clavister
VirtualSeries

Clavister Virtual Core

Funktionsreiche Next Generation Firewall mit exzellenter Performance, perfekt für die Cloud

FUNKTIONEN AUF EINEN BLICK

- kosteneffektive, virtuelle Next Generation Firewall für jede Organisation, gezielt gebaut für SecaaS (Security-as-a-Service), die Cloud und virtuelle Security (kein Rack Kit notwendig);
- Next Generation Firewall Services, darunter Clavister True Application Control, Clavister Content Security Services und User Identity Awareness;
- eine extreme kleine Abstellfläche bedeutet die Möglichkeit, 50 bis 100 mehr Firewalls als unsere Wettbewerber aufzustellen;
- leistungsfähige Stateful Firewall mit Deep Packet Inspection verleiht einen höheren Sicherheitsgrad;
- flexibles, dynamisches Routing und Konnektivität, die Link-Aggregation unterstützt;
- eingebauter Support für IPsec und SSL VPN bietet einfach zu nutzende Remote-Konnektivität;
- stets integriertes Securitymanagement: zentrales Securitymanagement, webbasiertes Management und eine Befehlszeilenoberfläche (Command-line interface, CLI) sind in den Clavister Subscriptions inklusive;
- High-End-Netzwerkinfrastruktur, wie Traffic Management, Hochverfügbarkeit (High Availability, HA), Server Load Balancing und WAN Load Balancing sind in den Clavister Subscriptions enthalten;
- perfekt für jegliche SecaaS-Angebote, da als cloud-basierte und virtuelle Security-Lösung nutzbar.

Die Clavister Virtual Series ist eine Zusammenstellung von Netzwerksicherheitsprodukten, die für virtuelle und Cloud-basierende Sicherheit entwickelt wurde. Sie bietet herausragende Performance, leistungsstarke Security-Features und arbeitet ressourceneffizient. Die Clavister Virtual Series umfasst dieselben Sicherheitsfunktionen wie unsere Hardware-Produkte, ist aber für virtuelle Umgebungen konzipiert. Die Lösung lässt sich auch einfach in marktführende, virtualisierte VMware- oder KVM-Umgebungen integrieren. Ihre minimale Aufstellfläche und der extrem geringere Ressourcenverbrauch macht die Clavister Virtual Series zur optimalen Lösung für alle Arten von virtuellen und Cloud-basierten Network Security-Lösungen.

Next-Generation Firewall Services

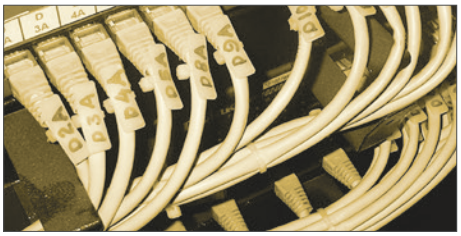
True Application Control

Clavister Virtual Series unterstützt True Application Control – einer unserer Next Generation Firewall Security Services.

Die Nutzung von True Application Control hilft Ihnen dabei, die in Ihrem Netzwerk genutzten Anwendungen sicherer zu verwalten. Mit zusätzlicher Sicherheit reduzieren Sie Ihre allgemeine Risikolage. In der Folge lassen sich kostspielige Security-Vorfälle und Downtime vermeiden. Die Funktion gibt Ihnen außerdem wertvolle Einblicke, welche Anwendungen von welchem User genutzt werden. Geschäftskritische Anwendungen lassen sich im Zuge dessen priorisieren und damit die Produktivität im Allgemeinen steigern.

Die True Application Control erkennt nicht nur mehr Anwendungen und Daten, es versteht auch, wie sich diese Applikationen verhalten, und kann direkt auf bösartige Verhaltensweisen reagieren.

Durch den einzigartigen Support der Deep Application Content Control (DACC)-Technologie ist unsere Anwendungskontrolle in der Lage, tiefgreifende Analysen durchzuführen und Anwendungsinhalte mit höheren Kontrollniveaus zu überwachen. Mit DACC können Sie Skype-IDs, SQL



Die Wahl der Konnektivität

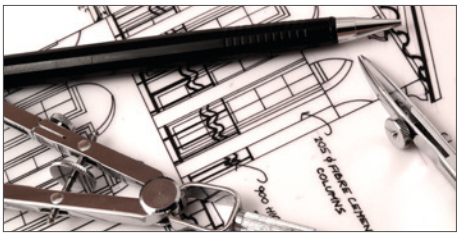
Die Clavister Virtual Series wartet mit denselben flexiblen Routing-Möglichkeiten auf wie unsere Hardware-basierten Produkte, aber sie hängt von den Fähigkeiten Ihrer Host-Umgebung ab.

Clavister Virtual unterstützt zudem die Link Aggregation, was bedeutet, dass Sie von einem weiteren Vorteil durch vergrößerten Durchsatz profitieren und die Widerstandsfähigkeit Ihres Systems erhöhen.

