Product Specifications

Clavister® CorePlus™
Version 8.90.11

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Published 2010-03-30

Product Specifications
Clavister® CorePlus™
Version 8.90.11

Published 2010-03-30

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

Preface

The target audience for this publication is those that require a summary of the capabilites of the Clavister CorePlus network security operating system. It is the specifications document referred to by the standard Clavister End User License Agreement (EULA).

The text is divided into sections and subsections. Each section deals with a specific aspect of CorePlus functionality and lists the primary functions and capabilities of that part of the product.

Features are listed and often followed by the word "Yes" to indicate the feature exists in CorePlus. In some cases a feature can be configured so that it is either turned "Off" or "On".

These specifications are suitable both for prospective or new users who wish to have a summarized overview of the CorePlus operating system, as well as existing users who wish to have an overview of all features offered by a particular product version.

Section 1. Interfaces and Addressing

Interfaces

Ethernet Standards	Gigabit Ethernet (IEEE 802.3z, IEEE 802.3ab) Fast Ethernet (IEEE 802.3u) Ethernet (IEEE 802.3)
Virtual LAN support	IEEE 802.1Q VLANs as Logical interfaces
PPPoE support	RFC 2516 compliant
GRE support	RFC 2784 RFC 2890
Tunnel interfaces	IPsec PPTP L2TP
Loopback interfaces	Yes
Interface grouping	Yes
Symmetric interface design	Yes

Addressing

CIDR support	Yes
IP ranges	Yes
IP and network grouping	Yes

Address Translation

NAT, True dynamic address translation (RFC 1631)	Yes
SAT, static address translation	Yes
Port translation	Yes
Per-rule address translation	Yes
Time-scheduled address translation	Yes

IP Address Assigment

Static	Yes
DHCP	Static server Relay
Proxy ARP	Yes
PPP over Ethernet (PPPoE)	Yes
PPTP	Yes
L2TP	Yes

Section 2. Routing

General

IP version 4 router compliance (RFC1812)	Yes

Static Routing

Static routing support	Yes
ProxyARP support	Yes
Route fail-over support	Yes
Route fail-over monitoring	Interface link status Gateway ARP resolution

Dynamic Routing

Multiple routing tables	Yes
Virtual routing	Yes
Policy-based virtual routing	Yes
Time-scheduled virtual routing	Yes

OSPF

RFC 2328 compliant	Yes
RFC 1583 compatibility mode	Yes
Multiple OSPF routing processes	Yes
OSPF over IPsec	Yes
Dynamic routing policy rules	Yes

Transparent Mode

Transparent mode implementation	Switch routes
BPDU support	Yes
BPDU spanning protocols supported	Normal Spanning Tree Protocol (STP) Rapid Spanning Tree Protocol (RSTP) Multiple Spanning Tree Protocol (MSTP) Cisco PVST+ Protocol

Multicast

RFC 2236 compatibility mode (IGMPv2)	Yes
RFC 3376 compatible (IGMPv3)	Yes
Routing methods	Proxy mode Snoop mode

Section 3. DHCP Services

DHCP Client

DHCP client support	Yes
Multiple DHCP clients	1 Client per Ethernet interface
Assign lease parameters to network objects	Yes
Request preferred parameters	IP address Lease time
Collision detection	Yes
Filter on	Leases Server IP addresses

DHCP IP Pool

Pre-fetch to pool	Yes
Hand out method	IKE config mode

DHCP Server

Integrated DHCP server	Yes
Multiple DHCP server instances	Yes
Filter on	Source interface
Basic parameters handed out to clients	IP address Netmask, default gateway Domain Lease time Primary and secondary DNS and NBNS/WINS servers Next server
Custom DHCP options	Yes
Lease persistence after power off	Yes

DHCP Relaying

DHCP relay support	Yes
Multiple DHCP relay instances	Yes
Relay modes	Full DHCP relay BOOTP forwarding
Filter on	Source interface IP ranges
Add dynamic routes	Yes
PXE booting support (allow NULL offers)	Yes
Lease persistence after power off	Yes

Section 4. Security Mechanisms

IP Filters

Interface filter	Source and destination interfaces
Network filter	Source and destination IP networks
TCP/UDP port filter	Source and destination ports Port ranges Groups
Pre-defined ICMP filters	Echo Request Echo reply Destination unreachable Source quenching Redirect Time exceeded Parameter problem
Custom ICMP message filter	Yes
Custom ICMP code filter	Yes
Custom IP protocol number filter	Yes
Pre-defined service definitions	Yes, approx. 80 services
Time-scheduled rules	Yes

