Security Target
Clavister cOS Core v.15.00

DOCUMENT HISTORY

Version	Status	Issue date	Revision description	Edited by
A1	Initial	2024-03-27	First version	Johan Forsberg
A2	Draft	2024-04-05	Updated after review	Johan Forsberg, Mattias Fredriksson
A	Approved	2024-04-11	Additional review edits	Johan Forsberg, Mattias Fredriksson
B1	Draft	2024-06-28	Updated after CSEC review	Daniel Mattila, Johan Forsberg
B	Approved	2024-07-05	Version B	Daniel Mattila, Johan Forsberg
C1	Draft	2024-10-08	Minor typos	Johan Forsberg
C	Approved	2024-11-01		Daniel Mattila, Johan Forsberg
D	Approved	2024-11-18	cOS Core version number	Johan Forsberg
E	Approved	2024-12-04	cOS Core version number	Johan Forsberg
F	Approved	2024-12-11	Updated table 14	Johan Forsberg
G	Approved	2025-02-11	Clarified evaluated test configuration	Johan Forsberg Daniel Mattila

Contents

1 ST Introduction

1.1 ST Reference

Title:	Security Target – Clavister cOS Core v.15.00
Version:	G
Date:	2025-02-11

1.2 TOE Reference

Target of Evaluation:	Clavister cOS Core
Version:	15.00.00.10
Developer:	Clavister AB

1.3 Document Overview

This is the Security Target for the Clavister cOS Core version 15.00 software.

Chapter 1 gives a description of the ST and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 2 states the conformance claims made.

In chapter 3, the security problem definition of the TOE is described. This includes assumptions about the environment of the TOE, threats against the TOE, TOE environment and organizational security policies that are to be employed to ensure the security of the TOE.

The Security Objectives stated in chapter 4 describe the intent of the Security Functions. The Security Objectives are divided into two groups of security objects, for the TOE and for the TOE environment.

No extended components are defined so chapter 5 is empty.

In chapter 6 the IT security functional and assurance requirements are stated for the TOE. These requirements are a selected subset of the requirements of part 2 and 3 of the Common Criteria standard.

A brief description of how the security functional requirements are implemented in the TOE is described in chapter 7.

1.4 TOE Overview

The TOE is the Clavister cOS Core 15.00.00 firewall software. cOS Core can be deployed as a virtual machine on the customer’s preferred choice of server hardware - Intel® 64 Architecture (x86_64) or Arm® architecture v8 - or installed on a range of Clavister hardware products - Intel® 64 Architecture (x86_64). The TOE is a Next Generation Firewall software, offering stateful firewall with deep-packet inspection functionality. The firewall can be installed as a

gatekeeper between networks such as local area networks and the Internet, where defined IP packet filtering policies protect the internal network or servers in DMZ zones from unauthorized traffic. Policies can be applied to interface and network combinations, as well as authenticated users and defined time periods. Decisions and other events occurring in the firewall can be logged to an external syslog server. Management of the TOE is done using an encrypted channel.

1.5 TOE Description

1.5.1 Product Overview

Designed as a network security operating system, cOS Core features high throughput performance with high reliability plus super-granular control.

The TOE includes Next Generation stateful firewalling with packet inspection functionality, IP Policies with and without user authentication, logging to a syslog server and secure remote management via HTTPS. cOS Core also offers other features not included in this evaluation, such as Application Control, Content Security Services, User Identity Awareness, Dynamic Routing, IPsec, SSL VPN, Intrusion Detection and Prevention, Anti-Virus, High Availability and a centralized management solution. These non-TOE features must be configured to be activated and may in some cases also need an additional service level software license, and therefore do not affect the evaluated configurations security properties.

1.5.2 System Overview

The system configuration is comprised of an internal, trusted network, external, untrusted network, management network, and a local management console, as illustrated in *Figure* 1.

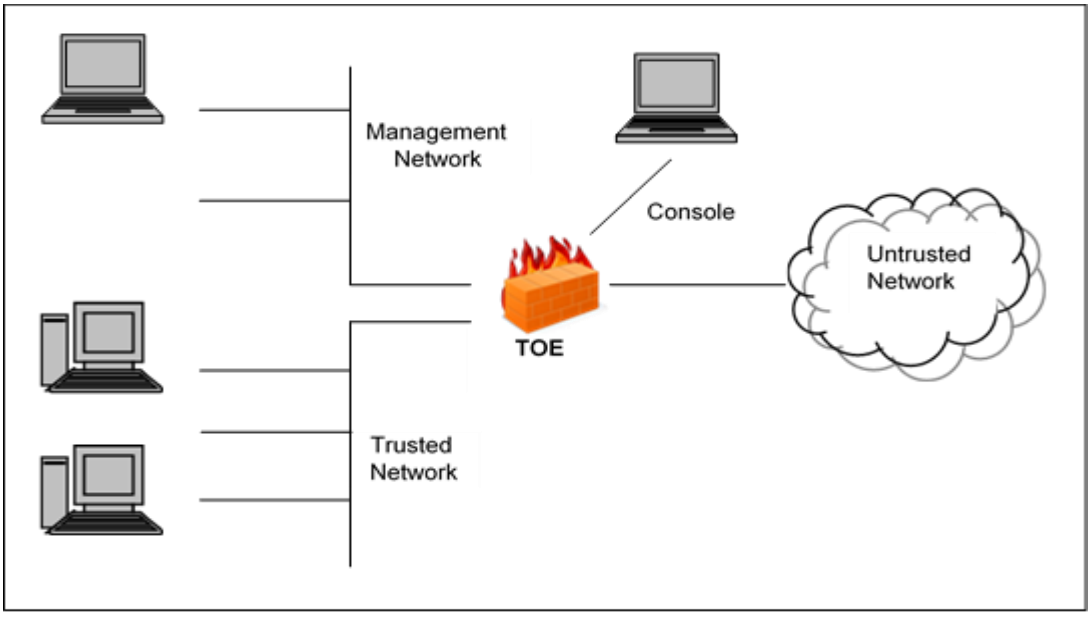

Figure 1, TOE configuration

1.5.3 Physical Scope

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

Binary	Deployment
15.00.00.10-39191	Intel® 64 Architecture (x86_64)
15.00.00.10-39192	Arm® architecture v8

Table 1, Deployment of binaries

Guidance Documentation

The following guides are required reading and are a part of the TOE:

- Clavister cOS Core Administration Guide, Version: 15.00.00
- Clavister cOS Core CLI Reference Guide, Version: 15.00.00
- Clavister cOS Core Log Reference Guide, Version: 15.00.00
- Guidance Documentation - Clavister cOS Core, Version 15.00.00

The guides are available in PDF format to download from Clavister's web site, or as HTML pages directly on Clavister´s web site.

1.5.3.1 Non-TOE Hardware/Software/Firmware

The TOE environment consists of the components listed below in *Table 2*. This table specifies the minimum system requirements for the proper operation of the TOE.

