Fortinet®
FortiManager® 5.6.6

Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 2051-000-D102
Version: 1.13
21 October 2019

Fortinet, Incorporated
899 Kifer Road
Sunnyvale, California, USA
94086

Prepared by:
EWA-Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

ewa canada | An Intertek Company

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:	Fortinet® FortiManager® 5.6.6 Security Target
ST Version:	1.13
ST Date:	21 October 2019

1.3 TOE REFERENCE

TOE Identification:	Fortinet FortiManager family: FortiManager-400E FortiManager-1000D FortiManager-2000E FortiManager-3000F FortiManager-3900E FortiManager-4000D FortiManager-4000E
TOE Version:	5.6.6 build7352 190510 (EAL4+)[1]
TOE Developer:	Fortinet, Inc
TOE Type:	Network Management Device Firmware

1.4 TOE OVERVIEW

The TOE is Fortinet® FortiManager® 5.6.6 running in stand-alone 'FIPS/CC mode'. The TOE provides network management to one or more Fortinet network security devices. Authorized administrators are able to configure and manage devices, using functions that include verification and update of firmware and license information. Administrators can create and modify policies and objects and push them to the devices. The TOE is able to retrieve up-to-date antivirus and intrusion prevention signatures from Fortinet's FortiGuard service to push to the managed devices.

The TOE is capable of grouping devices into administrative domains (ADOMs), which simplifies the application of policies, distribution of content security and firmware updates for large implementations. ADOMs are implemented in the evaluated configuration.

The TOE has extensive logging capabilities which include the logging of administrative actions and logging of use of the trusted cryptographic channels.

The TOE is a software only TOE. It is supported by the FortiManager appliance hardware, which is in the operational environment.

The Fortinet® and FortiManager® trademarks are owned by Fortinet, Inc. and are used in accordance with Fortinet® policy.

[1] The TOE is referred to as 'Fortinet® FortiManager® 5.6.6' or 'the TOE' throughout the ST. These terms should be considered to be synonymous with the TOE Reference.

1.4.1 Required Non-TOE Hardware/Firmware/Software

The following components are required for operation of the TOE in the CC-evaluated configuration. These items are not part of the TOE, but are necessary for its proper operation.

Non-TOE Component	Hardware/Software Requirements
FortiManager Appliance	Any of the following hardware models may be used with the TOE: • FMG-400E • FMG-1000D • FMG-2000E • FMG-3000F • FMG-3900E • FMG-4000D • FMG-4000E
Management Workstation	General purpose computing platform that supports the following: • Internet Explorer 11 • Transport Layer Security (TLS) 1.1 or 1.2
Fortinet Entropy Token	Fortinet Entropy Token hardware
Managed Devices	Fortinet FortiGate and FortiAnalyzer devices

Table 1 – Non-TOE Hardware/Firmware/Software

1.4.2 Hardware Guidance

All guidance is publicly available at http://docs.fortinet.com. The following guidance is part of the operational environment:

- FortiManager 400E QuickStart Guide, August 1, 2017 02-540-293606-20170801
- FortiManager 1000D QuickStart Guide, July 31, 2017 02-504-215127-20170731
- FortiManager 2000E QuickStart Guide, July 31, 2017 02-540-294824-20170731
- FortiManager 3000F QuickStart Guide, July 31, 2017 02-540-293672-20170731
- FortiManager 3900E QuickStart Guide, August 1, 2017 02-507-249407-20170801
- FortiManager 4000D QuickStart Guide, August 1, 2017 02-505-194824-20170801

- FortiManager 4000E QuickStart Guide, August 1, 2017 02-505-228134-20170801

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of Fortinet® FortiManager® 5.6.6.

Figure 1 shows the TOE in the evaluated configuration.

