Swedish Certification Body for IT Security

Certification Report Clavister cOS

Issue: 1.0, 2019-06-19

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a Next Generation Firewall software, offering stateful firewall and deep packet inspection functionality. The TOE, Clavister cOS Core v12.00.00, consists of three versions:

12.00.00.34-31984	VMware Virtual Machine for VMware ESXi
12.00.00.34-31985	intended for the appliances Clavister E20, E80 revA, E80 revB, W20 revA, W20 revB, W30, and W40
12.00.00.34-31986	intended for the appliance Clavister W50

The TOE can be delivered pre-installed on one of the Clavister appliances, or downloaded from Clavister's web site.

The ST does not claim conformance to any Protection Profiles.

There are seven assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the seven threats and comply with the two organisational security policy (OSP) in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB in their premises in Växjö, Sweden, to some extent in the developer's premises in Örnsköldsvik, Sweden and was completed on the 10th of June 2019.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 4, augmented by ALC_FLR.1 Flaw reporting procedures.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 4 + ALC_FLR.1.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2016009
Name and version of the certified IT product	Clavister cOS Core v12.00.00 binary versions: 12.00.00.34-31984 12.00.00.34-31985 12.00.00.34-31986
Security Target	Security Target Clavister cOS Core, version J
Assurance level	EAL 4 + ALC_FLR.1
Sponsor	Clavister AB
Developer	Clavister AB
ITSEF	Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2019-06-19

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)
- TOE Access

3.1 Security Audit

The TOE generates audit records for start-up and shutdown of the audit functions, blocked traffic, administrator account activity, firewall activity, firewall rule modification, network access, login attempts, etc.

Audit records are stored locally in memory and are exported to a Syslog server.

Administrators can select the severity level to be logged and include/exclude specific events.

The oldest record in the local memory based audit trail is overwritten when the trail space is full.

3.2 Cryptographic Support

The TOE provides TLS functionality for HTTPS communication to the Management Web interface. The library MbedTLS is used for cryptographic operations.

Hardware cryptographic acceleration may be enabled on the Clavister appliances or in the virtual machine environment hosting the TOE. Hardware cryptographic acceleration is not included in the TOE.

Keys and key material will be zeroized when no longer needed.

3.3 User Data Protection

The TOE controls network traffic via Information Flow Control Security Functional Policies (SFPs). The Access Rule SFP filter network traffic based on IP addressed and network interfaces. The IP Policy SFP filter network traffic based on source and destination network interfaces, source and destination IP networks and the Service (protocol) by stateful inspection. The Authenticated Information Flow SFP requires users to be authenticated to send information from specified source network addresses and/or access resources on destination network addresses.

3.4 Identification and Authentication

Authentication without identification is required for management through the local Console port. The Management Web interface and the Management CLI interface requires identification and authentication using username and password. The Authenticated Information Flow SFP requires the user to identify and authenticate through username and password.

3.5 Security Management

The TSF recognizes three roles: Admin, Audit and Authenticated User. The Admin and Audit roles have management privileges while the Authenticate User only have privileges related to the Authenticated Information Flow SFP. The Admin may query, modify, and delete attributes associated to the Information Flow SFPs, query and modify the TOE configuration and the set of events to be audited. The Audit may query the same entities. Both Admin and Audit may query TOE and device status information. The Admin may also restart the TOE.

3.6 Protection of the TOE Security Functions (TSF)

The TOS shall perform self-tests at during initial start-up and tests of the operation of underlying device entities may be initiated by administrators.

A secure state shall be preserved when failures occurs and are discovered by self-tests or tests of external entities.

3.7 TOE Access

Only one Admin may be authenticated at the same time. Subsequent administrator authentications will grant Audit privileges only. More than one Audit may be authenticated concurrently.

User sessions may automatically be terminated after a configurable time of inactivity and/or total session lifetime

4 Assumptions and Clarifications of Scope

4.1 Assumptions

The Security Target [ST] makes seven assumptions on the usage and the operational environment of the TOE.

A.NO_GENERAL_PURPOSE

The TOE underlying platform is assumed not to provide general purpose computing capabilities.

A.TRUSTED_ ADMINISTRATOR

Authorized administrators are assumed to be non-hostile and to act in the best interest of security for the organization. This includes being appropriately trained, following given policies, and adhering to guidance documentation. However, they are capable of making mistakes.

A.PHYSICAL_SECURE

The TOE is operated in a physically secure environment, i.e., no unauthorized person has physical access to the TOE or its underlying platform.

A.SINGLE_CONNECTION

Information cannot flow among the internal and external networks unless it passes through the TOE.

A.AUDIT_SERVER

It is assumed that an external audit server can receive and store audit events from the TOE.