RADIUS Relayer – Pinpoint Security

Die Clavister Virtual Series beinhaltet den Support für RADIUS Relayer, das Nutzerinformationen und DHCP IP-Provisioning für RADIUS-basierte, authentifizierte User bereitstellt.

Ein Beispiel: Ein Nutzer verbindet sich von einem mobilen Netzwerk mit einem drahtlosen Unternehmensnetzwerk, um auf Daten zuzugreifen. Hier ist die Funktion sinnvoll, um granulare User- und gruppenbasierte Richtlinienvergabe für Traffic und Zugangskontrolle zu Netzwerkressourcen einzuplanen.



Advanced Routing

Die Clavister Virtual Series stellt eine Advanced Routing Engine bereit, inklusive Policy-basierten Routing und nahtlosen Route Failover. Dies ermöglicht dynamisches, richtlinienbasiertes Routing, bei dem der Traffic in Abhängigkeit von dynamischen Events geroutet werden kann, darunter Nutzeridentität, Latenz, HTTP-Antworten etc.

Dadurch sind Sie in der Lage, wirklich flexible und anspruchsvolle Richtlinien anzulegen, die die echten Anforderungen Ihres Netzwerks reflektieren.

Queries, Facebook-Chattexte, VoIP-Anrufinformationen und mehr nachvollziehen und visualisieren.

Clavister SSL Inspection für Application Control ist ein hochperformanter und nicht-intrusiver Weg, um sogar SSL-verschlüsselte Anwendungen zu identifizieren und zu kontrollieren. True Application Control ist im Clavister Security Subscription (CSS)-Service enthalten.

Content Security Services

Da Angriffe immer schwerwiegender werden und sich die Bandbreite an Bedrohungen dynamisch wandelt, reicht der Einsatz einer herkömmlichen Firewall nicht aus, um Attacken auf Ihr Netzwerk zu verhindern. Vielmehr müssen zusätzliche Messtechniken eingesetzt werden. Clavister bietet Best of Breed Content Security Services, u.a. ein Intrusion Detection and Prevention-System, eine netzwerkzentrierte Antivirus-Software von Kaspersky Labs sowie Web Content Filtering, um weitere Security Layer zur Firewall hinzuzufügen. Diese Content Security Services schützen Ihr Netzwerk vor fortschrittlichen Bedrohungen, die Ihre Firewall allein nicht aufhalten kann. Die Content Security Services sind Teil des Clavister Security Subscription (CSS)-Service.

User Identity Awareness

User Identity Awareness (UIA) sorgt für granulare Sichtbarkeit der Nutzeridentität und ermöglicht es Ihnen, den Netzwerkzugang auf Nutzerlevel zu kontrollieren. Die User Identity Awareness in Kombination mit der True Application Control-Funktionalität gibt Ihnen ein vielseitiges Werkzeug an die Hand, um granulare Visibilität und Kontrolle darüber zu erlangen, wer was wann in den Netzwerken tut. Sie haben die Möglichkeit, Nutzerzugriffe auf Anwendungen zielgerichtet festzulegen – über drahtgebundene und drahtlose Netzwerke hinweg, unabhängig vom verbundenen Endgerät.

Echte Security-Werte

Clavister Subscriptions

Wir sind der Meinung, dass unsere Kunden die Wahl haben sollten. Aus diesem Grund lassen wir Ihnen die Wahl zwischen unserer umfangreichen Clavister Product Subscription (CPS) oder unserer All-inklusive-Option mit Full Service: Clavister Security Subscription (CSS).

Clavister Product Subscription

Die CPS umfasst erweiterte Produktdienstleistungen, wie z.B. Softwareupdates, Support für das zentralisierte Management und flexible Service-Pläne.

Um sicherzustellen, dass Sie das Beste aus Ihrem Clavister Security Gateway herausholen können, bieten wir Ihnen rund um die Uhr Support von unserem preisgekrönten technischen Support-Team -mit hochprofessionellen Technikern, die Ihnen im Falle eines Falles weiterhelfen. Die CPS hält Ihre Clavister-Lösungen 24/7 auf dem neuesten Stand, online und geschäftsbereit.

Clavister Security Subscription

Die CSS ist eine komplette, All-inklusive-Suite an Produktdienstleistungen. Sie umfasst alle Services der CPS, aber erweitert sie noch durch mehrere Next Generation Firewall Services, wie z.B. Clavister True Application Control, Web Content Filtering, Antivirus und Intrusion Detection and Prevention (IDP).

CSS stellt herausragende Serviceinhalte bereit, die Sie vor den fortschrittlicheren Arten von Malware und Expoits schützen. Sie gibt Ihnen Zugang zur aktuellsten Software und zu Signaturupdates, die Ihre Infrastruktur auf dem neuesten Stand halten und sie stabiler sowie sicherer machen.

Alle Clavister Subscriptions sind mit 12-, 24-, 36-, 48- und 60-monatiger Service-Laufzeit verfügbar, sodass Sie von maximaler Sicherheit und Flexibilität profitieren.