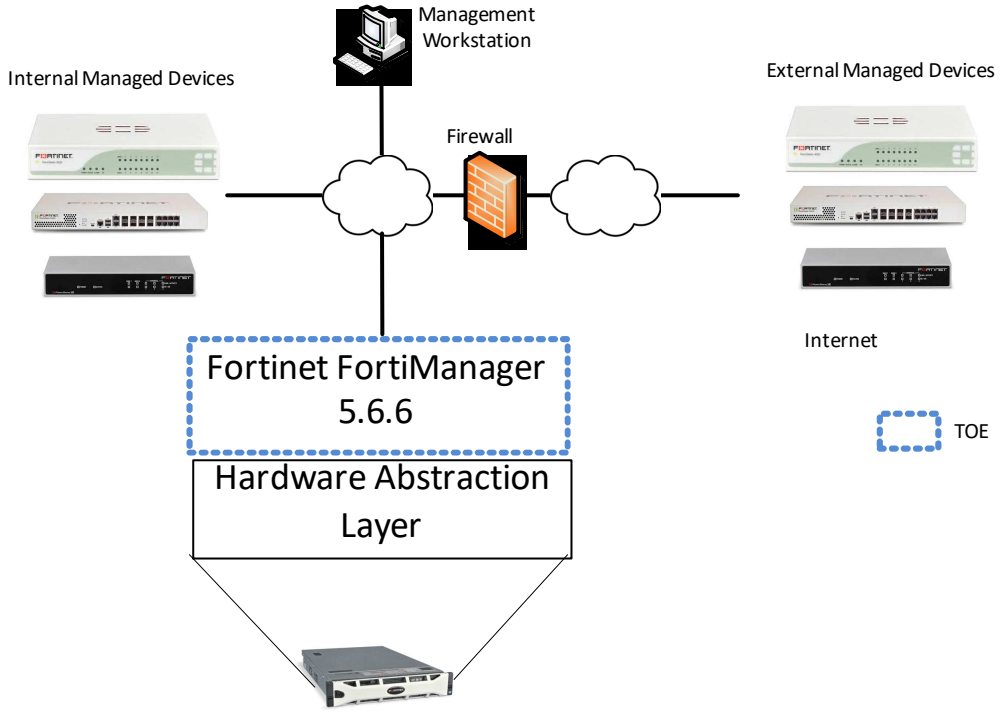

Figure 1 – FortiManager Deployment Diagram

The TOE may be described as the firmware instances found in Table 2.

Fortinet® FortiManager® 5.6.6 build 7352 190510 (EAL4+)
FMG-400E-v5.6.6-build7352-FORTINET.out
FMG-1000D-v5.6.6-build7352-FORTINET.out
FMG-2000E-v5.6.6-build7352-FORTINET.out
FMG-3000F-v5.6.6-build7352-FORTINET.out
FMG-3900E-v5.6.6-build7352-FORTINET.out

Fortinet® FortiManager® 5.6.6 build 7352 190510 (EAL4+)
FMG-4000D-v5.6.6-build7352-FORTINET.out
FMG-4000E-v5.6.6-build7352-FORTINET.out

Table 2 – TOE Firmware Description

The firmware is delivered to the end user via a web download from the Fortinet Customer Service & Support web site.

1.5.1.1 TOE Guidance

All guidance is publicly available at https://docs.fortinet.com. The following guidance documentation is an integral part of the TOE:

- FortiManager 5.6.6 Administration Guide, November 22, 2018, 02-566-400706-20181122 (available in Portable Document Format (pdf) as FortiManager-5.6.6-Administration-Guide.pdf)
- FortiManager 5.6.6 CLI Reference, November 15, 2018, 02-566-400067-20181115 (available in pdf as FortiManager 5.6.6 CLI Reference.pdf)
- FortiManager & FortiAnalyzer 5.6.6 Event Log Reference, October 02, 2018, 05-566-438656-20181002 (available in pdf as FMG-FAZ 5.6.6 Event Log Reference.pdf)
- FortiManager 5.6.6 Common Criteria EAL4 Technote, June 12, 2019, 02-566-486071-20190604 (available in pdf as FMG 5.6.6 CC EAL4 Technote.pdf)

It should be noted that the TOE is limited to the Fortinet® FortiManager® 5.6.6 firmware. This firmware is delivered and operated on specific devices, which are part of the operational environment and are listed in Section 1.4.1.

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	The TOE generates audit records for security relevant events. An Administrator[2] may view the contents of the audit records; however, this functionality is restricted to those users authorized to view the records.

[2] An Administrator with any pre-configured profile or with a custom profile with similar permissions. Profiles are discussed in Section 7.5.

