisement	Yes

NETWORK SERVICES

DHCPv4 Server	Yes, Multiple
DHCPv4 Server Custom Options	Yes
DHCPv4 Relay	Yes, Multiple
DHCPv6 Server	Yes, Multiple
IP Pool	Yes
Proxy ARP	Yes
Dynamic DNS Services for IPv4	Dyn.com, Dyns.cx, DuckDNS.org
Custom HTTP Poster for IPv4	Yes

BANDWIDTH MANAGEMENT FOR IPv4

Policy-Based Bandwidth Management	Yes
Scheduled Policies	Yes
Bandwidth Guarantees	Yes
Bandwidth Limits	Yes
Bandwidth Prioritization	Yes
DSCP-based / 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	4,500+
Application Content Control	5,700+
Policy-Based	Yes
Policy Matching on Application	Yes
Policy Matching on Application Content (Metadata)	Yes
Policy Actions	Audit, DROP, Bandwidth Management

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

19

INTRUSION DETECTION AND PREVENTION (IDS / IPS)

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 for IPv4	Yes
Automatic Signature Updates	Yes

IP REPUTATION FOR IPv4

Real-Time DoS Protection	Yes
Real-Time Botnet Protection	Yes
Real-Time Phishing Protection	Yes
Real-Time Scanner Protection	Yes
Real-Time SPAM Protection	Yes
Real-Time IP Reputation Scores	Yes

CONTENT SECURITY

Policy-Based	Yes
IPv4 Protocol Validation	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, TFTP, SIP, H.323, PPTP, TLS/SSL, DNS, Syslog
IPv6 Protocol Validation	HTTP, HTTPS

Web Content Filtering

HTTP / HTTPS	Yes / Yes
Audit / Blocking Mode	Yes / Yes
Classification Categories	86
URL Whitelisting / Blacklisting	Yes / Yes
Customizable Restriction Pages	Yes
Cloud-Based URL Classification Source	Yes
User-Agent Filter	Yes

Anti-Virus

Supported Protocols	HTTP, 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 Signature Updates	Yes

Anti-Spam

Supported Protocols	SMTP, POP3, IMAP

Anti-Spam Detection Mechanisms

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

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

20

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
Reject Email Reception	SMTP

File Integrity

Supported Protocols	HTTP, FTP, SMTP, POP3, IMAP
File Type Whitelisting / Blacklisting	Yes / Yes
File Extension and MIME Type Verification	Yes

Update Center

Scheduled Signature Updates	Hourly / Daily / Weekly / Monthly
Manual Signature Updates	Yes
HTTP / HTTPS Proxy Support	Yes

APPLICATION LAYER GATEWAY

HTTP / HTTPS (Content Security)	Yes
FTP (Content Security, NAT / SAT)	Yes
TFTP (NAT / SAT)	Yes
SIP (NAT / SAT)	Yes
Syslog	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
DNS	Yes

VPN TUNNELS

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-GCM, AES, 3DES, DES, Blowfish, Twofish, Cast-128
IPsec Encryption	AES-GCM, 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, 19, 20, 21, 28, 29, 30, 31
IKE Config Mode	Yes, Static Pool and RADIUS Assigned IP
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)	Client (EAP-MSCHAPv2, EAP-MD5) Server (EAP-MSCHAPv2, EAP-MD5, RADIUS)
PKI Certificate Requests	PKCS#1, PKCS#3, PKCS#7, PKCS#10
Self-Signed Certificates	Yes

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

21

Certificate Authority Issued Certificates	Yes, VeriSign, Entrust etc.
Certificate Revocation List (CRL) Protocols	LDAP, HTTP
CRL Fail-Mode Behaviour	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
MOBIKE	Yes
IPsec Dial-on-Demand	Yes
IPsec Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Redundant VPN Tunnels	Yes
IPsec Passthrough	Yes
Tunneling of IPv4 in IPv4 IPsec Tunnel	Yes
Tunneling of IPv4 in IPv6 IPsec Tunnel	Yes
Tunneling of IPv6 in IPv4 IPsec Tunnel	Yes
Tunneling of IPv6 in IPv6 IPsec Tunnel	Yes

OneConnect SSL VPN

TLS (TCP) Support	Yes
DTLS (UDP) Support	Yes
One-Time Client Installation	Yes
Multi-factor Authentication (MFA/2FA) Support	OpenID Connect (OIDC), RADIUS
Browser Independent	Yes
VPN Policy Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Split Tunneling	Yes
SSL VPN Client IPv4 Provisioning	IP Pool, Static
Client OS Support	Windows, macOS, iPadOS, iOS, Android

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 IPv4 Provisioning	IP Pool, Static

Other Tunnels

PPPoE IPv4 Client	Yes
PPPoE IPv6 Client	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 Routing Encapsulation, GRE (RFC2784, RFC2890)	Yes
6in4 Tunneling (RFC4213)	Yes
Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing

Last modified: March 17, 2025
Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

22

USER AUTHENTICATION

Local User Database	Yes, Multiple
OpenID Connect (OIDC) Authentication	Yes, Multiple Servers, for OneConnect
RADIUS Authentication	Yes, IPv4 / IPv6, Multiple Servers
RADIUS Accounting	Yes, IPv4 / IPv6, Multiple Servers
LDAP Authentication	Yes, Multiple Servers
RADIUS Authentication Protocols	PAP, CHAP, MS-CHAPv1, MS-CHAPv2
XAUTH IKEv1 / IPsec Authentication	Yes
EAP IKEv2 / IPsec Authentication	Yes
Web-Based HTTP / HTTPS Authentication	Yes
Customizable HTTP / HTTPS Portal	Yes
L2TP / PPTP / OneConnect / SSL VPN Authentication	Yes

Identity Awareness

Device-Based Authentication (MAC Address)	Yes
ARP Authentication	Yes
RADIUS Relay	Yes
Active Directory Integration	Microsoft Windows Server
Client-less Deployment	Yes

MANAGEMENT

Centralized Management	Clavister InControl
Web User Interface (WebUI)	HTTP and HTTPS
SSH Management	Yes
Command Line Interface (CLI)	Yes
REST API	User Authentication, SLB, Blacklist Control
Management Authentication	Local User Database, RADIUS
Management Brute Force Protection	Yes
Remote Fail-Safe Configuration	Yes
Local Console (RS-232)	Yes
Traffic Simulation (CLI)	ICMP, TCP, UDP
Scripting Support	CLI, WebUI
Packet Capture (PCAP)	Yes
Packet Capture (PCAP)	WebUI, InControl, SCP
System and Configuration Backup	WebUI, InControl, SCP
SNTP Time Sync	Yes

MONITORING AND LOGGING

Syslog	Yes, Multiple Servers
Clavister InControl Log	Yes, Multiple Servers
Real-Time Log	CLI, WebUI, InControl
Memory Log	CLI, WebUI
Mail Alerting	Yes, SMTP
Log Settings per Policy	Yes
Log Export via WebUI	Yes
SNMPv2c Polling / Traps	Yes / Yes
SNMPv3 Polling / Traps	Yes / Yes
Real-Time Monitor Alerts (Log action)	Yes
Real-Time Performance Monitoring	WebUI, InControl
Hardware Key Metrics Monitoring	CPU Load, CPU Temperature, Voltage, Memory, Fan etc

Last modified: March 17, 2025

Copyright © 2025 Clavister. All rights reserved.

SECURITY BY SWEDEN

Information in this document
is subject to change without prior notification.

23

HIGH AVAILABILITY

Active Node 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
DHCP Client	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

HYPERVISOR SUPPORT

VMware	Yes
KVM	Yes
Hyper-V	Yes

EASY DEPLOYMENT

Clavister Zero Touch	Yes
Cloud Init	Yes, Network Based

ACME (AUTOMATIC CERTIFICATE MANAGEMENT ENVIRONMENT)

Let´s Encrypt	Yes
Buypass	Yes
Custom Server	Yes

Hardware Appliance Line-up

100 300 500 6000 200R

SYSTEM					
Form Factor	Desktop / Wall Mounted	Desktop	Rack Mounted / Desktop	Rack Mounted	DIN-rail Mounted
Dimensions *(H x W x D)*	34 x 131 x 180 mm (1.34 x 5.16 x 7.09 in)	44 x 270 x 160 mm (1.73 x 10.62 x 6.29 in)	44 x 251 x 250 mm (173 x 9.88 x 9.84 in)	44 x 438 x 508 mm (1.73 x 17.24 x 20.00 in)	150 x 66 x 127 mm (5.9 x 2.6 x 5 in)
Rack Mountable	Yes (Optional)	Yes (Included)	Yes (Simple Kit Included)	Yes (Included)	-
DIN-rail Mountable	Yes (Optional)	-	-	-	Yes (Included)
Maximum Power Consumption	9.2 Watt	19.5 Watt	20.7 Watt	140.3 Watt	20 Watt
Power Supply *(AC)*	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz	-
Power Supply *(DC)*	-	-	-	48 VDC (Optional)	9 to 36V DC (Typical 12/24V)
Redundant Power Supplies	-	-	Yes (Optional)	Yes (Optional)	Yes (Optional)
Hot-swappable Power Supplies	-	-	Yes	Yes	Yes

INTERFACES & MODULES					
Ethernet Interfaces	4 x 1 GbE RJ45	6 x 1 GbE RJ45, 2 x 1 GbE SFP	6 x 1 GbE RJ45, 2 x 10 GbE SPF+	8 x 1 GbE RJ45, 2 x 10 GbE SFP+	4 x 2,5 GbE RJ45, 2 x 1 GbE SFP
Power-over-Ethernet Interfaces	-	-	Yes *(Enable PoE+ on two onboard RJ45 ports using optional PSU)*	Yes *(Using optional Expansion Module)*	-
Ethernet Bypass Interfaces	-	-	-	-	2 x 2,5 GbE RJ45
Console Port	1 x COM RJ45	1 x COM RJ45	1 x COM RJ45	1 x COM RJ45	1 x COM RJ45
Number of Expansion Slots	-	-	-	Two (2)	-