Weitere Informationen zu den Clavister Subscriptions sind in der separaten Broschüre über die Services zu finden.

Echte Flexibilität – mehr Performance, wenn Sie sie benötigen

Die Clavister Virtual Series sind als vier verschiedene Modelle erhältlich, die alle spezifische Kundenanforderungen abdecken. Sollten Sie mehr Performance benötigen, verleiht Ihnen Clavister die Flexibilität, auf eine leistungsfähigere Clavister Virtual Series-Lösung umzusteigen. Dazu bestellen Sie lediglich das gewünschte Upgrade und installieren die neue Lizenzdatei. So einfach ist das. Aufgrund der extrem kleinen Aufstellfläche müssen Sie Ihre Server-Hardware wahrscheinlich nicht upgraden. Die Lösung wird sich gut einfügen.

Das macht die Clavister Virtual Series zu einer risikoarmen Wahl in dynamischen Geschäftsumgebungen, in denen sich Anforderungen über Nacht ändern können. Clavister vermeidet teure Vorinvestitionen in Ihre Infrastruktur oder Sorgen über kostspielige Upgrades.

Uptime-Technologien

Die Clavister Virtual Series kommt mit leistungsfähigen Features, um sicherzustellen, dass Ihre Netzwerkinfrastruktur online und bereit für die Arbeit ist. Funktionen wie High Availability (HA) werden komplett unterstützt, ebenso wie Fast Route Failover-Technologien und Link Aggregation. Dies gewährleistet, dass Ihr Unternehmen nicht durch Netzwerk-Downtimes beeinträchtigt wird, die durch Link-Versagen oder Hardware-Probleme ausgelöst wurden. Sie unterstützt darüber hinaus Flood Protection-Technologien, um die Uptime zu erhöhen, wenn Ihr Netzwerk einer Denial-of-Service (DoS)-Attacke ausgesetzt ist.

Leistungsfähige Firewall

Die Clavister Virtual Series ist eine Next Generation Firewall, aber sie umfasst ebenso alle traditionellen Security-Features, so wie Stateful Firewall mit Deep Packet Inspection, die von unserem eigenen Inhouse-Netzwerksicherheitsbetriebssystem angetrieben werden: dem Clavister cOS Core. Neben der Bereitstellung traditioneller Firewall-Funktionen wie Port Blocking und Proxy Server bieten alle Clavister Firewall-Lösungen Next Generation Firewall-Funktionen, um fortschrittliche Angriffe auf Anwendungsebene zu erkennen und zu blockieren. Das Ergebnis: höhere Sicherheitslevel, höherer Traffic-Durchsatz und minimale Nutzung von Systemressourcen.

Performance

Die Clavister Virtual Series bietet Next Generation Security Services über alle Punkte Ihres Netzwerks hinweg, ohne den Leistungsdurchsatz zu schmälern. Spezifisch gebaute Hardware, die auf unserem hocheffizienten Netzwerksicherheitsbetriebssystem läuft, gewährleistet, dass der Firewall Performance-Durchsatz einer der höchsten der Industrie ist. Dies stellt sicher, dass Ihre Clavister-Firewall nicht zum Flaschenhals in Ihrer Netzwerkinfrastruktur wird.

Einfachheit

Wir streben danach, Dinge einfach, verständlich und bedienbar zu machen. Dieser Anspruch umfasst alles vom Hardware-Design bis zum Security Management. Wir bauen hoch individualisierbare Enterprise-Grade Firewalls; und trotz der enthaltenen Komplexität bemühen wir uns darum, es einfach bedienbar zu machen. Zum Beispiel nutzt unser bekanntes zentralisiertes Security Management System Clavister InControl farbcodierte Attributgruppen. Sie liefern einen klaren Überblick über die Abhängigkeiten, die zwischen den Firewall-Regeln untereinander bestehen. Auf diese Weise unterlaufen weniger menschliche Fehler. Durch die Zusammenlegung von Richtlinien und Services kann das Firewall Policy Management vereinfacht und einfacher bedienbar gemacht werden. Daraus folgen weniger Policy-Regeln, was die Verwaltung einfacher und eine Security-Lücke unwahrscheinlicher macht.

All inclusive-Sicherheitsmanagement

In jedem Netzwerk ist das Sicherheitsmanagement einer der wichtigsten Aspekte. Dabei sollte die Verwaltung intuitiv, effizient und einfach zu bedienen sein. Große Unternehmen mit verschiedenen Firewalls an verschiedenen Standorten, die geographisch weit voneinander entfernt sind, sollten ihr Sicherheitsmanagement konsequent, zentral und auf dem neuesten Stand halten, was keine einfache Aufgabe ist. All diese Security-Management-Features sind kostenlos in unsere Clavister cOS-Produkte integriert.