Functional Classes	Description
Cryptographic Support	The TOE provides key generation, key destruction and cryptographic operation functions supported by Cryptographic Algorithm Validation Program (CAVP)-validated algorithms.
User Data Protection	The TOE controls access to the security data required to perform security management functions including management of devices.
Identification and Authentication	All TOE administrative users must be identified and authenticated. Users are locked out after a number of unsuccessful authentication attempts. Administrator passwords must meet the configured length and composition requirements.
Security Management	The TOE provides administrative interfaces that permit users with administrative profiles to configure and manage the TOE. This includes management of the attributes used in the Administrative Access Control Security Functional Policy (SFP), and device management. Administrator roles are provided with differing privileges.
Protection of the TSF	Confidentiality is provided when policy information is transferred from the TOE to the managed devices. Reliable time stamps are provided in support of the audit function.
Trusted Path/Channel	The TOE requires an encrypted trusted channel for communication between the TOE and the managed devices in support of the transfer of policy information. A trusted path communication is required in support of remote administration.

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- FortiGuard update options. Automated updates from FortiGuard were not included in the evaluated configuration. Only manual updates are supported. Manual updates may be made over an air gapped connection using a Universal Serial Bus (USB) token, or over a protected connection. Automated updates that do not require administrative action were not evaluated.
- Application Programming Interfaces (APIs). The following APIs are not included in the evaluation:

- JavaScript Object Notation (JSON)
- eXtensible Markup Language (XML)
- Software Development Kit (SDK)

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CLAIM

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

2.3 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 4 augmented with ALC_FLR.3 Systematic Flaw Remediation.

2.4 CONFORMANCE RATIONALE

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

The threats discussed below are addressed by the TOE. Potential threat agents are persons or external IT entities not authorized to use the TOE itself. The threat agents are assumed to have an enhanced-basic attack potential and are assumed to have access to all publicly available information about the TOE and potential methods of attacking the TOE, a proficient level of expertise, standard equipment and minimal time to attack the TOE without detection. It is expected that the FortiManager units will be protected to the extent necessary to ensure that they remain connected to the networks they protect, and minimize the window of opportunity available for attack.

Threat	Threat Description
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not created and reviewed, thus allowing an attacker to escape detection.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE to access stored data and use security functions provided by the TOE.
T.PRIVIL	An unauthorized person or external IT entity may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE, or between the TOE and managed devices.

Table 4 – Security Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 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.ACCACT	Users of the TOE shall be accountable for their actions.
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, malicious activity, or unintended access must be collected.

OSP	Description
P.MANAGE	The TOE shall be manageable only by authorized administrators.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

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

Assumptions	Description
A.DELIVER	The TOE and all supporting hardware devices are delivered, installed, managed and operated in a manner which is consistent with IT Security best practices.
A.LOCATE	The TOE will be located within controlled access facilities and protected from unauthorized physical modification.
A.NOEVIL	Authorized administrators are properly trained, not malicious, and follow all administrative guidance. Authorized administrators are trusted to administer the TOE correctly.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

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.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide user accountability for authorized administrator use of security functions by providing a means to record and view a readable audit trail of security-related events, with accurate dates and times.
O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, or between the TOE and managed devices using cryptographic functions.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
O.PROTCT	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
O.TIME	The TOE shall provide reliable time stamps.

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.ADMIN	Those responsible for the TOE must ensure that the TOE and the supporting hardware devices are delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of trusted, authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators follow all administrator guidance and are not malicious.
OE.PHYCAL	Those responsible for the TOE must ensure that the TOE is 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.

	T.AUDACC	T.NOAUTH	T.PRIVIL	T.PROCOM	P.ACCACT	P.DETECT	P.MANAGE	A.DELIVER	A.LOCATE	A.NOEVIL	A.MANAGE
O.ACCESS			X				X				
O.ADMIN	X		X				X				
O.AUDIT	X				X	X					
O.ENCRYP				X							
O.IDAUTH		X	X		X		X				
O.PROTCT		X	X				X				
O.TIME	X				X	X					
OE.ADMIN							X	X		X	X
OE.PHYCAL								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: T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not created and reviewed, thus allowing an attacker to escape detection.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.AUDIT	The TOE must provide user accountability for authorized administrator use of security functions by providing a means to record and view a readable audit trail of security-related events, with accurate dates and times.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	O.ADMIN provides for security management functionality, including the functionality for reviewing the audit trail. O.AUDIT requires that authorized administrators are accountable for the use of security functions related to audit. The reliable time stamps provided by O.TIME ensure that audit records provide the detail required to demonstrate when an action took place.	