Component	Requirement
Management Console	General purpose computer with serial interface (COM-port)
Management Web interface	General purpose computer with web browser for HTTPS management sessions.
Syslog Server	General purpose computer with Syslog server compliant with RFC 5424 as a minimum.
Virtual deployment	VMware vSphere (ESXi) or KVM

Table 2, Non TOE hardware/software/firmware

VMware minimum specification:

- VMware ESXi version 6.5
- 1024MB guest RAM, 2048MB guest RAM recommended
- 2GB guest storage

KVM minimum specification:

- 1024MB guest RAM, 2048MB guest RAM recommended
- 2GB guest storage

1.5.4 Logical Scope

The logical boundary of the TOE will be broken down into security functions describing the security features of the TSF. The security functional requirements are stated in chapter 6 and the security functions are further described in chapter 7 of this ST.

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

1.5.4.1 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.

1.5.4.2 Cryptographic Support

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

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.

1.5.4.3 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.

1.5.4.4 Identification and Authentication

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

1.5.4.5 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 has 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.

1.5.4.6 Protection of the TOE Security Function (TSF)

The TOE shall perform self-tests 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 occur and are discovered by self-tests or tests of external entities.

1.5.4.7 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.

1.5.5 Physical/Logical Features and Functionality not Included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- 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
- Application Control
- Traffic/Bandwidth Management
- Hardware crypto accelerator

1.5.6 Interfaces

Figure 2 illustrates the TOE interfaces. Management can be performed by authenticated administrators locally, through the Console port, or remote over HTTPS for the Web interface.

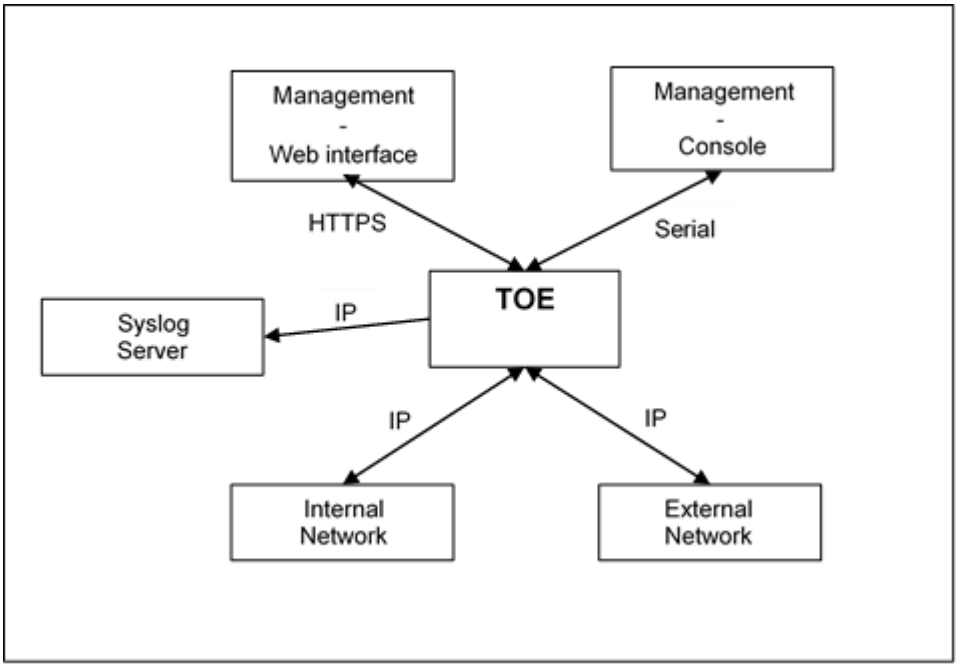

Figure 2, TOE interfaces

1.5.7 Configuration and Modes

1.5.8 Roles

There are three roles with privileges in the TOE:

Admin - Has full management authority with read/write privileges on the TOE configuration. Admin is authenticated through the Console or the remote management interfaces.

Audit - The Audit role is for monitoring purposes only and has read-only privileges. Audit is authenticated through the Console or the remote management interfaces.

Authenticated User - Has privileges to send and receive user data information through the TOE according to rules set up in a Security Functional Policy.

The Admin and Audit roles are collectively called administrators further on in this document.

1.5.9 Evaluated test configuration

The TOE has been tested in the virtual machine environments listed in Table 3 and Table 4.

Developer tests

Binary	Deployment	Virtual Machine Environment
15.00.00.10-39191	Intel® 64 Architecture (x86_64)	VMware ESXi 6.5.0
15.00.00.10-39191	Intel® 64 Architecture (x86_64)	VMware ESXi 6.7.0
15.00.00.10-39191	Intel® 64 Architecture (x86_64)	VMware ESXi 8.0 u2
15.00.00.10-39192	Arm® architecture v8	KVM/QEMU 2.11.1
15.00.00.10-39192	Arm® architecture v8	KVM/QEMU 8.2.2

Table 3, Developer tests

Evaluator tests

Binary	Deployment	Virtual Machine Environment
15.00.00.10-39191	Intel® 64 Architecture (x86_64)	VMware ESXi 7.0 u3

Table 4, Evaluator tests

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target is CC part 2 conformant and CC part 3 conformant to Common Criteria version 3.1, revision 5.

- Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5, CCMB-2017-04-001
- Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-002
- Part 3: Security Assurance Components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003

The guidance from ISO/IEC JTC 1/SC 27 N 2449 *Information technology – Security techniques – Guide for the production of protection profiles and security targets* has been used when developing this Security Target.

2.2 PP Conformance Claims

This Security Target does not claim compliance with any Protection Profile.

2.3 Package Conformance Claims

This Security Target claims conformance to assurance requirement package EAL4 augmented by ALC_FLR.1.

3 Security Problem Definition

3.1 Introduction

The security problem definition described below includes threats, organizational security policies and security usage assumptions.

3.2 Threats

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE must protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

3.2.1 Assets

The following types of Assets are protected by the TOE.

Asset	Description
User Data	User information and IT resources, within the network perimeter of the TOE.
TSF Data	The TOE software, configuration files and other system files.

Table 5, Assets

3.2.2 Threat Agents

The following types of Threat Agents are foreseen.

Threat Agent	Description
Attacker	Persons or external IT entities unauthorized to use the TOE. The Attacker possess: Public knowledge of how the TOE operates and of potential methods of attacking the TOE. Not unlimited resources. No physical access, but unlimited access to the TOE external network interface.
TOE Users	Persons authorized to use the TOE. The TOE Users possess: Extensive knowledge of how the TOE operates. High skill level. Physical access to the TOE. However, TOE Users are not willfully hostile, educated, follows their guidance, but still capable of doing mistakes.

Table 6, Threat agents

3.2.3 Threats

The threats against the TOE are identified according to *Table* 7.