Clavister InControl – zentralisiertes Sicherheitsmanagement

Clavister InControl ist eine zentralisierte Management-Lösung, die Administratoren dabei unterstützt, ihre täglichen Aufgaben einfacher, schneller und zielgerichteter durchzuführen. Die intuitive Benutzeroberfläche und die Integration eines taskgesteuerten Workflow-Managements erleichtern Administratoren das Erledigen komplexer, sich oft wiederholender Aufgaben, was speziell bei großen Installationen wichtig ist. Dank eines Triple-AAA-Supports (Authentifizierung, Autorisierung und Audit) verwaltet das Clavister InControl-System alle Konfigurationen und hält sie unter strenger Kontrolle. Dieser Grad der Kontrolle ermöglicht es, das Management zu delegieren, sodass bestimmtes Personal nur auf bestimmte Teile des Systems zugreifen darf.

Clavister InControl lässt sich erweitern und kann mit vielen anderen Managementsystemen zusammenarbeiten. Dies gelingt durch den Einsatz des Clavister InControl Software Development Kit (SDK). Das SDK versetzt Organisationen in die Lage, bestehende Systemmanagement-Tools, z.B. Helpdesk-Funktionen, in Clavister InControl zu integrieren.

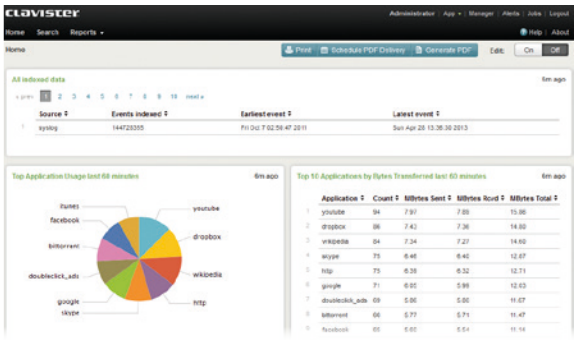
Splunk für Clavister

Splunk für Clavister cOS Core ist ein webbasierendes, unternehmensweites Enterprise-Reporting-System, das eng mit Clavister COS-Produkten zusammenarbeitet. Die Lösung Splunk unterstützt Echtzeit-Analysen mit Key Performance-Indikatoren (KPI), Grafiken, Tabellen und langfristigen Trendanalysen – skalierbar von einem einzigen Clavister Security Gateway bis hin zu großen Rechenzentren.

Mit Splunk können Sie Ihre Clavister-Sicherheitslösung visualisieren, z.B. indem Sie Problembereiche des Netzwerks, verteilte Attacken oder andere Security-Schwächen orten und anschließend in Geschäftsberichten zusammenfassen. Nutzen Sie zudem die Vorteile der integrierten Planungs- und Verteilungsfunktionen, um sicherzustellen, dass die Berichte rechtzeitig die richtigen Personen erreichen.

Andere Managementoptionen

Ergänzend zu unserer zentralen Managementlösung bieten wir ein Clavister-Webmanagementsystem an; eine einfach zu bedienende webbasierende Security-Management-Lösung für kleinere Installationen mit wenigen Firewalls. Jedes unserer Produkte unterstützt dabei unser Command-Line Interface (CLI), welches allgemeine Aufgaben festhält.



DIE HIGHLIGHTS DER CLAVISTER SECURITY GATEWAY SERIES

Next Generation Firewall Security

Durch die Integration von Next Generation Firewall-Funktionen wie True Application Control, Intrusion Detection und Prevention (IDP), Antivirus, Web Content-Filterung, Deep Packet Inspection, IPsec- und SSL VPN-Verbindungen ist unsere Lösung in der Lage, Sie gegen alle Attacken auf Netzwerk- und Anwendungsebene sowie Viren und Würmer zu schützen. Währenddessen haben Sie die volle Kontrolle über alles, was im Netzwerk passiert.

Clavister cOS Core

Clavister cOS Core ist unser eigens entwickeltes, hochperformantes Sicherheitsnetzwerkbetriebssystem. Jede Codezeile wurde dabei sorgfältig ausgearbeitet, um sicherzustellen, dass jederzeit die maximale Leistung erreicht werden kann. Sie haben unser Produkt jederzeit zu 100 % unter Kontrolle und müssen nicht ständig zwischen mehreren Open Source-Komponenten wechseln.

Flexibel und anpassungsfähig

Nicht alle Netzwerke sind gleich. Große Unterschiede liegen vor allem in der Netzwerktopologie und Konfiguration. Um für alle Bereiche gerüstet zu sein, benötigen Sie einen Security Gateway. Unsere Modelle geben Ihnen die Freiheit, Routing-Richtlinien einzurichten und Prozesse im Netzwerk granular zu kontrollieren. Um Richtlinien und Regeln zu erstellen, werden verschiedene Parameter verwendet. Damit lassen sich auch anspruchsvolle Netzwerkinstallationen individuell anpassen.