Threat: T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE to access stored data and use security functions provided by the TOE.	
Objectives:	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.

Rationale:	O.IDAUTH requires that users be uniquely identified before accessing the TOE. O.PROTCT objective addresses this threat by preventing unauthorized access to TOE security functions and data.

Threat: T.PRIVIL	An unauthorized person or external IT entity may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to access of TOE functions. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.ADMIN objective addresses the threat by ensuring that only authorized administrators are able to access TOE security functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.	

Threat: T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE, or between the TOE and managed devices.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, or

		between the TOE and managed devices using cryptographic functions.
Rationale:	O.ENCRYP requires that an authorized administrator uses encryption when performing administrative functions on the TOE remotely. The O.ENCRYP objective ensures that communications between the TOE and managed devices are protected.	

4.3.2 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.

Policy: P.ACCACT	Users of the TOE shall be accountable for their actions.	
Objectives:	O.AUDIT	The TOE must provide user accountability for authorized administrator use of security functions by providing a means to record and view a readable audit trail of security-related events, with accurate dates and times.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	The O.AUDIT objective implements this policy by requiring auditing of the use of TOE functions. The O.IDAUTH objective supports this policy by ensuring each administrative user is uniquely identified and authenticated. O.TIME supports the audit trail with reliable time stamps.	

Policy: P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, malicious activity, or unintended access must be collected.	
Objectives:	O.AUDIT	The TOE must provide user accountability for authorized administrator use of security functions by providing a means to record and view a readable audit trail of security-related events, with accurate dates and times.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	The O.AUDIT objective supports this policy by ensuring the collection of data on security relevant events. O.TIME supports this policy by ensuring that the audit functionality is able to include reliable timestamps.	

Policy: P.MANAGE	The TOE shall be manageable only by authorized administrators.	
Objectives:	O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
	OE.ADMIN	Those responsible for the TOE must ensure that the TOE and the supporting hardware devices are delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of trusted, authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators follow all administrator guidance and are not malicious.
Rationale:	The O.ACCESS objective supports this policy by ensuring that authorized administrators have appropriate access to manage the TOE. O.ADMIN supports this policy by ensuring that the TOE provides the appropriate security management functionality to authorized administrators. O.IDAUTH supports this policy by ensuring that administrators must be identified and authenticated prior to being granted access to TOE security management functions. O.PROTCT supports this policy by ensuring that the TOE security functions may not be bypassed to allow unauthorized access. OE.ADMIN supports this policy by ensuring that only appropriately trained administrators have access to the TOE security functions.	

4.3.3 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 operational environment.

Assumption: A.NOEVIL	Authorized administrators are properly trained, not malicious, and follow all administrative guidance. Authorized administrators are trusted to administer the TOE correctly.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE and the supporting hardware devices are delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of trusted authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators follow all administrator guidance and are not malicious.
Rationale:	The OE.ADMIN objective supports this assumption by ensuring that administrators are properly trained, not malicious, and follow all administrative guidance.	

Policy: A.DELIVER	The TOE and all supporting hardware devices are delivered, installed, managed and operated in a manner which is consistent with IT Security best practices.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE and the supporting hardware devices are delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of trusted, authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators follow all administrator guidance and are not malicious.
	OE.PHYCAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
Rationale:	The OE.ADMIN objective supports this assumption by ensuring that the TOE and its supporting hardware are delivered, installed, managed and operated in accordance with the IT security practices. OE.PHYCAL supports the assumption by requiring that the installation protects the TOE from physical attack.	

Assumption: A.LOCATE	The TOE will be located within controlled access facilities and protected from unauthorized physical modification.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.

Rationale:	The OE.PHYCAL objective supports this assumption by ensuring the physical protection of the TOE.

Assumption: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE and the supporting hardware devices are delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of trusted, authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators follow all administrator guidance and are not malicious.
Rationale:	The OE.ADMIN objective supports the assumption by ensuring that all authorized administrators are qualified and trained to manage the TOE.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements (SFRs).

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements (SARs).