DoS Prevention and Consistency Checks

SYN flood protection	Yes, using SYNRelay
Illegal addresses	Yes
Checksum control	Yes
TTL control	Yes
Layer size consistency	Yes
IP option sizes	Yes
IP source route	Yes
IP timestamp	Yes
IP bad options	Yes
IP reserved flag	Yes
TCP blind spoofing protection	Yes
TCP header option sizes	Yes
TCP MSS control	Yes
TCP selective ACK	Yes
TCP window scale	Yes
TCP timestamping	Yes
TCP alternate checksum	Yes
TCP bad options	Yes
TCP connection count	Yes
TCP flag combinations	Yes
TCP reserved field	Yes
TCP NULL packets	Yes
TCP insertion/evasion protection	Yes
TCP sequence number scrambling	Yes
ICMP response control	Yes
ARP spoofing protection	Yes
Strict interface matching	Yes
Connection timeout control	Yes

Payload size control	Yes
Reassembly timing control	Yes
Illegal fragments	Yes
Duplicate fragments	Yes

Section 5. Application Layer Gateways

FTP ALG

SAT/NAT support	Yes
Run-time active/passive FTP Transformation	Yes
Command restrictions	Unknown Commands, SITE EXEC
Control channel restrictions	Maximum line length Command rate 8-bit Strings
Verify MIME type	Yes

HTTP ALG

SAT/NAT support	Yes
Static content filtering	Yes
Static URL blacklist	Yes
Static URL whitelist	Yes
URL list wildcarding	Yes
Active content blocking	ActiveX Flash JavaScript VBscript Cookies UTF-8 formatting check
Dynamic web content filtering	Yes
Limit file sizes	Yes
Verify MIME type	Yes

SMTP ALG

SAT/NAT Support	Yes
Rate limiting	Yes, emails per minute
Verify file MIME type	Yes
Verify sender email address	Yes
Email address black listing	Yes
Email address white listing	Yes
SPAM filtering	Yes

- RFC 2327: Session description protocol (SDP) support
- RFC 3264: Offer/answer model with SDP support
- RFC 3581: Extension to SIP for symmetric response routing support
- RFC 4145: TCP-Based media transport in SDP support
- RFC 4961: Symmetric RTP/RTCP support

POP3

Block cleartext user/pass	Yes
No response to bad username	Yes
Disallow unknown commands	Yes
Check file integrity	Yes
Verify file MIME type	Yes
Anti-virus scanning	Yes
Block/allow specific filetypes	Yes

SIP

SAT/NAT support of clients	Yes
SAT/NAT support of proxy	Yes
TCP based media channels	Yes
UDP based media channels	Yes
Standards compliance	

H.323 ALG

SAT/NAT support	Yes
Gatekeeper support	Yes
Application sharing (T.120)	Yes
Version support	H.323 v5 H.225.0 v5 H.245 v10

Section 6. User Authentication

Databases

Built-in local user database	Yes, multiple
External RADIUS server database	Yes, multiple
Microsoft Active Directory integration support	Yes, via Microsoft IAS

RADIUS Authentication (RFCs 2865, 2866, 2869)

RADIUS PAP support	Yes
RADIUS CHAP support	Yes
RADIUS Microsoft-CHAP support	Version 1 Version 2

Web Authentication

HTTP authentication	Yes
HTTPS authentication	Yes
Customizable HTTP front-end	Yes

VPN Authentication

XAuth Authentication	Yes
PPP authentication over PPTP	Yes
PPP authentication over L2TP	Yes

Section 7. Unified Threat Management

Intrusion Detection and Prevention (IDP)

Subscription based feature	Yes
Local threat signature database	Yes
Automatic database updates	Yes
Forced database updates	Yes
Signature group selection	Yes
Detection actions	Log, protect
Automatic host/network blacklisting	Yes
Whitelist hosts or networks	Yes
Optional hardware acceleration	Yes

Anti-Virus (AV)