A.TIME

The TOE environment provides the TOE with a reliable time stamp.

A.VIRTUAL_DEPLOYMENT

Only one instance of the TOE is executing as a guest in the virtual deployment.

No other applications are running as guests in the TOE virtual deployment.

4.2 Organizational Security Policies

The Security Target [ST] places two organizational Security Policies on the TOE.

P.MANAGE

The TOE shall be manageable only by authorized administrators.

P.ACCOUNTABLE

The TOE shall provide audit records to hold administrators accountable for their actions.

4.3 Clarification of Scope

The Security Target [ST] contains seven threats, which have been considered during the evaluation.

T.NETWORK_ACCESS

An Attacker may attempt to bypass the information flow control policy by sending information through the TOE, which results in exploitation and/or compromise of protected resources on the internal network.

T.UNDETECTED

An Attacker may attempt to compromise the assets without being detected. This threat includes the Attacker causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking the Attacker’s actions.

T.ADMIN_ACCESS

The Attacker may attempt to gain administrator access to the TOE through illicit authentication.

T.ADMIN_COMMUNICATION

The Attacker may be able to view, modify, and/or delete security related information sent between a remotely located authorized administrator and the TOE.

T.BYPASS

The Attacker may attempt to bypass, deactivate, or tamper with TOE security functions to cause unauthorized access to TOE functions, user or TSF data, or to deny access to legitimate users.

T.HALT

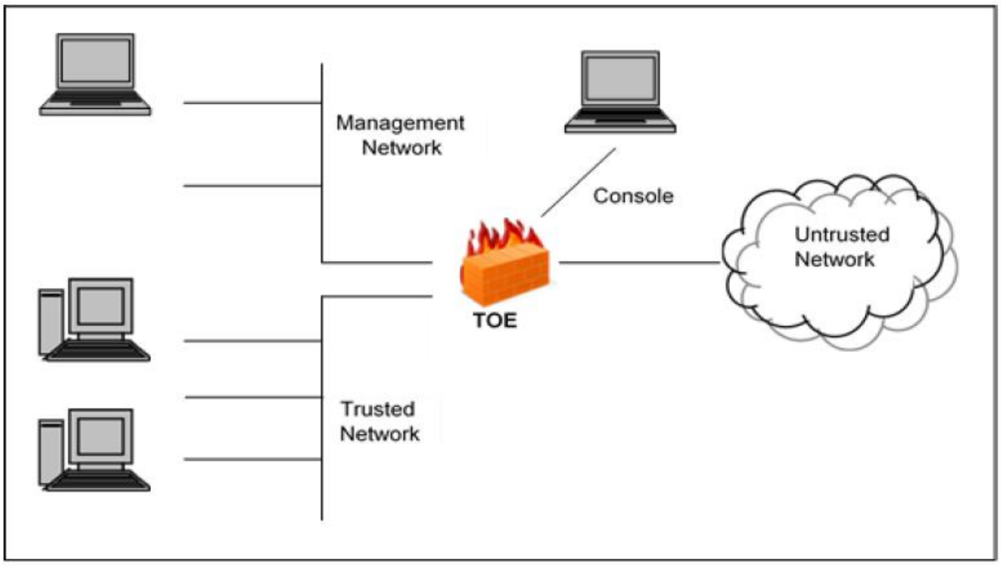
The Attacker may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.

T.FAILURE

A component of the TOE or in TOE operational environment may fail during start-up or during operations, or a TOE User may involuntarily causing a compromise or failure in the security functionality and leaving the TOE susceptible to attackers.

5 Architectural Information

The TOE is the base software engine that drives and controls dedicated hardware appliances or as a virtual deployment in a virtual machine environment. The TOE binary is pre-loaded or downloaded from Clavister’s web site.



TOE executes on one appliances: Clavister E20, E80 revision A, E80 revision B, W20 revision A, W20 revision B, W30, W40, and W50 or as a virtual machine in a VMware vSphere (ESXi) hypervisor.

The operational environment also contains the components listed below:

- Management Console
  General purpose computer with serial interface (COM-port)

- Remote administration computer
  General purpose computer with web browser for remote administration over HTTPS

- Syslog server
  General purpose computer with Syslog server compliant with RFC 5424.

6 Documentation

The guidance documentation below are part of the TOE:

- Clavister cOS Core Administration Guide, Version: 12.00.00
- Clavister cOS Core CLI Reference Guide, Version: 12.00.00
- Clavister cOS Core Log Reference Guide, Version: 12.00.00
- Guidance Documentation - Clavister cOS Core, version H

7 IT Product Testing

7.1 Developer Testing

The developer tested all three binaries, with manual and automated tests, with full TSFI coverage:

12.00.00.34-31984 on VMware ESXi v5.5

12.00.00.34-31985 on the HW appliances Clavister E20, E80 revA, E80 revB,
W20 revA, W20 revB, W30, and W40

12.00.00.34-31986 on the HW appliance Clavister W50

The tests were performed in the developer's premises in Örnsköldsvik, Sweden.

