Array Networks, Inc AppVelocity 10_7

Security Target

Evaluation Assurance Level (EAL): EAL2

Doc No: 2298-001-D102
Version: 1.2
23 October 2024

Array Networks, Inc
1371 McCarthy Blvd.
Milpitas, CA 95035

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview, and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Array Networks AppVelocity 10_7 Security Target
ST Version:	1.2
ST Date:	23 October 2024

1.3 TOE REFERENCE

TOE Identification:	Array Networks AppVelocity 10_7_2_5
TOE Developer:	Array Networks, Inc
TOE Category:	Network and Network Related Devices and Systems
TOE Type:	Software (virtual machine firmware)

1.4 TOE OVERVIEW

The AppVelocity 10_7 is an application delivery controller that helps optimize the interaction between clients and application servers. The application delivery controller is used within enterprise and cloud data centers and it improves the availability, security, and performance.

Leveraging robust distribution algorithms, distributing the workload to multiple processors, health check mechanisms, clustering and failover capabilities, AppVelocity maintains connections, ensures persistence, directs traffic away from failed servers, and intelligently distributes application services across multiple servers for optimized performance and availability. APV can load balance traffic for a wide variety of parameters and protocols at layers 2, 3, 4 and 7, including MAC, IP address, TCP, UDP, port, http, WebSocket and WebSocket Secure.

The TOE supports a vast library of policies that are hard-coded at the kernel level, are configurable with point-and-click simplicity via the Web GUI and can be combined and nested to create advanced customized application traffic management. SSL certificate/key management is also supported and can enable intelligent content management and routing. Computationally intensive key exchange and bulk encryption can also be offloaded.

Management is performed via a GUI (HTTPS) or CLI (console or SSH).

The TOE is a software and is either

- Delivered pre-installed on an appliance (APV x900 or AVX x900). Alternatively, the client may already have APV x900 or AVX x900 system and the TOE (software) can be downloaded and installed on APV x900/AVX x900. (*This configuration is in the scope of evaluation).*
- The software can be downloaded and installed on customer hardware. *(This configuration is not in the scope of evaluation).*

1.4.1 TOE Environment

The following software, hardware and networking components are not included in the evaluation of the TOE but required for operation of the TOE in the evaluated configuration.

Component	Software	Hardware
Host Server (hosting TOE)	KVM (Kernel-based Virtual Machine) server software in CentOS 6.0 or later	APV x900 or AVX x900 hardware
Administrator Workstation	Operating system supporting Chrome 122.0 or later, or Firefox 123.0 or later	General Purpose Computer Hardware
Syslog server	Software supporting RFC5424	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

The Array Networks APV Series hardware, which hosts the APV x900, is a line of high-performance application delivery controllers (ADCs). The table below provides some of the key features for the same:

APV x900 Hardware	Description
Architecture	Based on the SpeedCore architecture, designed for high-throughput and low latency.
Processing Power	Utilizes powerful CPUs and dedicated hardware accelerators for tasks like SSL/TLS encryption/decryption, compression, and deep packet inspection.
Memory	Equipped with 15915132 kbytes memory (RAM) to handle large traffic volumes and complex application scenarios.
Storage	Includes solid-state drives (SSDs) for fast boot times and improved performance.
Networking	Offers a variety of network interfaces, including 1GbE, 6GbE and 10GbE options, to support high-speed connections.
Physical form	Available in rack-mountable form factors for easy deployment in data centers.

The Array Networks AVX Series is a line of hardware appliances designed to host and run multiple instances of virtualized application delivery controllers (vAPVs). The table below provides some of the key features for the same:

AVX x900 Hardware	Description
Architecture	Unique hybrid hardware and software architecture that utilizes advanced SR-IOV, DPDK, NUMA boundary and CPU pinning optimizations to guarantee performance and scale.
Processing Power	Utilizes powerful CPUs and dedicated hardware accelerators for tasks like SSL/TLS encryption/decryption, compression, and deep packet inspection.
vAPV Management	• Multi-tenancy: Allows for the creation and management of multiple isolated vAPV instances on a single hardware appliance. Six platforms, ranging from 35Gbps with support for up to 8 VAs, to 160Gbps with support for up to 32 VAs • Resource Isolation: Provides dedicated resources (CPU, memory, network) to each vAPV instance, ensuring performance and security. • Scalability: Offers the ability to scale the number of vAPV instances as needed to meet changing traffic demands. • Flexibility: Enables the deployment of different vAPV configurations and features based on specific requirements.
Memory	Equipped with 3879188 kbytes memory (RAM) to handle large traffic volumes and complex application scenarios.
Storage	Includes solid-state drives (SSDs) for fast boot times and improved performance.
Networking	Offers a variety of network interfaces, including 1GbE and 10GbE options, to support high-speed connections.
Physical form	Available in rack-mountable form factors for easy deployment in data centers.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is a software running in the environment specified in Table 1 as summarized in the following table.

TOE Component	Details
AppVelocity 10_7 (Rel_APV_10_7_2_5)	TOE (AppVelocity 10_7 (Rel_APV_10_7_2_5)) running on KVM in CentOS 6.0 or later on the host server identified in Table 1

Table 2 - TOE Components

A typical TOE deployment is shown in the figure below.

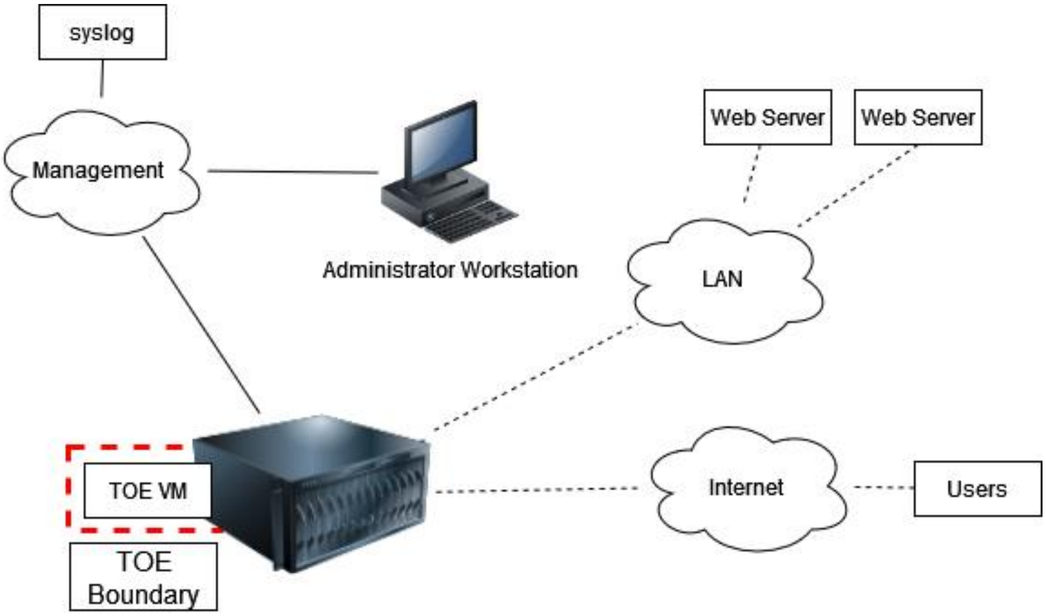

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE is a software

- Delivered pre-installed on an appliance (APV x900 or AVX x900) via commercial courier.
- Alternatively, the client may already have APV x900 or AVX x900 system and the TOE (software) can be downloaded and installed on APV x900/AVX x900.

Customers are provided with an account and can download the software (in a zip file) and the guidance documentation (pdf format).

1.5.1.2 TOE Guidance

The guidance documentation can be found by searching for the document on the Array Networks support site which has the current version of each document. The TOE includes the following documentation in pdf format:

- AVX5900 Quick Installation Guide, March 14, 2024
- AVX7900/9900 Quick Installation Guide, March 14, 2024

- APV5900 Quick Installation Guide, March 14, 2024
- APV7900/9900 Quick Installation Guide, March 14, 2024
- ArrayOS APV 10.7 User Guide, April 22, 2024
- ArrayOS AVX 2.7 User Guide
- ArrayOS APV 10.7 CLI Handbook, May 14, 2024
- AppVelocity vAPV Administration Guide, September 10, 2020
- Array Networks AppVelocity 10_7 Common Criteria Guidance Supplement, v0.7, 23 October 2024

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6.

