clavister VirtualSeries

# Clavister Virtual Stream

## High-Performance and fully virtualized security solution for agile Telecom Operators

### FEATURES AT-A-GLANCE

- High Performance - 120 Gbps of firewalling and 40 Gbps IPSec throughput
- Fully virtualized - Ready for SDN/NFV
- Flexible Orchestration and Management - Supporting multiple SDN/NFV Platforms
- 100% Carrier-Grade
- Designed for COTS x86 hardware
- Optimized for Intel Technologies such as SR-IOV and QuickAssist
- Swedish technology - No backdoors

The era of Big-Iron security products with massive costs and poor scalability is soon comming to its end. Meeting the challenges of rapidly increasing data traffic and number of IoT devices calls for new, more flexible, scalable and high-performing solutions.

Clavister Virtual Stream Series is our telecom-graded virtualized firewall powered by Clavister cOS Stream with support for both VMware vSphere and KVM hypervisors.

Thanks to its multi-core architecture and capability to utilize the latest technologies from Intel®, Clavister Virtual Stream Series delivers extreme performance, making it the fastest virtual security gateway on the market today.

High-performance, elastically scalable and a feature-set tailored for telecom scenarios make the VSS ideal for a wide range of use-cases including for example in:

- **Centralized LTE SEG in Evolved Packet Core (vEPC or EPC)**
  Replacing proprietary hardware with COTS systems.
- **Distributed LTE SEG in RAN (vRAN or RAN)**
  Run the Clavister VSS on dedicated COTS hardware in the access network.
- **Gi/SGi Firewall for Core Network Security**
  Replace the costly Big-Iron GI/SGi firewalls with a high performance and scalable virtual security gateway.

The power of virtualization enables the Clavister Virtual Stream Series to be used in a wide range of deployment scenarios, both centralized on dedicated hardware resources, as well as distributed edge cloud applications where it coexists with other virtual machines on shared hardware resources.

| Performance* and Capacity | Clavister VS3 | Clavister VS5 | Clavister VS7 | Clavister VS9 |
|---|---|---|---|---|
| Firewall Performance (plaintext throughput) | 5 Gbps | 10 Gbps | 20 Gbps | 40 Gbps |
| IPsec VPN Performance (large packets) | 2,5 Gbps | 5 Gbps | 10 Gbps | 20 Gpbs |
| Maximum Concurrent Connections | 1,000,000 | 2,500,000 | 5,000,000 | 10,000,000 |
| Maximum Concurrent IPsec VPN Tunnels | 2,000 | 3,000 | 5,000 | 10,000 |
| Maximum Number of Users | Unrestricted | Unrestricted | Unrestricted | Unrestricted |
| Maximum Number of Routing Tables (Virtual Routers) | 50 | 100 | 200 | 1,000 |
| Maximum Number of Ethernet Interfaces | 2 | 5 | 7 | 10 |
| Maximum Number of VLAN Interfaces IEEE 802.1Q | 256 | 512 | 1,024 | 2,048 |

| Product Specific Specification | Clavister VS3 | Clavister VS5 | Clavister VS7 | Clavister VS9 |
|---|---|---|---|---|
| Form Factor | Software | | | |
| Supported Hypervisor Platforms | VMware, KVM | | | |

* Actual performance may vary depending on network conditions, number of activated services and host hardware capabilities.