Threat	Assets	Description
T.NETWORK_ACCESS	User Data, TSF Data	An Attacker on an external or internal network 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	User Data, TSF Data	An Attacker on an external or internal network 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. An exhaustion attack can for example be done by sending a large number of packets over a long time period, causing generation of audit records.
T.ADMIN_ACCESS	TSF Data	The Attacker may attempt to gain administrator access to the TOE web management interface through illicit authentication.
T.ADMIN_COMMUNICATION	TSF Data	The Attacker may be able to view, modify, and/or delete security related information sent between a remotely located authorized administrator and the TOE. The Attacker may for example insert himself between the administrator and the TOE and acting as a man in the middle without the administrator's knowledge.
T.BYPASS	User Data, TSF Data	The Attacker on an external or internal network 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	TSF Data	The Attacker on an external or internal network may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.
T.FAILURE	User Data, TSF Data	A component of the TOE or in TOE operational environment may fail during start-up or during operations, or a TOE User may involuntarily cause a compromise or failure in the security functionality and leaving the TOE susceptible to attackers.

Table 7, Threats against the TOE

3.3 Organizational Security Policies

Organizational security policies, OSPs, for the TOE are stated according to *Table 8*.

OSP	Description
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.

Table 8, Organisational Security Policies for the TOE

3.4 Assumptions

Assumptions on the TOE operational environment is made according to *Table 9*.

Assumption	Description
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.

Table 9, Assumptions on the TOE environment

4 Security Objectives

4.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE.
- The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats countered by the TOE environment, organizational security policies or assumptions.

4.2 Security Objectives for the TOE

The following security objectives are defined for the TOE.

Security Objective	Description
O.RESTRICTED_ACCESS	The TOE must mediate the flow of all information and upheld the information flow control policy between the internal and external networks governed by the TOE.
O.AUDIT	The TOE must be able to provide an audit trail of security relevant events. An authorized administrator must be allowed to configure the security relevant events to be audited.
O.AUTHENTICATION	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
O.SECURE_COMMUNICATION	The TOE must protect the confidentiality and integrity and ensure the authenticity of data passed between itself and an authorized administrator.
O.BYPASS_PROTECTION	The TOE must protect itself against attempts by attackers to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to TOE functions, User or TSF data, or to deny access to legitimate users.
O.FAILURE_PROTECTION	The TOE must protect the assets against security breaches caused by accidental failures of the TOE security functions or components in the operational environment upon which the TOE depend.
O.MANAGE	The TOE shall be manageable only by authorized administrators.

Table 10, Security objectives for the TOE

4.3 Security Objectives for the Operational Environment

The following security objectives are defined for the operational environment.

Security Objective	Description
OE.NO_GEN_PURPOSE	The TOE underlying platform must not to provide general purpose computing capabilities.
OE.TRUSTED_ADMIN	Authorized administrators must 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.
OE.PHYSICAL_SECURE	The TOE must be operated in a physically secure environment, i.e., no unauthorized person shall have physical access to the TOE or its underlying platform.
OE.SINGLE_CONNECTION	Information must not flow among the internal and external networks unless it passes through the TOE.
OE.AUDIT_SERVER	An external audit server must be able to receive and store audit events from the TOE.
OE.TIME	The TOE environment must provide the TOE with a reliable time stamp.
OE.VIRTUAL_DEPLOYMENT	Only one instance of the TOE must execute as a guest in the virtual deployment. No other applications must be running as guests in the TOE virtual deployment.

Table 11, Security objectives for the TOE operational environment

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

	T.NETWORK_ACCESS	T.UNDETECTED	T.ADMIN_ACCESS	T.ADMIN_COMMUNICATION	T.BYPASS	T.HALT	T.FAILURE	P.MANAGE	P.ACCOUNTABLE	A.NO_GENERAL_PURPOSE	A.TRUSTED_ADMINISTRATOR	A.PHYSICAL_SECURE	A.SINGLE_CONNECTION	A.AUDIT_SERVER	A.TIME	A.VIRTUAL_DEPLOYMENT
O.RESTRICTED_ACCESS	X															
O.AUDIT		X							X							
O.AUTHENTICATION			X					X								
O.SECURE_COMMUNICATION				X												
O.BYPASS_PROTECTION					X	X										
O.FAILURE_PROTECTION							X									
O.MANAGE								X								
OE.NO_GEN_PURPOSE										X						
OE.TRUSTED_ADMIN											X					
OE.PHYSICAL_SECURE												X				
OE.SINGLE_CONNECTION													X			
OE.AUDIT_SERVER														X		
OE.TIME															X	
OE.VIRTUAL_DEPLOYMENT																X

Table 12, Security objectives coverage

4.4.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption or threat to the environment, that each security objective for the environment that traces back to a threat or an assumption about the environment of use.

Threat/OSP/Assumption	Objective	Rationale
T.NETWORK_ACCESS An Attacker on an external or internal network 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.	O.RESTRICTED_ACCESS The TOE must mediate the flow of all information and upheld the information flow control policy between the internal and external networks governed by the TOE.	By applying the information flow control policy on all traffic flowing between the internal and external networks, the TOE meets the T.NETWORK_ACCESS threat.
T.UNDETECTED An Attacker on an external or internal network 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. An exhaustion attack can for example be done by sending a large number of packets over a long time period, causing generation of audit records.	O.AUDIT The TOE must be able to provide an audit trail of security relevant events. An authorized administrator must be allowed to configure the security relevant events to be audited.	By recording relevant security audit events and allowing an authorized administrator to configure the audit events generated, the T.UNDETECTED threat is diminished.
T.ADMIN_ACCESS The Attacker may attempt to gain administrator access to the TOE web management interface through illicit authentication.	O.AUTHENTICATION The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.	By identification and authentication measures, the T.ADMIN_ACCESS threat is met.
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. The Attacker may for example insert himself between the administrator and the TOE and acting as a man in the middle without the administrator's knowledge.	O.SECURE_COMMUNICATION The TOE must protect the confidentiality and integrity and ensure the authenticity of data passed between itself and an authorized administrator.	A secure channel ensuring confidentiality, integrity and mutual authentication meets the T.ADMIN_COMMUNICATION threat.
T.BYPASS The Attacker on an external or internal network may attempt to bypass, deactivate, or tamper with TOE security functions to cause unauthorized access to TOE	O.BYPASS_PROTECTION The TOE must protect itself against attempts by attackers to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to	TOE self-protection diminishes the threats of T.BYPASS.

