clavister
cOSCore

Release Highlights

Clavister cOS Core 10.21

Clavister cOS Core 10.21 is the latest version of our network security operating system powering our Clavister product range of enterprise security solutions.

The main addition in this release is SSL Inspection for Application Control. This new feature enables customers to identify applications that use the HTTPS protocol. Customers can use the result in their policy framework, for example to log application usage, prioritize or block applications based on time, user based on application type, etc.

This release also has extended support for enabling customers to transition from IPv4 to IPv6 as smoothly as possible. And more importantly, to give our customers the tools to make this transition on their own terms, in their own time. Our 6in4 Tunneling approach enables customers to selectively transform their network to IPv6 while retaining IPv4 support for system that not yet support IPv6.

Additionally, this release includes a number of new features and enhancements, such as support for SafeSearch in the HTTP ALG, support for IEEE 802.1ad (Q-in-Q) Service VLAN, L2TPv3 Client, DHCP and PPPoE client support over VLAN interfaces, RADIUS enhancements, algorithm enhancements for IKE and ESP and additional CLI enhancements.

New Features

SSL Inspection for Application Control

This new feature provides Clavister Security Gateways the capability to identify applications that use the HTTPS protocol. Based on the result, the applications can be bandwidth managed, blocked and/or logged. Combined with Clavister InControl or Splunk for Clavister, customers can create reports for application top users, application usage including HTTPS based applications and many other useful reports.

6in4 Tunneling

The new 6in4 Tunneling feature is a transition mechanism that enables customers that lack native IPv6 connectivity to setup a tunnel towards a Tunnel Broker using IPv4 and thereby be able to access IPv6 hosts and offer services on IPv6.

Key Features

- SSL Inspection for Application Control
- 6in4 Tunneling
- SafeSearch HTTP ALG
- L2TPv3 Client
- Support for IEEE 802.1ad (Q-in-Q) Service VLAN
- DHCP Client Enhancements
- PPPoE Client Enhancements
- RADIUS Enhancements
- Algorithm enhancements for IKE and ESP
- Command-Line Interface (CLI) Enhancements

This feature greatly simplifies configuring mixed networks and enables customers to continue to use IPv4 only services in a more transparent way.

SafeSearch support in the HTTP Application Layer Gateway

The major search providers, such as Google, Bing and Yahoo allow enabling of safe-search functionality to filter out adult and "unsafe" search results. The HTTP Application Layer Gateway now supports mandatory enabling of SafeSearch for all search requests on these sites, enabling network administrators to control and limit searches for unwanted material.

L2TPv3 Client

The new Layer 2 Tunneling Protocol Version 3 (L2TPv3) client combined with the existing L2TPv3 server, offers customers a solution that can be used as an alternative protocol to expensive and complex MPLS solutions for encapsulation of Layer 2 communications traffic over IP networks.

Support for IEEE 802.1ad (Q-in-Q) Service VLAN

Clavister cOS Core already provide fine granularity for configuring 802.1q tagging, enabling customers to configure the same 802.1q tag on different Ethernet Interfaces. With the addition of 802.1ad it is now possible to configure Q-in-Q, using 802.1q VLANs on top of Service VLANs (802.1ad VLANs). This new feature is very useful in service provider scenarios or for larger enterprises.

DHCP Client Enhancements

The DHCP Client is now supported on VLAN interfaces.

PPPoE Client Enhancements

It is now possible to use the PPPoE client over VLAN as well as Ethernet Interfaces.

RADIUS Enhancements

This release has added support for the `Framed-IP-Netmask` attribute. This attribute together with the `Framed-IP` attribute can be combined to generate a route. This enables customers to set up VPN tunnels using RADIUS authentication with L2TPv2/IPsec.

Integrity and authentication algorithm enhancements for IKE and ESP

The HMAC-SHA-256 and HMAC-SHA-512 integrity and authentication algorithms are now supported for IKE and ESP.

Command-Line Interface (CLI) Enhancements

The Command-Line Interface (CLI) now support viewing and filtering the Memory Log and Real-Time Log using CLI commands.

For more detailed information about the new features in Clavister cOS Core 10.21, see the **Clavister cOS Core 10.21 Administration Guide**.

Availability

Clavister cOS Core 10.21 is available for download for all customers with an active Clavister Subscription. For download information, visit www.clavister.com/my-clavister (registration required). For more information about Clavister Subscriptions, visit www.clavister.com/support/clavister-subscriptions.

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®
WE ARE NETWORK SECURITY

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