## Product Features

| Firewall | |
|---|---|
| Stateful Firewall | IPv4, IPv6 |
| IP Policies | ALLOW, DROP and REJECT |
| IP Session Tracking | Stateful, Stateless |
| TCP Sequence Number Tracking | Yes |
| ICMP and ICMPv6 Echo Sequence Number Tracking | Yes |
| Threshold Rules | Flow Count, Flow Rate |
| Threshold Rule Actions | Audit, Drop, Random Drop |
| Threshold Rule Grouping | Source or Destination IP/Network/Interface |
| Ingress Filtering / IP Spoofing Protection | |
| Access Rules | IPv4, IPv6 |
| Strict Reverse Path Forwarding (RPF) | Yes |
| Feasible RPF by using Interface Equivalence | Yes |
| **Address and Port Translation** | |
| Policy-Based | Yes |
| Dynamic NAT (Source) | IPv4 |
| Symmetric NAT | IPv4 |
| NAT Pools | IPv4 |
| Determistic NAT | IPv4 |
| Port Block Allocation | IPv4 |
| Static Source Translation | IPv4, IPV6 |
| Static Destination Translation (Virtual IP / Port Forward) | IPv4, IPV6 |
| NAT Hairpinning | Yes |
| **Connectivity** | |
| Ethernet Interfaces | 1GbE, 10GbE |
| VLAN Interface, IEEE 802.1Q | Yes |
| Service-VLAN Interfaces, IEEE 802.1ad (Q-in-Q) | Yes |
| Configurable MTU | Yes |
| **Routing** | |
| Static Routing | IPv4, IPv6 |
| Policy-Based Routing (PBR) | IPv4, IPv6 |
| Virtual Routing (VR) | Yes |
| Multiple Routing Tables | Yes |
| Asymmetric Routing | Yes |
| Source-Based Routing | Yes |
| Route Failover | IPv4, IPv6 |
| Route Monitoring Methods | ARP, ND, ICMP Echo, ICMPv6 Echo |
| IPv6 Router Advertisement | Yes |
| Dynamic Routing | |
| Route Import Filtering / Route Export Filtering | Yes / Yes |
| OSPFv2 Routing Process (RFC2328) | Yes, multiple |
| OSPFv2 RFC1583 Compatibility Mode | Yes |
| OSPFv2 over VPN | Yes |
| **Interface IP Address Assignment** | |
| Static | IPv4, IPv6 |
| DHCPv4 Client | Ethernet, VLAN, Service-VLAN |
| IKE Config Mode | IPsec tunnels |
| Multiple IPv4 Addresses per Interface | Yes |
| Multiple IPv6 Addresses per Interface | Yes |

| | |
|---|---|
| **Network Services** | |
| DHCPv4 Server | Yes, multiple |
| DHCP Server Custom Options | Yes |
| IP Pool | IPv4 |
| Address Resolution Protocol (ARP) | Yes |
| ARP Publish | Yes |
| Static ARP Entries | Yes |
| Proxy ARP | Yes |
| Neighbor Discovery (ND) | Yes |
| ND Publish | Yes |
| Static ND Entries | Yes |
| Proxy ND | Yes |
| Path MTU Discovery | IPv4, IPv6 |
| **Bandwidth Management (QoS)** | |
| DSCP Forwarding | Yes |
| DSCP Copy to Outer Header | VLAN, IPsec |
| Static DSCP Assignment | VLAN, IKE, IPsec, Traffic Shaping |
| Dynamic DSCP Assignment | Traffic Shaping |
| ECN Propagation to Inner Header | IPsec |
| Traffic Shaping | |
| Policy-Based | IPv4, IPv6 |
| DSCP-Based | Yes |
| Traffic Limits / Guarantees / Prioritization | Bandwith (bps), Packet Rate (pps) |
| **Application Layer Gateway (ALG)** | |
| FTP | Allow, NAT, SAT |
| **IPsec VPN** | |
| Key Exchange | Manual, IKEv1, IKEv2 |
| Roaming Client Tunnels | Yes |
| Hub-and-Spoke VPN | Yes |
| Subnet-to-Subnet VPN | Yes |
| NAT Traversal (NAT-T) | Yes |
| Dial-on-Demand | Yes |
| Routes to Remote Network | Manual, Automatic |
| Receive Interface Filtering | Yes |
| Virtual Routing (VR) | User Data, IKE, ESP |
| Policy-Based Routing (PBR) | User Data, IKE, ESP |
| Asymmetric Routing | Yes |
| Configurable MTU | Yes |
| IPsec Pass-through | Yes |
| IKE | |
| IKE Encryption | AES-128-CBC, AES-192-CBC, AES-256-CBC, 3DES-CBC |
| IKE Authentication / Integrity | HMAC-SHA1-96, HMAC-SHA-256-128, HMAC-SHA-384-192, HMAC-SHA-512-256, HMAC-MD5-96, AES-XCBC-MAC-96 |
| Diffie-Hellman (DH) Groups | 1, 2, 5, 14, 15, 16, 17, 18 |
| IKE Identity | IP, FQDN, E-mail, X.500 Distinguished-Name (DN) |
| Rekey | IKEv1, IKEv2, IPsec |
| SA Lifetime | Seconds |
| Perfect Forward Secrecy (PFS) | Yes |
| Dead Peer Detection (DPD) | Yes |
| IKE Config Mode | Client, Server |
| IKE Negotiation over | IPv4, IPv6 |
| IKE Traffic Selectors | IPv4, IPv6 |
| IPsec Security Association (SA) Granularity | Net |
| DSCP Assignment | Static |
| IKEv1 | |
| Authentication | Pre-Shared Keys (PSK), X.509 Certificates, XAUTH |
| Phase 1 | Main Mode, Aggressive Mode |
| Phase 2 | Quick Mode |
| Initial Contact Notification | Yes |
| IKEv2 | |
| Authentication | Pre-Shared Keys (PSK), X.509 Certificates, EAP |
| Pseudo-Random Function (PRF) | PRF-HMAC-SHA1, PRF-HMAC-SHA-256, PRF-HMAC-SHA-384, PRF-HMAC-SHA-512, PRF-HMAC-MD5, AES-XCBC-PRF-128 |
| Reauthentication | Yes |