Subscription based feature	Yes
Protocols scanned	HTTP, SMTP, FTP
Local virus signature database	Yes
Automatic database updates	Yes
Ad-hoc forced updates	Yes
Uncompressed filetypes scanned	All
Compressed filetypes scanned	Zip, Gzip
File size limit	Unlimited as default
File size limit configurable	Yes
MIME filetype verification	Yes
Explicit filetype scan exclusion	Yes
Detection actions	Log, Protect
Optional hardware acceleration	Yes

Dynamic Web Content Filtering

Subscription based feature	Yes
24/7 main database availability	Yes
Continuous URL database updating	Yes
Unreachable URLs dropped from scan	Yes
Local database URL cache	Yes
Global URL coverage	Yes
Number of content categories	32
Block at page level	Yes
Category specific blocking	Yes
Audit Mode	Yes
Allow User Override	Yes
Request URL reclassification	Yes
Customizable block webpage	Yes

Section 8. Virtual Private Networks (VPN)

IPsec

Encryption Algorithms	AES (Rijndael) 3DES DES Twofish Blowfish CAST-128 NULL Encryption
Authentication Algorithms	SHA1 MD5
IKE Modes	Main or Aggressive mode for phase 1 Quick mode for phase 2
Diffie-Hellman groups	1, 2, 5
Security Associations	Per net Per host
Keying	X.509 certificates Pre-shared keys
Peer authentication	Built-in database; IP, DNS-name, Email or X.500 distinguished-name
LAN-to-LAN VPN	Yes
Roaming clients	Yes
DNS resolving of remote gateway	Yes
PKI certificate requests (PKCS#7, PKCS#10)	Yes
Self-signed certificates	Yes
IPsec NAT traversal	Yes
VPN policy selection through	Routing Policy-based routing
Config mode	Yes
VPN tunnel keep-alive	Yes

IPsec Compliance

- RFC 822 (Standard for the format of ARPA Internet text messages): Email address formatting conventions
- RFC 2003: IP encapsulation within IP
- RFC 2315: PKCS #7: cryptographic message syntax version 1.5
- PKCS #8 Private-Key Information Syntax Standard
- RFC 2314: PKCS #10: certification request syntax version 1.5
- RFC 2401: Security architecture for the Internet Protocol
- RFC 2402: IP authentication header
- RFC 2403: Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: ESP DES-CBC cipher algorithm with explicit IV
- RFC 2410: NULL encryption algorithm and its use With IPsec
- RFC 2411: IP security document roadmap
- RFC 2412: OAKLEY key determination protocol

- RFC 2437: PKCS #1: RSA Encryption
- RFC 2451: ESP CBC-Mode cipher algorithms
- RFC 2459: X.509 Public key infrastructure certificate and CRL profile
- RFC 2510: X.509 Public key infrastructure certificate management protocols
- RFC 2511: Internet X.509 certificate request message format
- RFC 2898: PKCS #5: Password based cryptography specification
- RFC 2985: PKCS #9: Selected objects & attribute types (partial support)
- PKCS #12 Personal Information Exchange Syntax (partial support)
- RFC 2986: PKCS #10: Certification request syntax specification
- RFC 3602: The AES-CBC cipher algorithm and it's use with IPsec
- RFC 3706: Traffic-based method of detecting dead IKE
- RFC 3948: UDP encapsulation of IPsec ESP packets
- RFC 3947: Negotiation of NAT-traversal in IKE
- RFC 4303: IP encapsulating security payload (ESP)

L2TP

Encryption	MPPE
MPPE versions	RC4 40 bits RC4 56 bits RC4 128 bits
Dial on demand	Yes
IP servers	Static or from IP pool
Client requests preferred IP	Yes
L2TP over IPsec	Yes

PPTP

Encryption	MPPE
MPPE versions	RC4 40 bits RC4 56 bits RC4 128 bits
Dial on demand	Yes
IP servers	Static or from IP pool
Client requests preferred IP	Yes

Section 9. Traffic Management

Traffic Shaping

Mode of operation	Weighted queues (pipes)
Policy-based traffic shaping	Yes
Time-scheduled traffic shaping	Yes
Traffic shaping for VPN tunnels	Yes
Number of pipes	64
Priority levels	8 per pipe
Applicable limits	Bandwidth, packets per second
Granularity	Per gateway rule / 1 kbps / 1 pps
Dynamic bandwidth limit balancing	Yes
Pipe chaining	Yes
TOS bits based shaping	Yes
Optionally triggered by IDP	Yes