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, extended requirements, 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 within the brackets, e.g., [*assigned item*]. Assignments within selections are also indicated in this manner.
- 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 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (AES)
	FCS_CKM.1(2)	Cryptographic key generation (RSA)
	FCS_CKM.1(3)	Cryptographic key generation (DH)

Class	Identifier	Name
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 10 – 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 [minimum] level of audit; and

c) [*All auditable events listed in Table 11*].

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, 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 ST, [*information specified in Table 12*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAR.1	Reading of information from the audit records (Opening the audit trail)	The identity of the administrator performing the function
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	The identity of the administrator attempting the function
FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.1(3)	Success or failure of the activity	
FCS_CKM.4	Failure of the key zeroization	
FCS_COP.1	Failure of the cryptographic operation	
FDP_ACC.1	none	
FDP_ACF.1	Administrator action	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and action taken	Identity of the unsuccessfully authenticated user
FIA_SOS.1	none	
FIA_UAU.2	All uses of the authentication mechanism	
FIA_UID.2	Unsuccessful use of the user identification mechanism	Claimed identity of the user using the identification mechanism
FMT_MSA.1	Modification of the	The identity of the administrator

Requirement	Auditable Events	Additional Audit Record Contents
	security attributes	performing the function
FMT_MSA.3	Modification to the default settings or initial values of security attributes	
FMT_MTD.1	Modifications made to a device configuration	Description of the configuration change event
FMT_SMF.1	Use of management functions	The identity of the administrator performing the function
FMT_SMR.1	Modifications to the group of users that are part of a role	User identification of the administrator performing modification, and the user whose role is modified
FPT_ITC.1	Transmission of policy information	Device status change
FPT_STM.1	Changes to the time	The identity of the administrator performing the operation
FTP_ITC.1	Failure of the trusted channel functions	Identification of the initiator and target of the failed trusted channel functions
FTP_TRP.1	Failure of the trusted path functions	Identification of the claimed user identity

Table 11 – 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 [*authorized administrators*] with the capability to read [*all audit information*] from the audit records.

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_SAR.2 Restricted Audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1(1) Cryptographic key generation (AES)

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1(1).1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*CTR DRBG (AES)*] and specified cryptographic key sizes [*listed in Table 12*] that meet the following: [*National Institute of Standards and Technology Special Publication 800-90A, Revision 1, June 2015*].

Key Usage	Key Size
AES	128, 256

Table 12 – Cryptographic Key Generation

6.2.2.2 FCS_CKM.1 (2) Cryptographic key generation (RSA)

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1(2).1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Rivest Shamir Adleman (RSA)*] and specified cryptographic key sizes [*2048, 3072 bit*] that meet the following: [*FIPS 186-4 Appendix B*].

6.2.2.3 FCS_CKM.1 (3) Cryptographic key generation (DH)

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1(3).1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Diffie-Hellman Key Exchange (DH)*] and specified cryptographic key sizes [*2048, 3072 bit*] that meet the following: [*RFC 2631 and National Institute of Standards and Technology Special Publication 800-56A, Revision 3, April 2018*].

6.2.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*no standard*].

6.2.2.5 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key generation
FCS_CKM.1 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in Table 13*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 13*] and cryptographic key sizes [*cryptographic key sizes specified in Table 13*] that meet the following: [*standards listed in Table 13*].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Encryption and Decryption	AES (Advanced Encryption Standard in CBC mode for TLS)	128, 256	FIPS PUB 197 (AES) and ISO 10116 (CBC mode)	C780
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS1 using SHA-256)	2048, 3072	PKCS #1 v. 2.2	C780
Hashing	SHA-1	160	ISO 10118-3	C780
	SHA-256	256	ISO 10118-3	C780
	SHA-384	384	ISO 10118-3	C780

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Keyed Hash	HMAC-SHA-1	160 key 160 digest	ISO 9797-2	C780
	HMAC-SHA2-256	256 key 256 digest	ISO 9797-2	C780
	HMAC-SHA2-384	384 key 384 digest	ISO 9797-2	C780

Table 13 – Cryptographic Operation

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] on [
Subjects: Administrators
Objects: Security data
Operations: read-write, read-only].

6.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] to objects based on the following: [
Subjects: Administrators
Subject Attributes: Username, Profile
Objects: Security data
Attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Administrators are permitted read-write or read-only access to security data in order to perform administrative functions if the user's profile includes that permission*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*Super Users have read-write access to all security data*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 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 [an administrator configurable positive integer within [*1 to 10*]] unsuccessful authentication attempts occur related to [*administrator login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock out the IP address for a configurable period of time*].