| | |
|---|---|
| Certificates | |
| Self-Signed Certificates | Yes |
| Certificate Authority (CA) Issued Certificates | Yes, e.g. VeriSign, Entrust |
| Certificate Requests | PKCS#1, PKCS#3, PKCS#7, PKCS#10 |
| Certificate Revocation List (CRL) Protocols | LDAP, HTTP |
| CRL Distribution Points (CDP) | From Certificate, Static |
| CRL Fail-Mode Behavior | Conditional, Enforced |
| Certificate Management Protocols | CMPv2 |
| IPsec | |
| IPsec Protocols | ESP |
| IPsec Modes | Tunnel |
| IPsec Encryption | AES-128-CBC, AES-192-CBC, AES-256-CBC, 3DES-CBC, NULL |
| IPsec Authentication / Integrity | HMAC-SHA1-96, HMAC-SHA-256-128, HMAC-SHA-384-192, HMAC-SHA-512-256, HMAC-MD5-96, AES-XCBC-MAC-96 |
| IPsec Outer Protocol | IPv4, IPv6 |
| IPsec Inner Protocol | IPv4, IPv6 |
| IPsec Pre-Fragmentation | IPv4, IPv6 |
| IPsec Post-Fragmentation | IPv4, IPv6 |
| Don't Fragment (DF) Bit | Copy to Outer Header, Static |
| DSCP Assignment | Copy to Outer Header, Static |
| ECN Propagation to Inner Header | Yes |
| Replay Attack Prevention (Anti-Replay) | Yes |
| Traffic Flow Confidentiality (TFC) | Inbound |
| **User Authentication** | |
| Local User Database | Yes, multiple |
| RADIUS Authentication Protocols | PAP, CHAP, EAP |
| RADIUS EAP Header Verification | EAP-SIM, EAP-AKA/AKA', EAP-MD5 |
| XAUTH IKEv1 Authentication | Yes |
| **Security Management** | |
| SSH/SCP Management | Password, Pre-Shared Keys (PSK) |
| Management Authentication | Local User Database, RADIUS |
| Command Line Interface (CLI) | Yes |
| Access Levels | Admin, Auditor |
| Remote Fail-Safe Configuration | Yes |
| Local Console (RS-232) | Yes |
| Scripting (CLI) | Yes |
| Packet Capture (PCAP) | Yes, with filters |
| System Upgrade | SSH/SCP. From version 2.10.00 and later. |
| System and Configuration Backup | SSH/SCP |
| SNTP Time Sync Client | NTPv3 (RFC1305), NTPv4 (RFC5905) |
| Configurable Time Zone | Location, UTC offset |
| Automatic Daylight Saving Time (DST) Adjustment | Yes |
| **Monitoring** | |
| Syslog | Yes, multiple servers |
| Real-Time Log (CLI) | Yes, filter |
| Log Settings per Policy | Yes |
| SNMPv2c Polling / Traps | Yes / Yes |
| Real-Time Performance Monitoring | CLI, SNMP |
| Key Metrics Monitoring | Yes, e.g. CPU Load and Memory |
| Hardware Key Metrics Monitoring | Fan Speeds, CPU and System Temperatures, Voltages, PSU Status, etc |
| **High Availability** | |
| Active Node with Passive Backup | Yes |
| Shared Virtual IP | IPv4, IPV6 |
| Firewall Connection State Synchronization | IPv4, IPV6 |
| IKE and IPsec State Synchronization | IPv4, IPV6 |
| User State Synchronization | Yes |
| DHCPv4 Client State Synchronization | Yes |
| DHCPv4 Server State Synchronization | Yes |
| Configuration Synchronization | Yes |
| Device Failure Detection | Yes |
| Dead Interface Detection | ARP, ND |
| Average Failover Time | < 800 ms |

Specifications subject to change without further notice.
Specifications in this document is based on cOS Stream 2.80.00

CID: 9150-0040-24 (2016/08)

**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

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