Clavister NetWall

Virtuelle Appliances 2019

CLAVISTER®
CONNECT . PROTECT

Virtuelle Clavister Appliances

Alle virtuellen Clavister Appliances werden mit dem von Clavister selbst entwickelten Betriebssystem cOS Core ausgeliefert.

Durch diese komplette Eigenentwicklung der Software in Schweden inklusive des Verzichts auf OpenSource-Komponenten sind Clavister Firewalls 100% Backdoor-frei. Ebenfalls sind auch Schwachstellen wie „Heartbleed“, „Shellshock/Bash“, „Ghost“ oder „FREAK“, aber auch noch zu entdeckende OpenSource-Bugs in Clavister Lösungen nicht möglich. Eine einheitliche Software auf allen Systemen stellt sicher, dass es keine Funktionsunterschiede zwischen den angebotenen Lizenzen gibt.

Auch gibt es keine Userlimitierungen, zusätzliche Bundles für die Nutzung bestimmter Funktionen oder ähnliche Einschränkungen. Die verschiedenen virtuellen Clavister Appliances unterscheiden sich lediglich in Bezug auf die zu erreichende maximale Leistung.

Clavister Services

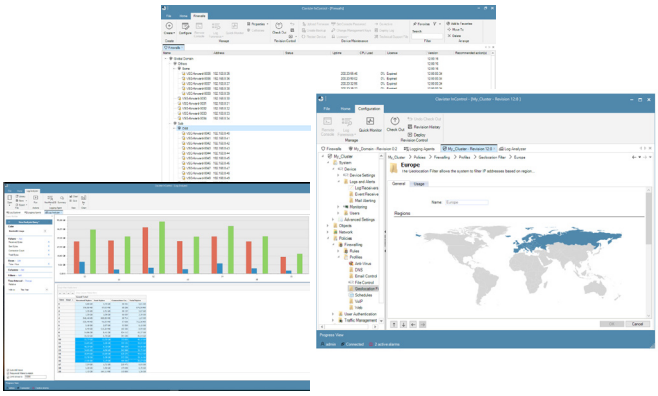
Alle virtuellen Clavister Appliances werden abhängig vom Kundenwunsch mit einem von zwei möglichen Services ausgestattet ausgeliefert, entweder der Clavister Product Subscription oder der Clavister Security Subscription.

Die Clavister Product Subscription beinhaltet sowohl Softwareservice, direkten 24/7 Herstellersupport (online, telefonisch) als auch das zentrale Management Clavister InControl. Alternativ dazu kann die Clavister Security Subscription lizenziert werden. Diese beinhaltet die Clavister Product Subscription und zusätzlich noch die vollen UTM-Funktionen (Unified Thread Management) in Form von Anti-Virus, WebContent-Filtering, Intrusion Detection and Prevention und True Application Control.

Zentrales Management Clavister InControl

Alle Clavister Appliances können zwar einzeln über eine Weboberfläche administriert werden, in beiden von Clavister angebotenen Subscriptions ist jedoch auch immer eine Lizenz für die Nutzung des zentralen Managements Clavister InControl mit enthalten.

Neben der revisionssicheren und rollenbasierten Verwaltung von allen Clavister-Lösungen in einer einheitlichen Oberfläche bietet das System auch zentrale Logging- und Auswertungsmöglichkeiten ohne weitere Kosten. Die generierbaren Reports sind komplett individuell anpassbar und können die gewünschten Informationen graphisch darstellen.



Highlights

True Application Control

Alle virtuellen Clavister Appliances bieten die Möglichkeit, True Application Control zu nutzen. Darüber lassen sich Anwendungen innerhalb des Netzwerkes und zwischen Netzwerk und Internet sowohl analysieren wie auch steuern, wie etwa Skype, SQL queries, Facebook Chat oder auch VoIP. So lassen sich unabhängig von IP-Adressen und Ports auch komplexe Anwendungen sauber abbilden.