Functional Class	Description
Identification and Authentication (FIA)	Administrators must identify and authenticate prior to TOE access. The TSF enforces a failure limit, password rules, and passwords are not revealed during authentication.
Protection of the TSF (FPT)	Reliable timestamps are provided in support of audit record creation and session timeout enforcement. Audit records help ensure that administrator actions related to TSF management are recorded thereby helping to ensure the integrity of TSF data. Changes to the system time itself are audited to provide some protection against changes that may impact TSF functions. Session timeout protects the TSF by ensuring that unattended administrator sessions can't be used.
Security Audit (FAU)	Audit entries are generated for security related events and the records also include the user or subject identity. The audit logs are protected from unauthorized modification and deletion and may be reviewed by authorized administrators. Timestamp information is provided to support auditing. An audit log storage duration is also

Functional Class	Description
	enforced.
Security Management (FMT)	The TOE provides management capabilities via a web based GUI (HTTPS or CLI (SSH)). Management functions allow the administrators to configure system and network settings, configure users and roles, and perform other TOE functions.
Trusted Path/Channel (FTP)	The communications link between the TOE and its remote administrators and the link with the syslog server is protected using HTTPS (TLS v1.2).

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- RESTful API
- SNMP
- XML RPC
- NTP

1.5.4 Functionality Supported but Not Evaluated

The following features are supported but have not been evaluated:

- WebWall web application firewall and DDos protection
- SAMPL SP for web single sign-on (SSO)
- Software SSL offloading
- SSL traffic interception and decryption for third party security appliances
- Integration with VMWare vRealize Orchestrator, Microsoft system Center, and OpenStack load balancing as a service (LBaaS)
- Link load balancing (LLb) and global server load balancing (GSLB)
- Traffic shaping and QoS
- N-1 clustering

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to CC:2022 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2022-11-001, CC:2022, Revision 1, November 2022
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2022-11-002, CC:2022, Revision 1, November 2022
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2022-11-003, CC:2022, Revision 1, November 2022

The TOE is CC Part 2 conformant and CC Part 3 conformant. The Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022 has been used for evaluation.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE to any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 (EAL2) package according to:

- Common Criteria for Information Technology Security Evaluation, Part 5: Pre-Defined Packages of Security Requirements; CCMB-2022-11-005, CC:2022, Revision 1, November 2022

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 - Threats lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attackers is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.
T.UNAUTH	An unauthorized user may gain access to TOE functionally that is restricted to authorized users.

Table 4 - Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 - Organizational Security Policies lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.MANAGE	The TOE shall be managed only by authorized users.
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.

Table 5 - Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6 – Assumptions.

Assumption	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative users.
O.TIME	The TOE must provide reliable timestamps.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

Objective	A.LOCATE	A.MANAGE	A.NOEVIL	P.ACCOUNT	P.MANAGE	T.ACCOUNT	T.UNAUTH	T.UNDETECT
O.ADMIN				X	X	X	X	
O.AUDIT						X		X
OE.PERSON		X	X		X			
OE.PHYSICAL	X						X	

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat	Objective	Rationale
T.ACCOUNT: An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.	O.ADMIN	O.ADMIN contributes to the mitigation of this threat by ensuring that only authorized users have access to TSF data.
T.ACCOUNT: An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.	O.AUDIT	O.AUDIT ensures that there are audit records that may be used to provide evidence of inappropriate activity.
T.UNAUTH: An unauthorized user may gain access to TOE functionally that is restricted	O.ADMIN	O.ADMIN contributes to supporting this threat by ensuring that the TOE restricts

Threat	Objective	Rationale
to authorized users.		specific functionality to administrators.
T.UNAUTH: An unauthorized user may gain access to TOE functionally that is restricted to authorized users.	OE.PHYSICAL	OE.PHYSICAL supports this objective by ensuring the physical protection is provided for the TOE.
T.UNDETECT: Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	O.AUDIT	O.AUDIT contributes to the mitigation of this threat by ensuring that audit records are available.