6.2.4.2 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 [

- *minimum length requirements, which may be configured to be between 8 to 32 characters;*
- *composition requirements, which may specify that passwords must contain:*
  - *upper case letters,*
  - *lower case letters,*
  - *numbers, and/or*
  - *special characters*].

6.2.4.3 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.

6.2.4.4 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.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Administrative Access Control SFP*] to restrict the ability to [modify, delete, [*create*]] the security attributes [*Username, Profile*] to [*Super Users*].

6.2.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Administrative Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Super User*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete] the [*data associated with remote managed devices*] to [*users with a profile that allows device access*].

6.2.5.4 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: [

a) Manage users;

b) View audit records;

c) Manage devices; and

d) Manage policies

].

1.1.1.1 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 [*Super User, Standard User, Package User, Restricted User*, *and any custom roles created by the organization*].

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

6.2.6.2 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.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*period of 15 minutes of user inactivity*].

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 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 [*device management, distribution of policies*].

6.2.8.2 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 [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 [[*remote administration*]].

6.3 SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.3). EAL 4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.3 augmentation since current Fortinet flaw remediation practices and procedures meet or exceed this level of assurance.

The assurance requirements are summarized in Table 14.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target	ASE_CCL.1	Conformance claims

Assurance Class	Assurance Components	
	Identifier	**Name**
Evaluation (ASE)	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.3	Focused vulnerability analysis

Table 14 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.PROTCT	O.TIME
FAU_GEN.1			X				
FAU_GEN.2			X				
FAU_SAR.1	X	X	X				
FAU_SAR.2	X		X				
FCS_CKM.1(1)				X			

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.PROTCT	O.TIME
FCS_CKM.1(2)				X			
FCS_CKM.1(3)				X			
FCS_CKM.4				X			
FCS_COP.1				X			
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_AFL.1						X	
FIA_SOS.1						X	
FIA_UAU.2	X				X		
FIA_UID.2	X				X		
FMT_MSA.1	X	X				X	
FMT_MSA.3	X	X				X	
FMT_MTD.1	X	X				X	
FMT_SMF.1		X				X	
FMT_SMR.1					X	X	
FPT_ITC.1				X			
FPT_STM.1							X
FTA_SSL.3						X	
FTP_ITC.1				X			
FTP_TRP.1				X			

Table 15 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

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

Objective: O.ACCESS	The TOE must allow an authorized user access to only those TOE functions and data necessary to perform the duties assigned to that user.	
Security	FAU_SAR.1	Audit review

Functional Requirements:	FAU_SAR.2	Restricted audit review
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
Rationale:	FAU_SAR.1 and FAU_SAR.2 meet this objective by ensuring that only authorized administrators are able to access and read audit records. FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated prior to being allowed access to TOE security management functionality. FMT_MSA.1 ensures that only authorized administrators have access to the security attributes associated with the Administrative Access Control SFP. FMT_MSA.3 restricts default security attributes to further ensure that access is restricted to authorized administrators. FMT_MTD.1 ensures that only authorized administrators have access to data required to manage devices.	

Objective: O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
Rationale:	FAU_SAR.1 meets this objective by providing authorized administrators with the ability to read audit logs. FDP_ACC.1 and FDP_ACF.1 meet this objective by restricting access to the security data required to perform administrative functions. FMT_MSA.1 meets the objective by providing the functionality to manage the parameters associated with the Administrative Access	

	Control SFP. FMT_MSA.3 meets the objective by providing the initial values required to manage the Administrative Access Control SFP. FMT_MTD.1 meets this objective by providing functionality to access the data required to manage devices. FMT_SMF.1 meets the objective by providing the management functions supporting the specific security management claims.

Objective: O.AUDIT	The TOE must provide user accountability for authorized administrator use of security functions by providing a means to record and view a readable audit trail of security-related events, with accurate dates and times.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
Rationale:	FAU_GEN.1 supports the objective by detailing the set of events that the TOE must be capable of recording, ensuring that any security relevant event that takes place in the TOE is audited. FAU_GEN.2 supports the objective by ensuring that the audit records associate a user identity with the auditable event. FAU_SAR.1 provides the means to read the audit information, while FAU_SAR.2 ensures that only those specifically granted access may read the logs.	