User Identity Awareness

Alle virtuellen Clavister Appliances bieten die Möglichkeit, User Identity Awareness (UIA) zu nutzen. Diese Funktion ermöglicht sowohl auf einzelnen Arbeitsplätzen wie auch in Terminalserverumgebungen das Erstellen und Nutzen von benutzerbasierten Regelwerken.

Traffic Management

Alle virtuellen Clavister Appliances bieten die Möglichkeit, sowohl Bandbreitenmanagement wie auch Load-Balancing zu nutzen. So können etwa mehrere Internetverbindungen zeitgleich genutzt und der Datenverkehr auf diese aufgeteilt werden. Auch eine Priorisierung oder Zuweisung von bestimmten Bandbreiten einer Anwendung ist darüber zu realisieren.

VPN

Alle virtuellen Clavister Appliances bieten die Möglichkeit, verschiedene Formen von VPN zu nutzen. Es werden unter anderem IPsec, L2TP und SSL unterstützt. Die in der Lizenz angegebene maximale Anzahl an Tunneln legt hierbei nur die gleichzeitig möglichen Verbindungen fest, nicht aber die Art oder Anzahl der konfigurierbaren.

IP Reputation

Eines der besten Werkzeuge für eine starke IT-Sicherheit ist ein IP Reputation-Service, der von Minute zu Minute immer die aktuellsten Daten über schädliche IP-Adressen bereithält. Bei über vier Milliarden IP-Adressen, darunter mehr als zwölf Millionen, die Malware und Viren verbreiten, bleibt die Netzwerksicherheit so immer auf dem neuesten Stand.

Performance* and Capacity	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Firewall Performance (plaintext throughput)	300 Mbps	1 Gbps	2 Gbps	3 Gbps	6 Gbps	10 Gbps
IPsec VPN Performance (large packets)	150 Mbps	500 Mbps	1 Gbps	2 Gbps	3 Gbps	5 Gpbs
Maximum Concurrent Connections	16,000	64,000	128,000	250,000	512,000	2,000,000
Maximum Concurrent IPsec VPN Tunnels	25	500	1,000	1,500	3,000	5,000
Maximum Concurrent L2TP/PPTP/SSL VPN Tunnels	25	500	1,000	1,500	3,000	5,000
Maximum Number of Users	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Maximum Number of Routing Tables (Virtual Routers)	5	25	50	100	200	1,000

Connectivity	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Ethernet Interfaces	Up to 3	Up to 4	Up to 6	Up to 8	Up to 10	Up to 10
Interfaces for Management / High Availability (HA)	n/a	n/a	n/a	n/a	n/a	n/a
Configurable Internal / External / DMZ Ports	n/a	n/a	n/a	n/a	n/a	n/a
RS-232 Console Ports	n/a	n/a	n/a	n/a	n/a	n/a
Link Aggregation IEEE 802.1AX-2008 (Static/LACP)	Yes	Yes	Yes	Yes	Yes	Yes
Maximum Number of VLAN Interfaces IEEE 802.1Q	8	32	256	512	1,024	2,048
Support for High Availability (HA)**	No	Yes	Yes	Yes	Yes	Yes
Service-VLAN Interfaces IEEE 802.1ad (Q-in-Q)	Yes	Yes	Yes	Yes	Yes	Yes

Product Specific Specification	Clavister V2	Clavister V3	Clavister V5	Clavister V7	Clavister V9	Clavister V10
Form Factor	Software					
Supported Virtual Platforms	VMware ESXi, KVM					

* Die tatsächliche Leistung kann je nach Netzwerkbedingungen, Anzahl der aktivierten Dienste und Host-Hardwarefähigkeiten variieren.

** Bei der Verwendung von Hochverfügbarkeitsclustern in virtuellen Umgebungen müssen die Hardwareeinstellungen für jede Schnittstelle auf den Clusterknoten identisch sein (Bus, Steckplatz und Port)

Sicherheits-Use-Cases

Unsere robusten Produkte sind die perfekten Plattformen für das, was unsere wahre Leidenschaft ist: Innovative Software, die unseren Kunden die besten Anwendungslösungen liefert. Ob es sich nun um unsere exzellenten VPNs oder um Anwendungsfälle zur Traffic-Optimierung handelt, Sie können sicher sein, dass Ihre Clavister Sie in Verbindung hält, schützt und Schäden verhindert, die Ihr Unternehmen bedrohen.