Große Leistung – minimaler Wartungsaufwand

Alle Clavister Security Gateways haben ein gemeinsames Merkmal: Sie unterstützen alle unser Clavister Service Provisioning Network (CSPN). Dieses sichere Hochgeschwindigkeitsnetzwerk stellt sicher, dass alle Clavister Security Subscription Services stets aktualisiert werden, um für aktuelle Bedrohungen ausgerüstet zu sein. Dies gibt Administratoren die Sicherheit, sich auf den Betrieb ihrer Netzwerke zu konzentrieren, ohne stets neue Security Patches installieren zu müssen.

Skalierbare Lizenz

Ein wichtiger Aspekt unserer Produkte ist ihre Skalierbarkeit. Unser Lizenzmodell ermöglicht Ihnen, die Firewall-Leistung zu nutzen, die Sie wirklich benötigen. Falls Sie zu einem späteren Zeitpunkt mehr Leistung benötigen, können Sie bei uns einfach upgraden. Sie haben dabei die Möglichkeit, zwischen zwei Subscription-Modellen zu wählen: Zum einen gibt es die Security Subscription, unsere All inclusive-Subscription, zum anderen steht Ihnen unsere reguläre Clavister Produkt-Subscription zur Verfügung.

Niedrige Gesamtbetriebskosten

Unser Ziel ist es, eine komplette Sicherheitslösung anzubieten, die kostengünstiger als Konkurrenzprodukte ist. Die Clavister Security Gateways verfügen über integrierte Security-Features, bieten einen kundenorientierten Service und Support und ermöglichen eine umfassende Administration des Netzwerks. Sie sparen sich somit die Zeit, die Sie früher in puncto Security-Management opfern mussten: Das Netzwerk ist ab sofort immer up to date, wodurch die Gesamtbetriebskosten Ihrer Sicherheitsinfrastruktur deutlich minimiert werden.

Performance* und Kapazität	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Firewall Performance (Klartext-durchsatz)	300 Mbps	1 Gbps	2 Gbps	3 Gbps	6 Gbps	10 Gbps
IPsec VPN Performance (große Pakete)	150 Mbps	500 Mbps	1 Gbps	2 Gbps	3 Gbps	5 Gpbs
Maximale parallele Verbindungen	16,000	64,000	128,000	250,000	512,000	2,000,000
Maximale parallele IPsec VPN-Tunnel	25	500	1,000	1,500	3,000	5,000
Maximale parallele L2TP-/PPTP-/SSL VPN-Tunnel	25	500	1,000	1,500	3,000	5,000
Maximale Nutzerzahl	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt	Unbeschränkt
Maximale Anzahl von Routing Tables (virtuelle Router)	5	25	50	100	200	1,000

Konnektivität	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Ethernet Interfaces	Bis zu 3	Bis zu 4	Bis zu 6	Bis zu 8	Bis zu 10	Bis zu 10
Interfaces für Management/High Availability (HA)	n/a	n/a	n/a	n/a	n/a	n/a
Konfigurierbare interne/externe/DMZ-Ports	n/a	n/a	n/a	n/a	n/a	n/a
RS-232-Konsolenports	n/a	n/a	n/a	n/a	n/a	n/a
Link Aggregation IEEE 802.1AX-2008 (Statisch/LACP)	Ja	Ja	Ja	Ja	Ja	Ja
Maximalanzahl VLAN Interfaces IEEE 802.1Q	8	32	256	512	1,024	2,048
Support für High Availability (HA)**	No	Ja	Ja	Ja	Ja	Ja
Service VLAN Interfaces IEEE 802.1ad (Q-in-Q)	Ja	Ja	Ja	Ja	Ja	Ja

Produktspezifische Spezifikation	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Formfaktor	Software					
Unterstützte virtuelle Plattformen	VMware ESXi, KVM					

* Die tatsächliche Leistung kann in Abhängigkeit von den Netzwerkbedingungen, der Anzahl der aktivierten Services und den Hardware-Kapazitäten des Hosts variieren.

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

Wo gibt es Clavister zu kaufen?

Mehr Informationen zu den Clavister-Produkten finden Sie auf www.clavister.com/partners. Zusätzliche Informationen und Kundenreferenzen sind unter www.clavister.com/resources verfügbar.