Traffic Rate Limiting

Connection limiting	Total connections, connections/second
Possible actions	Log Protect by blocking source
Automatic host or network blacklisting	Yes

Server Load Balancing

Policy-based server load balancing	Yes
Distribution methods	Round-robin Connection rate
Server health monitoring	ICMP Echo Custom TCP port
Server stickiness	State based IP address based Network based

Section 10. High Availability

Implementation

High availability (HA) mode	Active gateway with passive backup
State synchronization	Yes (partial for IPsec)

Detection

Device failure detection	Yes
Dead link detection	Yes
Dead gateway detection	Yes
Dead interface detection	Yes

Fail-over

Interface fail-over	Yes
Average fail-over time	800 ms

Section 11. Accounting and Logging

Accounting

RADIUS accounting	Yes
Multiple RADIUS servers	Yes
User configurable messages	Yes

Logging

Network logging	Yes
Log receivers	Syslog Clavister Logger
SNMPv2 traps	Yes
Multiple log receivers	8 maximum
Log settings per policy	Yes
Drop entry byte dump (150 bytes)	Yes (Clavister Logger only)
Real-time log message display	Yes, in FineTune
Clavister Log query facility	Yes, in FineTune
Clavister InSight support	Yes

Clavister Logger

Included with CorePlus	Yes
Unlimited installations	Yes
Platform	Microsoft Windows, Linux
Message format	Clavister FWLog format
Configuration interface	Via FineTune
Command line log query tool	Yes

Section 12. Management

Management Options

GUI Client	Clavister FineTune
Remote console commands	Via FineTune or Clavister *fwctl* tool
Linux based management	With Clavister *fwctl* tool
Local console commands	Via RS232

Clavister FineTune

Included with CorePlus	Yes
Unlimited installations	Yes
Platform	Microsoft Windows
GUI interface	Yes
Remote use	Yes
Secure communication	Via Clavister NetCon protocol
From multiple locations	Yes
Control multiple gateways	Yes

Configuration Control

Live configuration updating	Yes
Configuration version history	Yes
Configuration rollback	Yes

Hardware Monitoring (only certain hardware models)

CPU core temperature
Fan speeds
Power supply voltage
GPIO

Section 13. Monitoring

Monitoring Tools

Realtime graphical monitor	Yes, from FineTune
Command line counter display	Yes, with Clavister *fwctl* tool
SNMP client query	Yes, standard MIB

Throughput Statistics

Percentage CPU use
Forwarded bits/second
Forwarded packets/second
Percentage buffer usage
Total connections

Rule Usage Statistics

IP rules
PBR rules
DHCP rules
User authentication rules
IDP rules

Interface/VLAN/VPN Tunnel Statistics

Rx/Tx ring counters
Total bits/second
Bits/second sent
Bits/second received
Total packets/second
Packets/second sent
Packets/second received
Fragments received
Fragment reass OK
Fragment reass fail
Send fails
IP errors
Drops
Active SAs (VPN only)

Pipe Statistics

Total users
Users per pipe
Bytes/second per pipe and per precedence
Packets/second per pipe and per precedence
Dynamic limiting per pipe and per user
Delayed per pipe and per precedence
Drops per pipe and per precedence

State Engine Statistics

ICMP connections
UDP connections
Open TCP connections
TCP SYN connections
TCP FIN connections
Other connections eg. IPsec

DHCP Server Statistics

Percentage usage
Active clients
Percentage active clients
Rejected requests
Total number of leases

DHCP Relay Statistics

Total active relayed clients
Ongoing transactions
Rejected requests
Active clients per DHCP rule
Rejected packets per DHCP rule

IP Pools

Prepared
Free
Used
Misses
Client failures

General ALG Statistics

Total sessions
Total connections
Total TCP streams

HTTP ALG and Web Content Filtering Statistics

Total requests
Total allowed
Total blocks
URLs requested per category
URLs allowed per category
URLs blocked per category

User Authentication Statistics

PPP
HTTPAuth
Secure HTTPAuth
XAuth

Link Monitor Statistics

Packets lost/second
Percentage short-term loss
Percentage of hosts up

Packet Reassembly Statistics

Input drops
Load factor
Allowed buffers per connection

High Availability Statistics

Sync interface queue length
Queue usage (packets)
Queue usage (bytes)
Packets sent over sync
Resent packets

Hardware Parameters (certain hardware models only)

Temperature
Fan status

Alphabetical Index