Table 10 - Rational for Objectives Related to Threats

4.3.2 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Policy	Objective	Rationale
A.LOCATE: The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	OE.PHYSICAL	OE.PHYSICAL supports this assumption by ensuring that authorized administrators provide for physical protection of the TOE.
A.MANAGE: There are one or more competent individuals assigned to manage the TOE.	OE.PERSON	OE.PERSON supports this assumption by ensuring that the TOE administrators have been specifically chosen to be careful, attentive, and non-hostile.
A.NOEVIL: The authorized administrators are not careless, willfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	OE.PERSON	OE.PERSON supports this assumption by ensuring that the TOE administrators have been specifically chosen to be careful, attentive, and non-hostile.

Table 11 - Rational for Objectives Related to Assumptions

4.3.3 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE.

Assumption	Objective	Rationale
P.ACCOUNT: The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ADMIN	O.ADMIN contributes to the enforcement of this policy by ensuring that all administrative users are identified and authenticated.
P.MANAGE: The TOE shall be managed only by authorized users.	O.ADMIN	O.ADMIN supports this policy by ensuring that only authorized users have access to TSF data.
P.MANAGE: The TOE shall be managed only by authorized users.	OE.PERSON	OE.PERSON supports this policy by ensuring that administrators are carefully selected and trained.

Table 12 - Rational for Objectives Related to OSPs

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 13.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Audit data storage location
	FAU_STG.2	Protected audit data storage
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets

Class	Identifier	Name
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
Trusted Path/Channel (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 13 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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 events listed in Table 14 - Auditable Events].

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;

~~b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*none*].~~

SFR	Auditable Event
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded
FIA_UAU.2	Unsuccessful authentication attempts are audited for the GUI.
FMT_SMR.1	An audit record is created when a user's role assignment is changed.

SFR	Auditable Event
FPT_STM.1	Changes to the time.
FTP_ITC.1	Initiation, termination, and failure of the trusted channel including identifying the initiator and target.
FTP_TRP.1	Initiation, termination, and failure of the trusted path.

Table 14 - Auditable Events

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of Identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*administrators*] with the capability to read [*all records*] from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_STG.1 Audit data storage location

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.1.1 The TSF shall be able to store generated audit data on the [TOE itself, transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC].

6.2.1.5 FAU_STG.2 Protected audit data storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit data in the audit trail.

6.2.2 Identification and Authentication (FIA)

6.2.2.1 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [*Web GUI and CLI authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block password based logins for 5 minutes*].

6.2.2.2 FIA_SOS.1 Verification of Secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*the following rules:*

a) password length must be in the range of 8 to 116 characters, and it must be a combination of the three of the following: uppercase, lowercase, numeric and special characters; and
b) the password cannot contain the username, which is case-insensitive].

6.2.2.3 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

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.

6.2.2.4 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.

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.

6.2.3 Security Management (FMT)

6.2.3.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions identified* in Table 15 - Management Activities.

SFR	Management Activity
FIA_UAU.2	Administrators are responsible for maintaining the administrative users.
FIA_UID.2	Administrators are responsible for maintaining the administrative users.
FMT_SMR.1	An administrator can configure administrator users and assign them to a role.
FPT_STM.1	An administrator can set the system time.
FTP_ITC.1	Administrators can configure the syslog connection.

Table 15 - Management Activities

6.2.3.2 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*role_administrator, role_operator, role_auditor*].

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

6.2.4 Protection of the TSF (FPT)

6.2.4.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.5 Trusted Path/Channels (FTP)

6.2.5.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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 [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*remote syslog*].

6.2.5.2 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*administration of the TOE*]].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance as defined in the CC Part 3. The assurance requirements are summarized Table 16.

Assurance Class	Component Identifier	Component Name
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirement

Assurance Class	Component Identifier	Component Name
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 16 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following table provides the mapping between the SFRs and Security Objectives.