Product Features

Firewall	
Stateful Firewall / Deep Packet Inspection	Ja / Ja
IP Policies	ALLOW, DROP und REJECT
Mehrfache IP-Regelsätze	Ja
User- und Gruppen-basierte Policies	Ja
Vorgeplante Policies	Ja
DoS- und DDoS-Erkennung und -Prävention	Ja
Grenzwertregeln (Threshold, Verbindungszähler und Grenzwerte)	Ja
IP Blacklisting / Whitelisting	Ja / Ja
TCP Sequenznummernverfolgung	Ja
Ingress Filtering/IP Spoofing-Schutz	
Zugangsregeln	Ja
Strict Reverse Path Forwarding (RPF)	Ja
Durchführbares RPF unter Nutzung der Interface-Äquivalenz	Ja
Adressen- und Port-Übersetzung	
Policy-basiert	Ja
Dynamisches NAT (Quelle)	Ja
Symmetrisches NAT	Ja
NAT Pools	Ja
Statische Quellenübersetzung	Ja
Statische Zielübersetzung (virtuelle IP/Port Forward)	Ja
NAT Hairpinning	Ja
Server Load Balancing (SLB)	
SLB Verteilungsmethoden	Round-Robin, Verbindungsrate
SLB Monitoringmethoden	ICMP Echo, Custom TCP Port, HTTP Request/Response
SLB Server Stickiness	State, IP-Adresse, Netzwerk
Betriebsmodus	
Transparent-Modus (Layer 2)	Ja
Routing-Modus (Layer 3)	Ja
Gemischter Transparent- und Routing-Modus	Ja
Routing	
Statisches Routing	Ja
Policy-basiertes Routing (PBR)	Ja
Vorgeplantes Policy-basiertes Routing	Ja
Virtuelles Routing	Ja
Mehrfache Routing-Tabellen	Ja
Loopback Interfaces	Ja
Route Load Balancing (Equal Cost Multipath)	Ja
Route Failover	Ja
Route Monitoringmethoden	ARP, ICMP Echo, Custom TCP Port, HTTP Request/Response
Quellenbasiertes Routing	Ja
Dynamisches Routing	
Policy-basiertes dynamisches Routen	Ja
OSPFv2 Routing-Prozess (RFC2328)	Ja, mehrfach
OSPFv2 RFC 1583 Kompatibilitätsmodus	Ja
OSPFv2 über VPN	Ja
Multicast	
Multicast Forwarding	Ja
IGMPv2 Kompatibilitätsmodus (RFC2236)	Ja
IGMPv3 (RFC3376)	Ja
IGMP Proxy-Modus	Ja
IGMP Snoop-Modus	Ja
Transparent-Modus (L2 Bridge Mode)	
Policy-basiert	Ja
MPLS Passthrough	Ja
Spanning Tree BPDU Relaying	Normal (STP), Rapid (RSTP), Multiple (MSTP), Per VLAN Spanning Tree Plus (PVST+)
IP-Adressvergabe	
Adressvergabe pro Interface	Ja
Statisch	Ja
DCHP Client	Ethernet, VLAN
PPPoE Client	Ethernet, VLAN
PPTP/L2TP Client	Ja
Netzwerk-Services	
DHCP Server	Ja, mehrfach

DHCP Server Custom-Optionen	Ja
DHCP Relay	Ja, mehrfach
IP Pool	Ja
Proxy ARP	Ja
Dynamische DNS-Services	DynDNS.org, Dyns.cx, CJB.net, Peanut Hull
Custom HTTP Poster	Ja
Bandbreitenmanagement	
Policy-basiertes Bandbreitenmanagement	Ja
Vorgeplante Policies	Ja
Bandbreitengarantien/-grenzen/-priorisierungen	Ja / Ja / Ja
DSCP-/ToS-basiert	Ja
Bandbreitenmanagement pro Gruppe	Ja
Dynamische Bandbreiten-Balance zwischen Gruppen	Ja
Paketratengrenzen	Ja
DSCP Forwarding	Ja
DSCP-Kopie an Auftragskopf	VLAN, IPsec
Application Control	
Erkennbare Anwendungen	< 2,000
Erkennung von SSL-basierten Anwendungen	Ja
Application Content Control	2.400
Policy-basiert	Ja
Auf Anwendungen zutreffende Policies	Ja
Auf Anwendungsinhalte (Metadaten) zutreffende Policies	Ja
Policy-Aktionen	Audit, DROP, Bandbreitenmanagement
Intrusion Detection and Prevention	
Policy-basiert	Ja
Signaturauswahl pro Policy	Ja
Policy-Aktionen	Audit, DROP, Bandbreitenmanagement
Stateful Pattern Matching	Ja
Protokoll- und Ratenanomalien-Erkennung	Ja
Schutz vor Einfügen und Umgehen	Ja
Dynamisches IP Blacklisting	Ja
Automatische Signatur-Updates	Ja
Content Security	
Policy-basiert	Ja
Protokollvalidierung	HTTP, HTTPS, FTP, SMTP, POP3, TFTP, SIP, H.323, PPTP, TLS/SSL
Web Content Filtering	
HTTP / HTTPS	Ja / Ja
Audit-/Blockmodus	Ja / Ja
Klassifizierungskategorien	32
URL Whitelisting/Blacklisting	Ja / Ja
Individualisierbare Beschränkungsseiten	Ja
Cloud-basierte URL-Klassifizierungsquelle	Ja
SafeSearch-Durchsetzung	Google, Yahoo, Bing
Antivirus	
Unterstützte Protokolle	HTTP, HTTPS, FTP, SMTP, POP3
Stream-basiertes Scanning	Ja
Dateityp-Whitelisting	Ja
Scanning von Dateien in Archiven (ZIP/GZIP)	Ja
Nested Archives Support (ZIP/GZIP)	Ja, up to 10 levels
Automatische Updates	Ja
Anti-Spam	
Supported Protocols	SMTP, POP3, IMAP
Anti-Spam Detection Mechanisms	Ja
Reply Address Domain Verification	POP3, IMAP
Malicious Link Protection	POP3, IMAP
Distributed Checksum Clearinghouses (DCC)	POP3, IMAP
DNS Blacklisting	SMTP, POP3, IMAP
Anti-Spam Actions	
Strip Malicious Links	POP3, IMAP
Tag Subject and Headers	SMTP, POP3, IMAP
Send to Quarantine E-mail Address	SMTP
E-mail Rate Limiting	SMTP
Dateiintegrität	
Unterstützte Protokolle	HTTP, HTTPS, FTP, SMTP, POP3