Threat/OSP/Assumption	Objective	Rationale
functions, user or TSF data, or to deny access to legitimate users.	TOE functions, User or TSF data, or to deny access to legitimate users.	
T.HALT The Attacker on an external or internal network may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.	O.BYPASS_PROTECTION The TOE must protect itself against attempts by attackers to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to TOE functions, User or TSF data, or to deny access to legitimate users.	TOE self-protection diminishes the threats of T.HALT.
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 cause a compromise or failure in the security functionality and leaving the TOE susceptible to attackers.	O.FAILURE_PROTECTION The TOE must protect the assets against security breaches caused by accidental failures of the TOE security functions or components in the operational environment upon which the TOE depend.	By monitoring the own operation, allowing monitoring of components in the operational environment and acting on failures, the TOE protect the assets against security breaches.
P.MANAGE The TOE shall be manageable only by authorized administrators.	O.AUTHENTICATION The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.	Authorized administrators shall be granted credentials that allow them to manage the TOE after authentication.
	O.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.	O.AUDIT The TOE must be able to provide an audit trail of security relevant events. An authorized administrator must be allowed to configure the security relevant events to be audited.	By record security relevant audit events, e.g. caused by administrators, the P.ACCOUNTABLE OSP is met.

Table 13, Security objectives sufficiency

The security objectives for the environment directly reflects the corresponding assumptions.

5 Extended Components Definition

No extended components are defined.

6 Security Requirements

6.1 Security Functional Policies

The following Information Flow Control Security Functional Policies are defined.

6.1.1 Access Rule SFP

The Access Rule SFP is used as a source (sender) IP anti-spoofing mechanism and applies to all network traffic sent through the TOE over the network interfaces. Subjects are users and IT entities that send and receive user data information through the TOE network interfaces to one another. It may precede other Information Flow Control Policy rules such as the IP Policy SFP.

The Default Access Rule reject network packets not coming from a source that is accessible via the network interface on which the packet arrived. The validation is performed by reverse lookup in the TOE routing tables.

Additional access rules may be defined based on the subject's presumed IP addresses, the destination network interface, and the network address or addresses defined for the source.

The access rules may result in one of the following actions:

- **Drop**: Discard the packets that match the defined fields.
- **Accept**: Accept the packets that match the defined fields for further inspection in the rule set.
- **Expect**: If the source address of the packet matches the IP network address or addresses specified by this rule, the destination network interface is compared to the specified network interface. If the network interface matches, the packet is accepted in the same way as an Accept action. If the network interfaces do not match, the packet is dropped in the same way as a Drop action.

6.1.2 IP Policy SFP

Stateful packet inspection and filtering at the internet and transport layers in the TCP/IP model may be applied. Subjects are users and IT entities that send and receive user data information through the TOE network interfaces to one another.

Filtering can be based on the following attributes:

- Source Network Interface,
- Source Network,
- Destination Network Interface,
- Destination Network,
- Geolocation and
- Authenticated User

The IP Policy may result in one of the following filtering actions:

- **Allow:** The packet is allowed to pass after stateful inspection.

- **Stateless policy:** The packet is allowed to pass, bypassing stateful inspection.
- **Deny:** The packet is discarded.

In addition, dynamic address translation (NAT) and static address translation (SAT) can be performed. A reply message can also be sent after a Deny action.

6.1.3 Authenticated Information Flow SFP

Authentication of user subjects sending user data information through the TOE network interfaces may be required by applying the Authenticated Information Flow SFP.

The authentication rule is based on the user's presumed IP address, its username and password and the source and destination network address ranges.

6.2 Security Functional Requirements

6.2.1 Conventions

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using **bold font style**.
- Completed selection statements are identified using **bold font style**.
- Refinements are identified using **bold font style** for amendments and ~~strikethrough~~ for removed text.
- Iterations are identified by appending a letter to the component identification and an explanatory text in parenthesis, for example, FDP_IFF.1a (Access Rule) for the first iteration and FDP_IFF.1b (IP Policy) for the second iteration.

6.2.2 Summary

The SFRs summarized in *Table* 14 are defined for the TOE.

Component	Description
FAU_GEN.1	Audit data generation
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation

Component	Description
FDP_IFC.2	Complete information flow control (Access Rule)
FDP_IFC.1b	Subset information flow control (IP Policy)
FDP_IFC.1c	Subset information flow control (Authenticated)
FDP_IFF.1a	Simple security attributes (Access Rule)
FDP_IFF.1b	Simple security attributes (IP Policy)
FDP_IFF.1c	Simple security attributes (Authenticated)
FDP_RIP.1	Residual Information Protection
FIA_UAU.1	Timing of authentication (Console)
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1a	Management of security attributes (Access Rule)
FMT_MSA.1b	Management of security attributes (IP Policy)
FMT_MSA.1c	Management of security attributes (Authenticated)
FMT_MSA.3a	Static attribute initialization (Access Rule)
FMT_MSA.3b	Static attribute initialization (IP Policy)
FMT_MTD.1a	Management of TSF data (Admin)
FMT_MTD.1b	Management of TSF data (Audit)
FMT_SMF.1	Specification of management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_TEE.1	Testing of external entities
FPT_TST.1	TSF self-test
FTA_SSL.3a	TSF-initiated termination (User Sessions)
FTA_SSL.3b	TSF-initiated termination (Administrator Sessions)
FTA_TSE.1	TOE session establishment
FTP_ITC.1	Inter-TSF trusted channel

Table 14, Security Functional Requirements

6.2.3 Security Audit – FAU

6.2.3.1 Audit data generation – FAU_GEN.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **The audit events specified in** *Table 15***.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP~~/ST, **the information specified in** *Table 15***.**

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1	---	---
FAU_STG.1	---	---
FAU_STG.3	---	---
FCS_CKM.1	---	---
FCS_CKM.4	---	---
FCS_COP.1	Generic failure event without any specific details	---
FDP_IFC.2 FDP_IFF.1a	Decisions to permit/deny information flows	---
FDP_IFC.1b FDP_IFF.1b	Decisions to permit/deny information flows	---
FDP_IFC.1c FDP_IFF.1c	Decisions to permit/deny information flows	---
FDP_RIP.1	---	---
FIA_UAU.1	All uses of the authentication mechanism	The user identity provided to the TOE
FIA_UAU.2	All uses of the authentication mechanism	The user identity provided to the TOE
FIA_UID.2	Unsuccessful use of the user identification mechanism	The user identity provided to the TOE
FMT_MOF.1	Configuration change	The identity of the administrator changing the configuration
FMT_MSA.1a	Configuration change	The identity of the administrator changing the configuration
FMT_MSA.1b	Configuration change	The identity of the administrator changing the configuration
FMT_MSA.1c	Configuration change	The identity of the administrator changing the configuration
FMT_MSA.3a	Configuration change	The identity of the administrator changing the configuration

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MSA.3b	Configuration change	The identity of the administrator changing the configuration
FMT_MTD.1a	Configuration change	The identity of the administrator changing the configuration
FMT_MTD.1b	Configuration change	The identity of the administrator changing the configuration
FMT_SMF.1	Configuration change	The identity of the administrator changing the configuration
FMT_SMR.1	---	---
FPT_FLS.1	Failure of the TSF	---
FPT_TEE.1	Outcome of the test	Failing component or function
FPT_TST.1	Outcome of the test	Failing component or function
FTA_SSL.3a	Termination on session	---
FTA_SSL.3b	Termination on session	---
FTA_TSE.1	Denied authentication attempt	---
FTP_ITC.1	Failure of the trusted channel functions	Identification of the initiator and target of the failed trusted channel functions

Table 15, Audit events

6.2.3.2 Selective audit – FAU_SEL.1

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) **event type**

b) **exceptions to exclude or include events from the event type rule can be based on the following attributes: Category and ID**

Application note: The event type is specified by the lowest event severity level to be logged:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

Where Info is the default level.