OPERATING ENVIRONMENT & CERTIFICATIONS					
Safety	CE, UL	CE, UL	CE, UL	CE, UL, TUV	CE, FCC
EMC	FCC, CE, VCCI	FCC, CE, VCCI	FCC, CE, VCCI	FCC, CE, VCCI	FCC, CE
Operating & Storage Humidity	0 % to 95 % (Non-condensing)	0 % to 95 % (Non-condensing)	0 % to 95 % (Non-condensing)	0 % to 95 % (Non-condensing)	10 % to 95 %
Operating Temperature	5°C to 35°C (41°F to 95°F)	5°C to 35°C (41°F to 95°F)	5°C to 35° C (41°F to 95°F)	0°C to 40°C (32°F to 104°F)	-40°C to 70°C (-40°F to +158°F)

SYSTEM PERFORMANCE & CAPACITY	NETWALL 110	NETWALL 140	NETWALL 310	NETWALL 340	NETWALL 510	NETWALL 550	NETWALL 6200	NETWALL 6600	NETWALL 200R
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	1 / 1 / 0.38 Gbps	4 / 3 / 0.38 Gbps	4 / 3.6 / 0.47 Gbps	8 / 3.6 / 0.47 Gbps	10 / 5.7 / 0.72 Gbps	15 / 5.7 / 0.72 Gbps	20 / 20 / 2.58 Gbps	50 / 20 / 2.58 Gbps	10 / 7 / 1.1 Gbps
Firewall Throughput[1] *(Packet per Second)*	742 Kpps	742 Kpps	923 Kpps	923 Kpps	1.3 Mpps	1.3 Mpps	4.7 Mpps	4.7 Mpps	1.6 Mpps
Concurrent Connections	128,000	256,000	500,000	1,000,000	1,000,000	2,000,000	5,000,000	8,000,000	256,000
New Connections/Second *(TCP)*	42,000	42,000	82,000	82,000	92,000	92,000	300,000	300,000	85,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	100 / 100 / 73 Mbps	250 / 250 / 73 Mbps	1 / 1 / 0.2 Gbps	2 / 1.4 / 0.2 Gbps	3 / 1.8 / 0.3 Gbps	5 / 1.8 / 0.3 Gbps	5 / 5 / 0.78 Gbps	15 / 6 / 0.78 Gbps	0.25 / 0.25 / 0.2 Gbps
IPsec VPN Throughput[2] *(Software Only) (1420 / 512 / 64 byte, UDP)*	-	-	-	-	-	-	1.12 / 0.82 / 0.20 Gbps	1.12 / 0.82 / 0.20 Gbps	-
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	50	100	500	1,000	1,000	2,000	2,500	5,000	100
OneConnect VPN Throughput *(TCP)*	100 Mbps	250 Mbps	250 Mbps	500 Mbps	500 Mbps	700 Mbps	2 Gbps	3.5 Gbps	250 Mbps
OneConnect VPN Tunnels	50	100	500	512	1,000	2,000	2,500	5,000	100
VLANs	128	128	256	512	512	1,024	4,096	4,096	256
Virtual Routers	10	20	20	50	50	100	250	500	20

[1] Firewall Throughput tested according to RFC2544   [2] IPsec VPN performance test uses AES-GGM-128 ICV16

On a Mission to Cyber-Protect Europe

Clavister provides top-tier cybersecurity solutions made in Sweden.
For over 25 years, we are the trusted partner for customers with
mission-critical applications.

YOUR TRUSTED PARTNER

In today's rapidly evolving cyberthreat environment, everyone needs all the help they can get – but who do you trust? With over 20,000 satisfied customers and 25 years of innovation, Clavister has proven itself as the reliable choice, trusted by major brands and recognised for our strong partnerships.

SWEDISH ENGINEERING AT HEART

Clavister's solutions are rooted in the strong tradition of Swedish engineering, known for reliability, quality, and cutting-edge innovation. We believe we offer the most robust cybersecurity solutions, built on long-standing security expertise, resulting in record-low vulnerabilities and unparalleled uptime. Our commitment to innovation keeps us at the forefront of the industry.

A CARING RELATIONSHIP

At Clavister, cybersecurity is a team game. That's why we focus on building long-term relationships where you engage directly with our domain experts. Our presence in Europe includes a dedicated team and a strong reseller network, ready to support you.
We've got you covered!

TRUSTED BY MAJOR BRANDS

MUSTANG®   NOKIA   BAE SYSTEMS

SAAB   ERICSSON

Clavister

CLAVISTER.COM