SFR	O.ADMIN	O.AUDIT	O.TIME
FAU_GEN.1		X	
FAU_GEN.2		X	
FAU_SAR.1		X	
FAU_STG.1		X	
FAU_STG.2		X	
FIA_AFL.1	X		
FIA_SOS.1	X		
FIA_UAU.2	X		
FIA_UID.2	X		
FMT_SMF.1	X		
FMT_SMR.1	X		
FPT_STM.1		X	X

SFR	O.ADMIN	O.AUDIT	O.TIME
FTP_ITC.1	X		
FTP_TRP.1	X		

Table 17 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following table provides the rationale that traces each SFR back to the Security Objectives for the TOE.

Objective	SFR	SFR Description	Rationale
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FIA_AFL.1	Authentication failure handling	The TOE enforces a failure limit on WEB GUI and CLI login attempts. After 5 unsuccessful attempts logins for that user are blocked for a 5 minutes.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FIA_SOS.1	Verification of secrets	The TOE enforces rules on administrator passwords.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management	FIA_UAU.2	User authentication before any action	Authentication is required before any TSF mediated actions can be performed.

Objective	SFR	SFR Description	Rationale
of the security of the TOE, and restrict these functions and facilities from unauthorized use.			
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FIA_UID.2	User identification before any action	Identification is required before any TSF mediated actions can be performed.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_SMF.1	Specification of Management Functions	FMT_SMF.1 supports this objective by identifying the management functions authorized administrators are able to perform.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from	FMT_SMR.1	Security roles	FMT_SMR.1 meets this objective by supporting a list of authorized roles for the TOE.

Objective	SFR	SFR Description	Rationale
unauthorized use.			
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FTP_ITC.1	Inter-TSF trusted channel	FTP_ITC.1 helps meet this objective by providing a trusted communication channel using a secure protocol that protects data in transit from disclosure.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FTP_TRP.1	Trusted path	The TOE uses a trusted path for administrator sessions which helps to prevent unauthorized access. This includes all methods of access encompassing the Web GUI and CLI.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative users.	FAU_GEN.1	Audit data generation	This SFR outlines what data must be included in audit records and what events must be audited.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events.	FAU_GEN.2	User identity association	FAU_GEN.2 supports this objective by associating a user identity with each auditable event

Objective	SFR	SFR Description	Rationale
The audit records must be viewable by administrative users.			generated.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative users.	FAU_SAR.1	Audit review	FAU_SAR.1 provides the means to review audit records.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative users.	FAU_STG.1	Audit data storage location	The TOE stores audit records locally.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative users.	FAU_STG.2	Protected audit data storage	The TOE does not have provision for deleting audit records.
O.AUDIT: The TOE must record audit records security relevant administrative actions and events. The audit records must be viewable by administrative	FPT_STM.1	Reliable time stamps	The TSF provides time stamps for the audit records.

Objective	SFR	SFR Description	Rationale
users.			
O.TIME: The TOE must provide reliable timestamps.	FPT_STM.1	Reliable time stamps	This SFR meets the objective by providing reliable timestamps for use in audit records.

Table 18 - Security Objectives and SFRs

6.4.3 Dependency Rationale

Table 19 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	
FIA_SOS.1	None	N/A	
FAU_STG.1	FAU_GEN.1	✓	
	FTP_ITC.1	✓	
FAU_STG.2	None	N/A	
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has

SFR	Dependency	Dependency Satisfied	Rationale
			been satisfied.
FIA_UID.2	None	N/A	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 19 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 5. EAL2 was chosen for competitive reasons. This EAL level is consistent with the threat environment defined in section 3.1.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

The TOE audits the events listed in Table 14 - Auditable Events.

Auditing must be enabled by an administrator during initial configuration and audit log entries are created when the function is enabled or disabled. In the evaluated configuration auditing must be left enabled. Once auditing has been enabled the 'Start up and shutdown of the audit function' audit record is captured as start up and shutdown messages for the TOE itself.

Logs can be read by all administrative users using the Web GUI or CLI. The logs are presented in human readable format. The time shown to the Web GUI user will be adjusted according to their local settings.