6.2.3.3 Protected audit trail storage – FAU_STG.1

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorized modifications to the stored audit records in the audit trail.

Application note: The audit records are exported to a Syslog server. In addition, logs are also stored locally in the MemLog, using a circular buffer that can be used for troubleshooting.

6.2.3.4 Action in case of possible audit data loss – FAU_STG.3

FAU_STG.3.1 The TSF shall **overwrite the oldest MemLog record** if the audit trail **becomes full**.

6.2.4 Cryptographic Support – FCS

6.2.4.1 Cryptographic key generation – FCS_CKM.1

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes **specified in** *Table 16***,** that meet the following: **the cryptographic standards specified in** *Table 16.*

Primitive	Key lengths	Standard
RSA	2048 bits	FIPS 186-5, Appendix B
AES	128, 256 bits	FIPS 197
3DES	168 bits	FIPS 46-3
ChaCha20	256 bits	RFC8439

Table 16, Key generation

6.2.4.2 Cryptographic key destruction - FCS_CKM.4

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroization** that meets the following: **FIPS PUB 140-2 Cryptographic Key Management Security Level 1**.

Application note: RSA keys within certificates that are part of the configuration are not zeroized.

6.2.4.3 Cryptographic operation - FCS_COP.1

FCS_COP.1.1 The TSF shall perform **the cryptographic operations specified in** *Table 17* in accordance with a specified cryptographic algorithm **the cryptographic algorithms** and cryptographic key sizes **specified in** *Table 17*, that meet the following: **the cryptographic standards specified in** *Table 17*.

Operation	Algorithm and mode/scheme	Key lengths	Standard
TLS v1.3	AES GCM	128, 256 bits	RFC5288
TLS v1.3	ChaCha20 Poly1305	256 bits	RFC8439
TLS v1.2	RSA - RSASSA-PKCS1-v1_5	2048 bits	PKCS #1 v. 2.2
TLS v1.2	AES - CBC	128, 256 bits	FIPS PUB 197 NIST Special Publication 800-38A
TLS v1.2	TDEA - CBC	168 bits	NIST SP 800-67 NIST Special Publication 800-38A
TLS v1.2	SHA256	NA	FIPS 180-5

Table 17, Cryptographic operations

Application note: RSA - RSASSA-PKCS1-v1_5 is used as digital signature scheme for compatibility with TLS v1.2.

Application note: SHA1 is used as a component in the pseudo random number generator Yarrow.

6.2.5 User data protection - FDP

6.2.5.1 Complete information flow control - FDP_IFC.2 (Access Rule)

FDP_IFC.2.1 The TSF shall enforce the **Access Rule SFP** on

a) Subjects: Users and IT entities that send and receive user data information through the TOE network interfaces to one another

b) Information: Any network traffic sent through the TOE from one subject to another

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.2.5.2 Subset information flow control – FDP_IFC.1b (IP Policy)

FDP_IFC.1.1b The TSF shall enforce the **IP Policy SFP** on

a) **Subjects: Users and IT entities that send and receive user data information through the TOE to one another**
b) **Information: Any network traffic sent through the TOE from one subject to another**

6.2.5.3 Subset information flow control – FDP_IFC.1c (Authenticated)

FDP_IFC.1.1c The TSF shall enforce the **Authenticated Information Flow SFP** on

a) **Subjects: Authenticated users that send and receive user data information through the TOE**
b) **Information: Any network traffic sent through the TOE from or to a subject**

6.2.5.4 Simple security attributes – FDP_IFF.1a (Access Rule)

FDP_IFF.1.1a The TSF shall enforce the **Access Rule SFP** based on the following types of subject and information security attributes:

a) **Subject security attributes:**
   – **Presumed IP address**
b) **Information security attributes:**
   – **Interface: The network interface that the packet arrives on**
   – **Network: The IP address or addresses that the source address should belong to**

FDP_IFF.1.2a The TSF shall permit an information flow **for further inspection** between a controlled subject and controlled information via a controlled operation if the following rules hold:

An Accept Access Action is defined, specifying the network interface on which the information is received and one or many IP network addresses including the source presumed IP address.

FDP_IFF.1.3a The TSF shall enforce the **Expect Access Action:**

If the source address of the packet matches the IP network specified by this rule, the destination network interface is compared to the specified network interface. If the network interface matches, the packet is accepted in the same way as an Accept action. If the network interfaces do not match, the packet is dropped in the same way as a Drop action.

FDP_IFF.1.4a The TSF shall explicitly authorize an information flow based on the following rules: **None**.

FDP_IFF.1.5a The TSF shall explicitly deny an information flow based on the following rules:

– **A Drop Access Action is defined, specifying the network interface on which the information is received and one or many network IP addresses including the source presumed IP address**.
– **The TSF shall reject network packets**
– **not coming from a source that is accessible via the network interface on which the packet arrived (Default Access Rule)**
– **with fragmentation faults**
– **with port 0 or address 0.0.0.0**
– **with invalid checksum**
– **with a non-IP protocol**

- **with wrong TCP/UDP/ICMP size**
- **with low (configurable, default 3) or 0 Time To Live, TTL**
- **with a multicast source or multicast mismatch**
- **with directed broadcast**
- **with loopback network**
- **with IP reserved flag set**
- **with IP Options**

6.2.5.5 Simple security attributes – FDP_IFF.1b (IP Policy)

FDP_IFF.1.1b The TSF shall enforce the **IP Policy SFP** based on the following types of subject and information security attributes:

a) Subject security attributes:
- **Source Network Interface**
- **Source Network**
- **Destination Network Interface**
- **Destination Network**
- **Geolocation**

b) Information security attributes:
- **Service**

FDP_IFF.1.2b The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **The information flow matches an IP Policy defined with Allow action and it passes the stateful inspection based on its Service.**
- **The information flow matches a Stateless Policy defined with Allow action.**

FDP_IFF.1.3b The TSF shall enforce the **additional information flow control SFP rules:**

- **Dynamic address translation (NAT),**
- **Static address translation (SAT),**
- **Source address, destination address, and port translations, and**
- **Sending reply message on a Deny action**

shall be performed if specified as a Policy Option.

FDP_IFF.1.4b The TSF shall explicitly authorize an information flow based on the following rules: **None**.