7.2 Evaluator Testing

The evaluators repeated a sample of 50% of the developer test cases in the developer site in Örnsköldsvik, Sweden on all three binaries:

12.00.00.34-31984 on VMware ESXi v6.5

12.00.00.34-31985 on the HW appliances Clavister E80 revA, and W40

12.00.00.34-31986 on the HW appliance Clavister W50

In addition, the evaluators performed complementary testing using the binary 12.00.00.34-31984 on VMware ESXi v6.5 in the evaluator premises in Växjö, Sweden.

7.3 Evaluator Penetration Testing

The evaluators used the binary 12.00.00.34-31984 on VMware ESXi v6.5 for penetration testing. Port scanning, vulnerability scanning with several tools, and fuzzing was performed. The penetration testin took place in the evaluator premises in Växjö, Sweden.

8 Evaluated Configuration

The following features are NOT part of the evaluated configuration:

- Authentication using other methods than local username and password validation
- SSH based Management CLI interface
- Secure Copy, SCP
- Clavister InControl management interface
- SMTP and InControl log receivers, SNMP traps
- SNMP
- Software update
- High Availability (HA) configuration
- VPN
- Intrusion Detection & Prevention
- Anti-Virus
- Anti-Spam
- Traffic/Bandwidth Management
- Routing
- Hardware crypto accelerator

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family		*Short name*	*Verdict*
Development		ADV	PASS
	Security Architecture	ADV_ARC.1	PASS
	Functional Specification	ADV_FSP.4	PASS
	TOE Design	ADV_TDS.3	PASS
	Implementation Representation	ADV_IMP.1	PASS
Guidance Documents		AGD	PASS
	Operational User Guidance	AGD_OPE.1	PASS
	Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support		ALC	PASS
	CM Capabilities	ALC_CMC.4	PASS
	CM Scope	ALC_CMS.4	PASS
	Delivery	ALC_DEL.1	PASS
	Development Security	ALC_DVS.1	PASS
	Life-cycle Definition	ALC_LCD.1	PASS
	Flaw Remediation	ALC_FLR.1	PASS
	Tools and Techniques	ALC_TAT.1	PASS
Security Target Evaluation		ASE	PASS
	ST Introduction	ASE_INT.1	PASS
	Conformance Claims	ASE_CCL.1	PASS
	Security Problem Definition	ASE_SPD.1	PASS
	Security Objectives	ASE_OBJ.2	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.2	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
Tests		ATE	PASS
	Coverage	ATE_COV.2	PASS
	Depth	ATE_DPT.1	PASS
	Functional Tests	ATE_FUN.1	PASS
	Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
cOS	Clavister Operating System
CPU	Central Processing Unit
CRL	Certificate Revocation List
HMAC	Keyed Hash Message Authentication Code
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure (i.e. TLS over http)
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NAT	Network Address Translation
RAM	Random Access Memory
RFC	Request for Comments
SHA	Secure Hashing Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
VPN	Virtual Private Network

12 Bibliography

ST Security Target - Clavister cOS Core, Clavister AB, 2019-06-10, document version J

ECG Guidance Documentation - Clavister cOS Core, Clavister AB, 2019-03-11, document version H

ADM Clavister cOS Core Administration Guide, Clavister AB, 2017-06-13, document version 12.00.00

CLI Clavister cOS Core CLI Reference Guide, Clavister AB, 2017-06-13, document version 12.00.00

LOG Clavister cOS Core Log Reference Guide, Clavister AB, 2017-06-13, document version 12.00.00

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2019-01-21, document version 30.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2019-01-16, document version 8.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2016-10-07:

QMS 1.19.3	valid from 2016-06-02
QMS 1.20	valid from 2016-10-20
QMS 1.20.1	valid from 2017-01-12
QMS 1.20.2	valid from 2017-02-27
QMS 1.20.3	valid from 2017-04-24
QMS 1.20.4	valid from 2017-05-11
QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13
QMS 1.21.5	valid from 2018-11-19
QMS 1.22	valid from 2019-02-01
QMS 1.22.1	valid from 2019-03-08
QMS 1.22.2	valid from 2019-05-02
QMS 1.22.3	valid from 2019-05-20

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.22.3”.

The certifier concluded that, from QMS 1.19.3 to the current QMS 1.22.3, there are no changes with impact on the result of the certification.