Objective: O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, or between the TOE and managed devices using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1(1)	Cryptographic key generation (Symmetric keys)
	FCS_CKM.1(2)	Cryptographic key generation (RSA keys)
	FCS_CKM.1(3)	Cryptographic key generation (DH)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Rationale:	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.4, and FCS_COP.1 support the objective by providing the cryptographic functionality required to support trusted links. FPT_ITC.1, FTP_ITC.1 and FTP_TRP.1 support the objective by specifying the use of that cryptography between the TOE and the remote administrator, and between the TOE and the managed devices.

Objective: O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_SMR.1	Security roles
Rationale:	FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated prior to being granted access to TOE security management functions, or to a connected network. FMT_SMR.1 supports the objective by providing roles which are used to provide users access to TOE security functionality.	

Objective: O.PROTCT	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.	
Security Functional Requirements:	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination
Rationale:	The security management SFRs: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1, support the objective by ensuring that access to TOE security functions is limited to authorized users. FIA_AFL.1 supports the objective by ensuring that unauthorized users are locked out following a configurable number of unsuccessful authentication attempts, thereby thwarting a brute force attack on the TOE. FIA_SOS.1 ensures that administrator	

	passwords meet requirements for length and composition to reduce the risk of a successful brute force attack. FTA_SSL.3 supports the objective by ensuring that open sessions are closed automatically after a period of inactivity to reduce the risk of an attacker using an open session.

Objective: O.TIME	The TOE shall provide reliable time stamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 supports this objective by providing reliable time stamps.	

6.4.3 Dependency Rationale

Table 16 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	✓	Satisfied by FPT_STM.1
FAU_GEN.2	FAU_GEN.1	✓	Satisfied by FAU_GEN.1
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	Satisfied by FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	✓	Satisfied by FAU_SAR.1
FCS_CKM.1 (1)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4
FCS_CKM.1 (2)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4
FCS_CKM.1 (3)	FCS_CKM.2 or FCS_COP.1		Satisfied by FCS_COP.1. These keys are used as the TLS exchange keys.
	FCS_CKM.4		Satisfied by FCS_CKM.4

SFR	Dependency	Dependency Satisfied	Rationale
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	✓	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	✓	Satisfied by FDP_ACC.1
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; therefore this dependency has been satisfied.
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; therefore this dependency has been satisfied.
FIA_SOS.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1
	FMT_SMR.1	✓	Satisfied by FMT_SMR.1
	FMT_SMF.1	✓	Satisfied by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	✓	Satisfied by FMT_MSA.1
	FMT_SMR.1	✓	Satisfied by FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	✓	Satisfied by FMT_SMR.1
	FMT_SMF.1	✓	Satisfied by FMT_SMF.1
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency has been satisfied.
FPT_ITC.1	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 16 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.3). EAL 4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.3 augmentation since current Fortinet flaw remediation practices and procedures meet or exceed this level of assurance.

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 creates audit records for administrative events, including device management and the provision of policy information to managed devices. The TOE records the identity of the Administrator who caused the event for which the audit record is created. The TOE applies timestamps to auditable events as they occur.

An Administrator in any of the four pre-configured administrative profiles can review the audit records. The pre-configured profiles are described in Section 7.5. The audit records are stored locally, using memory, but may also be stored on a hard disk or a FLASH memory card, depending on the supporting hardware model.

Logs may be read using the Command Line Interface (CLI) or the Graphical User Interface (GUI) on the TOE. This functionality is provided to a user in any profile with Log View privileges.

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

7.2 CRYPTOGRAPHIC SUPPORT

The TOE implements a FIPS-validated cryptographic module.

Cryptographic support is provided using a software based, deterministic random bit generator (DRBG) that conforms to the National Institute of Standards and Technology Special Publication 800-90A, Revision 1, June 2015. This generates cryptographic keys whose strengths are modified by available entropy. Entropy is provided using a Fortinet entropy token to seed the DRBG during the boot process and to periodically reseed the DRBG. Operation of the token is based on a wide-band Gaussian white noise generator and provides a source of entropy. The default reseed period is once every 24 hours (1440 minutes). The token is connected to the Fortinet hardware device or virtual machine hardware using a standard USB interface, and must be installed to complete the boot process and to reseed of the DRBG. The entropy token is responsible for loading a minimum of 256 bits of entropy. Although the hardware token (in the operational environment) provides entropy to the TOE, it is the TOE that implements all of the claimed cryptographic functionality, including key generation, key destruction and cryptographic operation.