FDP_IFF.1.5b The TSF shall explicitly deny an information flow based on the following rules:

- **The information flow matches an IP Policy defined with Deny actions.**
- **No IP Policy is defined.**

6.2.5.6 Simple security attributes – FDP_IFF.1c (Authenticated)

FDP_IFF.1.1c The TSF shall enforce the **Authenticated Information Flow SFP** based on the following types of subject and information security attributes:

- **a) Subject security attributes:**
  - **– Presumed IP address**
  - **– Username and password**
- **b) Information security attributes:**
  - **– Source Network: The IP address or addresses that the source address should belong to**
  - **– Destination Network: The IP address or addresses that the destination address should belong to**

FDP_IFF.1.2c The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

The User may send information from the Source Network or access resources at the Destination Network after successful authentication to an Authentication Group defined for corresponding network.

FDP_IFF.1.3c The TSF shall enforce the **additional information flow control SFP rules: None.**

FDP_IFF.1.4c The TSF shall explicitly authorize an information flow based on the following rules: **None**.

FDP_IFF.1.5c The TSF shall explicitly deny an information flow based on the following rules: **None.**

6.2.5.7 Subset residual information protection - FDP_RIP.1

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- **– Cryptographic keys and key material**

Application note: RSA keys within certificates that are part of the configuration are not zeroized.

6.2.6 Identification and authentication – FIA

6.2.6.1 Timing of authentication - FIA_UAU.1 (Console)

FIA_UAU.1.1 The TSF shall allow

- **– Login**
- **– Start System - This initiates the start-up of the TOE**
- **– Display Latest Shutdown Message - This shows the last console message shown before system shutdown**

- **Display Latest Crash Dump Message - This shows the latest crash dump message caused by a TOE problem**
- **Enable Console Password/Change Console Password – Only available initially**

On behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.6.2 User authentication before any action - FIA_UAU.2 (Remote)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note: Remote authentication is required for users belonging to the Admin, Audit, or Authenticated Users roles accessing the remote administration or the network interfaces.

6.2.6.3 User identification before any action - FIA_UID.2

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.7 Security management – FMT

6.2.7.1 Management of security functions behavior - FMT_MOF.1

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behavior** of the functions

- **Change the configuration of the TOE**
- **Restart the TOE**

To **Admin**.

6.2.7.2 Management of security attributes - FMT_MSA.1a (Access Rule)

FMT_MSA.1.1a The TSF shall enforce the **Access Rule SFP** to restrict the ability to **query, modify, and delete** the security attributes **Network Interface and Network** to **Admin and Audit (query only)**.

6.2.7.3 Management of security attributes - FMT_MSA.1b (IP Policy)

FMT_MSA.1.1b The TSF shall enforce the **IP Policy SFP** to restrict the ability to **query, modify, and delete** the security attributes **Source Network Interface, Source Network, Destination Network Interface, Destination Network, and Service** to **Admin and Audit (query only)**.

6.2.7.4 Management of security attributes - FMT_MSA.1c (Authenticated)

FMT_MSA.1.1c The TSF shall enforce the **Authenticated Information Flow SFP** to restrict the ability to **query, modify, and delete** the security attributes **Source Network and Destination Network** to **Admin and Audit (query only)**.

6.2.7.5 Static attribute initialization - FMT_MSA.3a (Access Rule)

FMT_MSA.3.1a The TSF shall enforce the **Access Rule SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the **Admin** to specify alternative initial values to override the default values when an object or information is created.

6.2.7.6 Static attribute initialization - FMT_MSA.3b (IP Policy)

FMT_MSA.3.1b The TSF shall enforce the **IP Policy SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b The TSF shall allow ~~**the**~~ **None** to specify alternative initial values to override the default values when an object or information is created.

6.2.7.7 Management of TSF data - FMT_MTD.1a (Admin)

FMT_MTD.1.1a The TSF shall restrict the ability to **query or modify** the

- **TOE and device status information (only query)**
- **TOE configuration (query and modify)**
- **The set of events to be audited (query and modify)**

To **Admin**.

6.2.7.8 Management of TSF data - FMT_MTD.1b (Audit)

FMT_MTD.1.1b The TSF shall restrict the ability to **query** the

- **TOE and device status information**
- **TOE configuration**
- **The set of events to be audited**

to **Audit**.

6.2.7.9 Specification of Management Functions – FMT_SMF.1

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Query TOE and device status information**
- **Apply configuration changes**
- **Select the set of events to be audited**
- **Restart the TOE**

6.2.7.10 Security roles - FMT_SMR.1

FMT_SMR.1.1 The TSF shall maintain the roles**: Admin, Audit, and Authenticated User**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: The Admin role has full administrative read/write privileges. The Audit role is for monitoring purposes only and has read-only privileges. The Authenticated User has privileges to send and receive information through the TOE according to the Authenticated Information Flow SFP.

6.2.8 Protection of the TSF - FPT

6.2.8.1 Failure with preservation of secure state – FPT_FLS.1

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **Failing self-test**
- **Failing test of external entities.**

6.2.8.2 Testing of external entities – FPT_TEE.1

FPT_TEE.1.1 The TSF shall run a suite of tests **at the request of ~~an authorized user~~ the Admin** to check the fulfilment of

- **The sanity of the RAM**
- **The sanity of the disk drive**
- **MAC address collision avoidance on the network interfaces**
- **Network Interface reachability using a ping command (ICMP Echo Request/Reply)**
- **Network Interface throughput**
- **Correct behaviour of traffic with mixed frame sizes over the network interfaces**
- **The correct functioning of the crypto accelerator cards (if applicable)**

Application note: Hardware acceleration cards may not be available on the Virtual Next Generation Firewall (depending on host hardware configuration).

FPT_TEE.1.2 If the test fails, the TSF shall **be able to report to Admin.**

6.2.8.3 TSF testing – FPT_TST.1

FPT_TST.1.1 The TSF shall run a suite of self-tests **during initial start-up**, to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of **the TSF**.

Application note: Image is digitally signed at disc.

6.2.9 TOE access - FTA

6.2.9.1 TSF-initiated termination - FTA_SSL.3a (User Sessions)

FTA_SSL.3.1a The TSF shall terminate an interactive **user** session after a **configurable time based on inactivity and/or the total session lifetime**.

Application note: Authenticated users' sessions may be terminated if a timeout is specified in an Authentication Rule. Separate timeouts exist for inactivity and total session lifetime.

6.2.9.2 TSF-initiated termination - FTA_SSL.3b (Administrator Sessions)

FTA_SSL.3.1b The TSF shall terminate an interactive **Admin or Audit** session after a **configurable time based on inactivity**.

Application note: Administrator sessions will be terminated when the idle timeout is reached. The timeout is configurable and the default value is 900 seconds.

6.2.9.3 TOE session establishment - FTA_TSE.1

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **the following rule: Only one Admin may be authenticated concurrently.**

Application note: Only one Admin may be logged in at the same time, however, the same Admin may start more than one user session, e.g. over different management interfaces. Subsequent users may authenticate as Audit.

6.2.10 Trusted path/channels – FTP

6.2.10.1 Inter-TSF trusted channel – FTP_ITC.1

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **Management Web interface over HTTPS.**

6.3 Security Assurance Requirements

The security assurance requirements according to *Table* 18 have been chosen. They comprise EAL4 augmented by ALC_FLR.1.