CONNECT

Zuverlässiges & sicheres VPN
Anbindung von Niederlassungen und entfernten Standorten sicher und kostengünstig umsetzen

Routing & Load Balancing
Vermeiden Sie Ausfallzeiten und sichern Sie Ihre Geschäftskontinuität durch Redundanz

Sichere Netzwerkzonen
Netzwerksegmentierung zum Schutz der digitalen Unternehmensressourcen

Server Load Balancing
Vereinfachung der Skalierung und Ermöglichen einer präventiven Wartung

Sicherer Fernzugriff
Ermöglicht Remote-Mitarbeitern und -Geräten einen flexiblen und sicheren Zugriff

Single Sign-On
Schnelle, sichere Anmeldung an Ihren Apps, VPNs und Cloud Services

Stabile Verbindungskonnektivität
Vernetzung mit dem Border Gateway Routing (BGP) für Carrier-Unabhängigkeit

Carrier Grade NAT
Leistungsstarke IPv4 - IPv6 Netzwerk-Adressübersetzung

PROTECT

Firewalling
Netzwerk-Firewall zur Absicherung der IT-Ressourcen und Benutzer

Schutz vor Netzwerkangriffen
Einbruchserkennungs- und -vermeidungs-System (IDS/IPS) und Denial of Service-Schutz (DoS)

Antiviren-Überprüfung
Kontinuierlicher Scan von Anhängen in E-Mails, Web- und Datei-Downloads nach bösartigen Inhalten

Endbenutzer-Gerätesicherheit
Blockieren von Bedrohungen und Erkennen von Datenverlusten an Endgeräten

Control Signalling Validation
Gateway-Funktion für spezifische Signalisierungs-Validierung einschließlich DNS, SIP, GTP und SCTP

Sicherer Server-Schutz
Entschlüsselung des Server-Traffics für die vollständige Inspektion des eingehenden Verkehrs

PREVENT

Anwendungssichtbarkeit & Kontrolle
Kontrolle von Anwendungen und Benutzerverhalten zur Optimierung der Nutzung von Netzwerkressourcen

Web Content Filtering
Beschränken Sie den Zugriff auf unangemessene Inhalte und gefährliche Webseiten

Aktive Traffic-Optimierung
Traffic-Priorisierung sichert die gewünschte Verteilung von Ressourcen

Multi-Faktor-Authentifizierung
Eine Plattform, welche die Authentizität von Endanwendern für Cloud-/ Webanwendungen, VPN's etc. sichert

Password Self Service
Ermöglicht Endbenutzern die Verwaltung von Firmenpasswörtern

Captive Portal-Authentifizierung
Integration ins Active Directory- sowie 2FA-Verfahren für den offenen Netzzugang

Botnetz-Blockierung
Blockieren von ausgehendem und eingehendem Datenverkehr durch IP-Reputation

Benutzerverifizierung
Einfache On-Demand-Validierung der Identität des Endbenutzers

Für eine vollständige Übersicht der in Clavister-Lösungen enthaltenen Features besuchen Sie bitte www.clavister.com oder kontaktieren Sie uns direkt.

SECURITY BY SWEDEN

#NoBackDoors und Zugangsbeschränkung für Dritte

Clavister bestätigt hiermit, dass Clavister-Produkte keine "Hintertüren" enthalten, was bedeutet, dass es keine bewusst eingebauten Mechanismen gibt, die es einem Unternehmen oder einer Organisation ermöglichen würden, ohne vorherige Zustimmung des Administrators des betreffenden Produkts auf ein Clavister-Produkt zuzugreifen oder es zu kontrollieren.

John Vestberg, CEO, Clavister

www.clavister.com/SecurityBySweden

clavister®
CONNECT • PROTECT

Clavister GmbH • Kirchstr.23a • 31595 Steyerberg • Germany
Phone: +49 (0)89 21 09-3400 • Mail: info@clavister.de • Web: www.clavister.com