Dateityp-Whitelisting/Blacklisting	Ja / Ja
Dateierweiterung und MIME-Typenverifikation	Ja
Application Layer Gateway	
Unterstützte Protokolle	Ja
Dateityp-Whitelisting/Blacklisting	Ja
Dateierweiterung und MIME-Typenverifikation	Ja
SIP (NAT / SAT)	Ja
H.323 / H.323 Gatekeeper (NAT / SAT)	Ja
SMTP (Content Security)	Ja
POP3 (Content Security)	Ja
SSL / TLS (Offloading)	Ja
PPTP (Passthrough, NAT / SAT)	Ja
IPsec VPN	
Internet Key Exchange	IKEv1
IKEv1-Phase 1	Main Mode, Aggressive Mode
IKEv1-Phase 2	Quick Mode
IPsec-Modi	Tunnel, Transport
IKE-Verschlüsselung	AES, 3DES, DES, Blowfish, Twofish, Cast-128
IPsec-Verschlüsselung	AES, 3DES, DES, Blowfish, Twofish, Cast-128, NULL
AES Key Size	128, 192, 256
IKE-/IPsec-Authentifizierung	SHA-1, SHA-256, SHA-512, MD-5
Perfect Forward Secrecy (DH-Gruppen)	1, 2, 5, 14, 15, 16, 17, 18
IKE-Konfigurationsmodus	Ja
Dead Peer Detection (DPD)	Static
Pre-Shared Keys (PSK)	Ja
X.509-Zertifkate	Ja
PKI-Zertifikatsanforderungen	Ja
PKI Certificate Requests	PKCS#1, PKCS#3, PKCS#7, PKCS#10
Self-Signed-Zertifikate	Ja
Certificate Authority Issued Certificates	Ja, VeriSign, Entrust etc.
Certificate Revocation List (CRL)-Protokolle	LDAP, HTTP
CRL Fail-Mode Behavior	Conditional, Enforced
IKE-Identität	IP, FQDN, E-mail, X.500 Distinguished-Name
Security Association Granularity	Net, Host, Port
Replay Attack Prevention	Ja
Richtlinienbasiertes Routing	Ja
Virtuelles Routing	Ja
Roaming Client Tunnels	Ja
NAT Traversal (NAT-T)	Ja
IPsec Dial-on-Demand	Ja
IPsec Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Redundante VPN-Tunnel	Ja
IPsec Passthrough	Ja
SSL VPN	
TLS/SSL VPN	Ja
Einmalige Client-Installation	Ja
Browserunabhängig	Ja
VPN Policy Selection Through	Firewall Rule Set, Routing und Policy-Based Routing
Split Tunneling	Ja
SSL VPN IP Provisioning	IP Pool, Static
L2TP VPN	
L2TPv2 Client (LAC)	Ja
L2TPv2 Server (LNS)	Ja
L2TPv3 Client (LAC)	Ja
L2TPv3 Server (LNS)	Ja
L2TP over IPsec	Ja
L2TP Tunnel-Auswahl durch	Firewall Rule Set, Routing, Policy-Based Routing
L2TP Client Dial-on-Demand	Ja
L2TPv2 Server IP Provisioning	IP Pool, Static
Andere Tunnels	
PPPoE Client (RFC2516)	Ja
Unnumbered PPPoE	Ja
PPPoE Client Dial-on-Demand	Ja
PPTP Client (PAC)	Ja
PPTP Client Dial-on-Demand	Ja