Assurance Class	Assurance Component Name	Component
ADV: Development	Security architecture description	ADV_ARC.1
	Complete functional specification	ADV_FSP.4
	Implementation representation of the TSF	ADV_IMP.1
	Basic modular design	ADV_TDS.3
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life-cycle support	Production support, acceptance procedures and automation	ALC_CMC.4
	Problem tracking CM coverage	ALC_CMS.4
	Delivery procedures	ALC_DEL.1
	Basic flaw remediation	ALC_FLR.1
	Developer defined life-cycle model	ALC_LCD.1
	Well-defined development tools	ALC_TAT.1
	Development security	ALC_DVS.1
ASE: Security Target evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
AVA: Vulnerability assessment	Focused vulnerability analysis	AVA_VAN.3

Table 18, Security Assurance Requirements

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Dependencies

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FAU_GEN.1	FPT_STM.1	---	Reliable time stamps are provided by the TOE operational environment according to OE.TIME.
FAU_SEL.1	FAU_GEN.1 FAU_MTD.1	FAU_GEN.1 FAU_MTD.1	
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	
FAU_STG.3	FAU_STG.1	FAU_STG.1	
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1 FCS_CKM.4	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1	
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1a	
FDP_IFC.1b	FDP_IFF.1	FDP_IFF.1b	
FDP_IFC.1c	FDP_IFF.1	FDP_IFF.1c	
FDP_IFF.1a	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 FMT_MSA.3a	FDP_IFC.2 is hierarchical to FDP_IFC.1.
FDP_IFF.1b	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1b FMT_MSA.3b	
FDP_IFF.1c	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1c	No default attribute values exist.
FDP_RIP.1	---	---	
FIA_UAU.1	FIA_UID.1	---	Identification is not required over the Console management interface.
FIA_UAU.2	FIA_UID.1	FIA_UID.2	FIA_UID.2 is hierarchical to FIA_UID.1 and meets therefore the dependency.
FIA_UID.2	---	---	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	
FMT_MSA.1a	[FDP_ACC.1 or FDP_IFC.1] and FMT_SMR.1 and FMT_SMF.1	FDP_IFC.2 and FMT_SMR.1 and FMT_SMF.1	
FMT_MSA.1b	[FDP_ACC.1 or FDP_IFC.1] and FMT_SMR.1 and FMT_SMF.1	FDP_IFC.1b and FMT_SMR.1 and FMT_SMF.1	
FMT_MSA.1c	[FDP_ACC.1 or FDP_IFC.1] and FMT_SMR.1 and FMT_SMF.1	FDP_IFC.1c and FMT_SMR.1 and FMT_SMF.1	
FMT_MSA.3a	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1a and FMT_SMR.1	
FMT_MSA.3b	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1b and FMT_SMR.1	
FMT_MTD.1a	FMT_SMF.1 and FMT_SMR.1	FMT_SMF.1 and FMT_SMR.1	
FMT_MTD.1b	FMT_SMF.1 and FMT_SMR.1	FMT_SMF.1 and FMT_SMR.1	
FMT_SMF.1	---	---	
FMT_SMR.1	FIA_UID.1	FIA_UID.2	FIA_UID.2 is hierarchical to FIA_UID.1 and meets therefore the dependency.
FPT_FLS.1	---	---	
FPT_TEE.1	---	---	
FPT_TST.1	---	---	
FTA_SSL.3a	---	---	
FTA_SSL.3b	---	---	
FTA_TSE.1	---	---	
FTP_ITC.1	---	---	

Table 19, SFR dependencies

6.4.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level EAL4 augmented by ALC_FLR.1. Since all dependencies are met internally by the EAL package only the augmented the assurance components dependencies are analyzed.

Assurance Component	Dependencies	Met
ALC_FLR.1	No dependencies.	---

Table 20, Security Assurance Dependencies Analysis

According to *Table 20* all dependencies are met.

6.4.3 Security Functional Requirements Coverage

	O.RESTRICTED_ACCESS	O.AUDIT	O.AUTHENTICATION	O.SECURE_COMMUNICATION	O.BYPASS_PROTECTION	O.FAILURE_PROTECTION	O.MANAGE
FAU_GEN.1		X					
FAU_SEL.1		X					
FAU_STG.1		X					
FAU_STG.3		X					
FCS_CKM.1				X			
FCS_CKM.4				X			
FCS_COP.1				X			
FDP_IFC.2	X						
FDP_IFC.1b	X						
FDP_IFC.1c	X						
FDP_IFF.1a	X						
FDP_IFF.1b	X						
FDP_IFF.1c	X						
FDP_RIP.1			X	X			
FIA_UAU.1			X				
FIA_UAU.2			X				
FIA_UID.2			X				
FMT_MOF.1							X
FMT_MSA.1a	X						X
FMT_MSA.1b	X						X

	O.RESTRICTED_ACCESS	O.AUDIT	O.AUTHENTICATION	O.SECURE_COMMUNICATION	O.BYPASS_PROTECTION	O.FAILURE_PROTECTION	O.MANAGE
FMT_MSA.1c	X						X
FMT_MSA.3a	X						X
FMT_MSA.3b	X						X
FMT_MTD.1a							X
FMT_MTD.1b							X
FMT_SMF.1							X
FMT_SMR.1							X
FPT_FLS.1					X	X	
FPT_TEE.1						X	
FPT_TST.1					X	X	
FTA_SSL.3a					X		
FTA_SSL.3b					X		
FTA_TSE.1					X		
FTP_ITC.1				X			