The audit records contain the following fields:

- Date and time of the log entry
- Type of event
- Subject identity (user when applicable)
- Name of the command

Audit logs can only be deleted by a role_administrator user. The audit logs cannot be modified. All audit records generated on the TOE are sent to a remote audit server over the TLS protected trusted channel. The audit records that are stored locally and those sent to the remote audit server are identical in content and format. Locally generated audit records are sent to the remote audit server as soon as they are generated. If the trusted channel is not operational, then audit records will not be sent to the remote audit server; however, they will still be locally stored. The TSF does not queue up audit records that were not sent to the remote audit server for transmitting upon re-establishment of the trusted channel.

TOE Security Functional Requirements addressed: FAU_STG.1, FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.2

7.2 IDENTIFICATION AND AUTHENTICATION

The identification and authentication function ensures that a user requesting a TOE administrative function through the Web GUI has provided their username/password and is authorized to access the TOE.

The Web GUI interface is protected by TLS v1.2. Insecure http connection attempts are redirected to https. The CLI is available either from a local console or on the management interface where the connection is protected by SSHv2. The TSF requires that each administrative user be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user. When a user submits a username/password combination, the TSF attempts to authenticate the user. If the username/password combination match an authorized administrator's credentials, the user is granted access to web-based graphical user interface or command line interface. Dots are echoed by the Web GUI or CLI when the password is being entered.

When a password is set or changed the TSF ensures that it meets the following rules:

- password length must be in the range of 8 to 116 characters, and it must be a combination of the three of the following: uppercase, lowercase, numeric and special characters
- the password cannot contain the username (case-insensitive)

If a Web GUI or CLI user enters an incorrect password 5 times, the offending user account will be prevented from successfully authenticating for 5 minutes. Failed authentication attempts are tracked using a monotonically incrementing counter. This counter is reset upon successful authentication of the offending account or after the fixed 5 minute lockout time for the account has elapsed. Each valid account attempting to authenticate remotely gets its own counter.

TOE Security Functional Requirements addressed:FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2

7.3 SECURITY MANAGEMENT

The evaluated configuration requires the enabling of the admin mode separation function. When this function is enabled the system provides three predefined roles and three administrative accounts along with their corresponding rules.

The three administrative accounts are administrator, operator and auditor. These accounts are automatically assigned the appropriate roles which are role_administrator, role_operator, and role_auditor. An administrator with the role_administrator role can maintain and configure other administrator users. The user roles can be assigned manually by the administrator to other existing or newly created users.

Privileged operations of the three administrative accounts are as follows:

- Administrator: can change the passwords of all users except other administrators and can execute all CLI except log operations.
- Operator: can change only its own password and can execute all CLI except log, role and user operations.
- Auditor: can change only its own password and can execute "show" CLI and part of the log operations

An administrator with the role_administrator role can set the system time and configure the syslog connection.

TOE Security Functional Requirements addressed:FMT_SMF.1, FMT_SMR.1

7.4 PROTECTION OF THE TSF

The TOE uses the system clock. The system clock is set to UTC and this is used for the following:

- audit logs.
- Web GUI and CLI session timeouts.

TOE Security Functional Requirements addressed: FPT_STM.1

7.5 TRUSTED PATH / CHANNELS

The TOE (when serving as a client) uses OpenSSL and syslog-ng to communicate with a remote audit log server (syslog) via TLS v1.2. All the audit records are securely transmitted to the configured remote syslog server.

The TOE (when serving as a server) uses TLS v1.2 for communications via the Web GUI and SSHv2 for the command line interface (CLI). The communication path is initiated by the remote user.

The TOE uses SSL thus incorporating cryptography using RSA and ECC algorithms. Furthermore, the use of digital certificates and signatures serves as an authentication mechanism for providing a trusted path to the management interfaces.

TOE Security Functional Requirements addressed:FTP_ITC.1, FTP_TRP.1

8 ACRONYMS

The following acronyms are used in this ST:

	Definition
AD	Active Directory
API	Application Programming Interface
CLI	Command Line Interface
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
KVM	Kernel-based Virtual Machine
NTP	Network Time Protocol
REST	Representational State Transfer
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSO	Single Sign On
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
XML	Extensible Markup Language

Table 20 – Acronyms