PPTP Server (PNS)	Ja
PPTP Server IP Provisioning	IP Pool, Static
MPPE Encryption (PPTP/L2TP)	RC4-40, RC4-56, RC4-128
Generic Router Encapsulation (RFC2784, RFC2890)	Ja
6in4 Tunneling (RFC4213)	Ja
Tunnel-Auswahl durch	Firewall-Regeln, Routing, richtlinienbasiertes Routing
Nutzerauthentifizierung	
Lokale Nutzerdatenbank	Ja, verschiedene
RADIUS-Authentifizierung	Ja, verschiedene Server
RADIUS-Buchhaltung	Ja, verschiedene Server
LDAP Authentication	Ja, verschiedene Server
RADIUS-Authentifizierungsprotokolle	PAP, CHAP, MS-CHAPv1, MS-CHAPv2
XAUTH IKE/IPsec-Authentifizierung	Ja
Web-Based HTTP/HTTPS-Authentifizierung	Ja
Configurable HTTP/HTTPS Front-End	Ja
L2TP/PPTP/SSL VPN-Authentifizierung	Ja
Single Sign-On	
Gerätebasierende Authentifizierung (MAC- Adresse)	Ja
ARP-Authentifizierung	Ja
RADIUS Relay	Ja
Active Directory-Integration	Microsoft Windows Server 2003, 2008 R2, 2012
Clientloser Einsatz	Ja
Client-Support	iOS, Android, Windows, OSX, Linux
Sicherheitsmanagement	
Clavister InControl für zentralisiertes Management	Clavister InControl[1]
Web User Interface (WebUI)	HTTP und HTTPS
SSH / SCP Management	Ja / Ja
Command Line Interface (CLI)	Ja
Managementauthentifizierung	Lokale Nutzerdatenbank, RADIUS
Fehlersichere Konfiguration (remote)	Ja
Lokale Konsole (RS-232)	Ja
Traffic Simulation (CLI)	ICMP, TCP, UDP
Scripting (CLI)	Ja
Packet Capture (PCAP)	Ja
System-Upgrade	SSH / WebUI / Clavister InControl. From version 9.00.01 und later.
System- und Konfigurations-Backup	SSH / WebUI / Clavister InControl
SNTP TimeSync	Ja
Monitoring	
Syslog	Ja, verschiedene Server
Clavister Log	Ja, verschiedene Server
Real-Time Log	WebUI, Clavister InControl
Log-Einstellungen mittels Richtlinien	Ja
Log Export via WebUI	Ja
SNMPv2c Polling / SNMPv2c Traps	Ja / Ja
Real-Time Monitoring-Alarme	Ja
Real-Time Performance-Management	WebUI, Clavister InControl
Hardware Key Metrics-Monitoring	CPU-Last, CPU-Temperatur, Stromspannung, Speicher etc.
NOTE: Für die Clavister-Firewalls stehen verschiedene Plugins zum Log-Monitoring bereit. Diese Monitoring-Plugins sind sowohl im Handel als auch als Open-Source-Lösung erhältlich.	
IPv6	
IPv6 Ready-Zertifizierung	Core-Protokolle, Phase-2-Router
Neighbor Discovery	Ja
Proxy Neighbor Discovery	Ja
IPv6 Path MTU Discovery	Ja
ICMPv6	Ja
IPv6 Router-Werbung	Ja
Interfaces	Ja
Ethernet Interfaces	Ja
VLAN Interfaces (802.1q)	Ja
Link Aggregation IEEE 802.1AX-2008 (Static/LACP)	Ja
Interface IPv6 Address Assignment	Static
Firewall	
IP-Richtlinien	ALLOW, DROP und REJECT
Stateful Firewall	Ja
Ingress Filtering	Ja
Pv6-Routing / Richtlinienbasiertes Routing	Ja / Ja

Funktionalität	
DHCPv6 Server	Ja
Application Control	Ja
Hochverfügbarkeit	
Aktiver Modus mit passiven Backups	Ja
Firewallverbindung-Zustandssynchronisierung	Ja
IKE-/IPsec-Zustandssynchronisierung	Ja / Ja
Nutzer- und Buchhaltungszustandssynchronisierung	Ja
DHCP Server and Relayer- Zustandssynchronisierung	Ja
Synchronisierung dynamischer Regeln	Ja
IGMP-Zustandssynchronisierung	Ja
Server Load Balancing (SLB)-Zustandssynchronisierung	Ja
Konfigurationssynchronisierung	Ja
Gerätefehler-Erkennung	Ja
Dead Link- / Gateway- / Interface-Erkennung	Ja / Ja / Ja
Durchschnittliche Failover-Zeit	< 800 ms

Technische Daten können ohne vorherige Ankündigung geändert werden. CID: 9150-0040-24 (2015/10)

[1] See Clavister InControl datasheet for compatible versions.

Über Clavister:
Gegründet im Jahr 1997, ist Clavister ein führender Mobile- und Network Security-Provider. Die preisgekrönten Lösungen basieren auf Einfachheit, gutem Design und sehr guter Performance, um sicherzustellen, dass Cloud-Service-Anbieter, große Unternehmen und Telekommunikationsbetreiber den bestmöglichen Schutz gegen die digitalen Bedrohungen von heute und morgen erhalten. Alle Produkte sind in einem skandinavischen Design entworfen, gekoppelt mit schwedischer Technologie. Clavister hält außerdem einen Weltrekord für den schnellsten Firewall-Durchsatz. Weitere Informationen erhalten Sie unter www.clavister.com.

Wo kaufen?
www.clavister.com/partners

Kontakt
www.clavister.com/contact

clavister®
WE ARE NETWORK SECURITY

Clavister DACH, Paul-Dessau-Str. 8, D-22761 Hamburg, Germany
■ **Phone:** +49 40 411259-0 ■ **Fax:** +49 40 411259-299 ■ **Web:** www.clavister.com