Table 21, Security Functional Requirements Coverage

6.4.4 Security Functional Requirements Sufficiency

Objective	SFR	Rationale
O.RESTRICTED_ACCESS The TOE must mediate the flow of all information and upheld the information flow control policy between the internal and external networks governed by the TOE.	FDP_IFC.2 FDP_IFC.1b FDP_IFC.1c FDP_IFF.1a FDP_IFF.1b FDP_IFF.1c FMT_MSA.1a FMT_MSA.1b FMT_MSA.1c FMT_MSA.3a FMT_MSA.3b	An information flow control policy applied at transport layer on all traffic through the TOE (FDP_IFC.2, FDP_IFF.1a) together with information flow control measures at the internet and transport layers (FDP_IFC.1b, FDP_IFF.1b) and information flow control policy for authenticated user data traffic (FDP_IFC.1c, FDP_IFF.1c) ensures restricted access through the TOE. Authority to access and initialize the security attributes that the policies rely upon is only granted to administrators (FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.1c, FMT_MSA.3a, and FMT_MSA.3b).
O.AUDIT The TOE must be able to provide an audit trail of security relevant events. An authorized administrator must be allowed to configure the security relevant events to be audited.	FAU_GEN.1 FAU_SEL.1 FAU_STG.1 FAU_STG.3	Security relevant events shall be generated and stored (FAU_GEN.1). Authorized administrators shall be able to configure the events to be stored (FAU_SEL.1). The audit event trail is protected and the oldest record is overwritten when it becomes full (FAU_STG.1, FAU_STG.3).
O.AUTHENTICATION The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.	FIA_UAU.1 FIA_UAU.2 FIA_UID.2 FDP_RIP.1	Administrators are authenticated when accessing the Console management interface (FIA_UAU.1). Administrators and users are identified and authenticated before any other actions when accessing the Web/CLI interfaces and the network interfaces, respectively (FIA_UID.2, FIA_UAU.2). Secrets are overwritten when no longer used (FDP_RIP.1).
O.SECURE_COMMUNICATION The TOE must protect the confidentiality and integrity and ensure the authenticity of data passed between itself and an authorized administrator.	FCS_CKM.1 FCS_CKM.4 FCS_COP.1 FDP_RIP.1 FTP_ITC.1	A trusted channel has to be established from the Web/CLI interfaces (FTP_ITC.1, FCS_CKM.1, FCS_COP.1). Cryptographic keys and key material have to be destroyed when no longer used (FCS_CKM.4, FDP_RIP.1).
O.BYPASS_PROTECTION The TOE must protect itself against attempts by attackers to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to TOE functions, User or TSF data, or to deny access to legitimate users.	FPT_FLS.1 FPT_TST.1 FTA_SSL.3a FTA_SSL.3b FTA_TSE.1	The TSF integrity has to be verified (FPT_TST.1) to ensure correct security functionality and a secure state applied if the testing fails (FPT_FLS.1). User's and administrator's sessions have to be terminated if no longer legitimate used (FTA_SSL.3a, FTA_SSL.3b). Only one Admin may be accepted at the same time (FTA_TSE.1).
O.FAILURE_PROTECTION The TOE must protect the assets against security breaches caused by accidental failures of the TOE security functions or components in the operational environment upon which the TOE depend.	FPT_FLS.1 FPT_TEE.1 FPT_TST.1	The TSF integrity and environmental components' operation have to be verified (FPT_TST.1, FPT_TEE.1) to ensure correct security functionality and a secure state applied if the testing fails (FPT_FLS.1).

Objective	SFR	Rationale
O.MANAGE The TOE shall be manageable by authorized administrators.	FMT_MOF.1 FMT_MSA.1a FMT_MSA.1b FMT_MSA.1c FMT_MSA.3a, FMT_MSA.3b FMT_MTD.1a FMT_MTD.1b FMT_SMF.1 FMT_SMR.1	The TOE has to be managed by the roles Admin and Audit (FMT_SMR.1, FMT_SMF.1, FMT_MOF.1). Security attributes for the information flow control SFPs have to be initialized and managed by administrators (FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.1c, FMT_MSA.3a, FMT_MSA.3b). TSF data has to be managed by administrators (FMT_MTD.1a, FMT_MTD.1b).

Table 22, Security Functional Requirements Sufficiency

6.4.5 Justification of the Chosen Evaluation Assurance Level

EAL4 is applicable in those circumstances where customers require an enhanced basic level of independently assured security. The assurance level EAL4 augmented with ALC_FLR.1 has been chosen as the minimum requirement for a network device separating an internal network from an external (public) network. It provides a focused vulnerability analysis (in addition to the search of the public domain). The augmentation ALC_FLR.1 (basic flaw remediation) has been made to ensure that basic flaw remediation is in place.

7 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. *Table 23* lists the security functions and their associated SFRs.

TOE Security Function	SFR	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
Trusted Channel	FTP_ITC.1	Inter-TSF trusted channel
	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_IFC.2	Complete information flow control (Access Rule)
	FDP_IFC.1b	Subset information flow control (IP Policy)
	FDP_IFC.1c	Subset information flow control (Authenticated)
	FDP_IFF.1a	Simple security attributes (Access Rule)
	FDP_IFF.1b	Simple security attributes (IP Policy)
	FDP_IFF.1c	Simple security attributes (Authenticated)
	FDP_RIP.1	Residual Information Protection
Identification and Authentication	FIA_UAU.1	Timing of authentication (Console)
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1a	Management of security attributes (Access Rule)
	FMT_MSA.1b	Management of security attributes (IP Policy)
	FMT_MSA.1c	Management of security attributes (Authenticated)
	FMT_MSA.3a	Static attribute initialization (Access Rule)

TOE Security Function	SFR	Description
	FMT_MSA.3b	Static attribute initialization (IP Policy)
	FMT_MTD.1a	Management of TSF data (Admin)
	FMT_MTD.1b	Management of TSF data (Audit)
	FMT_SMF.1	Specification of management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_TEE.1	Testing of external entities
	FPT_TST.1	TSF self-test
TOE Access	FTA_SSL.3a	TSF-initiated termination (User Sessions)
	FTA_SSL.3b	TSF-initiated termination (Administrator Sessions)
	FTA_TSE.1	TOE session establishment

Table 23, TOE Security Functions

7.1.1 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.

7.1.2 Trusted Channel

A trusted channel offering confidentiality, integrity protection and mutual authentication of the end points are established. The TOE provides TLS v1.3 for HTTPS communication to the Management Web interface.

The following cipher suites are allowed for TLS v1.3:

AES_128_GCM_SHA256
AES_256_GCM_SHA384
CHACHA20_POLY1305_SHA256

The following cipher suites are allowed for TLS v1.2:

ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE_RSA_WITH_AES_256_GCM_SHA384

ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
DHE_RSA_WITH_AES_128_GCM_SHA256
DHE_RSA_WITH_AES_256_GCM_SHA384

The library WolfSSL is used for cryptographic operations. Keys and key material will be zeroized when no longer needed.

7.1.3 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 the source and destination network interfaces, source and destination IP networks and service (protocol) entities 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.

7.1.4 Identification and Authentication

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

7.1.5 Management

The TSF recognizes three roles: Admin, Audit and Authenticated User. The Admin and Audit roles have management privileges while the Authenticate User only has 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.

7.1.6 Protection of the TOE Security Function (TSF)

The TOE shall perform self-tests during initial start-up and may test the operation of underlying device entities at the request of the Admin.

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

7.1.7 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.

Appendix A – Abbreviations and Acronyms

Acronym or Abbreviation	Explanation
AES	Advanced Encryption Standard
AV	Anti-Virus
CBC	Cipher-block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
COM-port	Serial interface
cOS	Clavister Operating System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4, IPv6	Internet Protocol version 4, Internet Protocol version 6
IT	Information Technology
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
PKCS	Public-Key Cryptography Standards
PP	Common Criteria Protection Profile
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman

Acronym or Abbreviation	Explanation
RSASSA-PKCS1	RSA Signature Scheme with Appendix PKCS1
SAT	Static Address Translation
SCP	Secure Copy
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TDEA	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

Table 24, Abbreviations and acronyms

Appendix B - Referenced Documents

[1] Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017

[2] Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017

[3] Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017