Each FortiManager unit is delivered with a factory installed 2048-bit RSA public/private key pair. Asymmetric keys are also generated in support of TLS functionality, using Diffie-Hellman key exchange and RSA. RSA asymmetric keys and Diffie-Hellman key exchange are also used in support of SSH.

AES keys are generated and used in CBC mode.

Cryptographic key destruction is performed by overwriting the key material with random data. The TOE only stores keys in memory, either in Synchronous Dynamic Random Access Memory (SDRAM) or Flash Random Access Memory (RAM).

Cryptographic operations are performed in accordance with the detail provided in Table 13.

TOE Security Functional Requirements addressed: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

The TOE provides an Administrative Access Control SFP that controls access of Administrators with any of the pre-configured profiles to the data required to manage the TOE functions. Access to the TOE functions are based on the Administrator profile, as described in Section 7.5.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1.

7.4 IDENTIFICATION AND AUTHENTICATION

In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access. Authentication failure handling is implemented to further protect this interface. Administrators can set an administrative lockout threshold between 1 and 10 login attempts. When authentication of an Administrator from a particular IP address fails the set number of times, the IP address is locked out for an Administrator-configurable period of time. The default number of unsuccessful login attempts for triggering lockout is three, and the default lockout time period is 60 seconds.

Administrators can set a password policy that specifies the minimum number of characters in a password (8 to 32) and the types of characters that a password must contain (uppercase letters, lowercase letters, numbers and/or special characters). User management, including management of identification and authentication settings, is performed by an Administrator with a Super User profile, or a custom profile with similar user management permissions.

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

7.5 SECURITY MANAGEMENT

The TOE provides a web-based GUI and a CLI to manage all of the security functions. The GUI is accessed through a TLS-protected session and may be accessed remotely. The CLI is accessed using a direct console connection, or through a Secure Shell (SSH) protected connection. The functions provided through these interfaces include the management of FortiManager administrative users, and review of audit records. The interfaces also allow for the management of networked Fortinet devices, including configuration of devices and policy management.

Management of the security attributes that control access to user management functions is limited to users who have been assigned Super User profiles. Users with the associated Super User privileges are able to create, modify, and delete other user accounts. The default values for the security attributes (username, profile) are restrictive in nature in that there is no username until it is entered by an administrator. Likewise, no profile is associated with a username until that information is entered by an administrator with Super User privileges.

The TOE also restricts access to the data associated with the remote managed devices. Although all of the predefined profiles include some device manager privileges, users with Restricted User and Package User profiles have read-only access to some of the device data. Users assigned Super User or Standard User profiles have read-write access to all device manager data allowing them the ability to perform all device management functions.

The TOE provides four predefined administrator profiles. Each profile has a set of associated system privileges. Users assigned to the Super User profile have access to all data and functions. Users assigned the Standard User profile have most device and policy management privileges, but are not able to manage users and system settings. Package Users have similar access to data, but with read-only privileges to some of the data, and are therefore not able to perform as many functions. Restricted users are limited to read-only access to most data, and no access to the data related to system level functionality. Additionally, the organization can create custom profiles, selecting from the permissions in Table 17, with the exception of the CLI only settings, which are only available in the preconfigured profiles.

Setting	Super User	Standard User	Restricted User	Package User
System Settings	Read-Write	None	None	Read-Only
Administrative Domain	Read-Write	Read-Write	None	Read-Write
FortiGuard Center	Read-Write	None	None	Read-Only
License Management	Read-Write	None	None	Read-Only
Firmware Management	Read-Write	None	None	Read-Only
Advanced	Read-Write	None	None	Read-Only
Device Manager	Read-Write	Read-Write	Read-Only	Read-Write
Add/Delete Devices/Groups	Read-Write	Read-Write	None	Read-Write

Setting	Super User	Standard User	Restricted User	Package User
Retrieve Configuration from Devices	Read-Write	Read-Write	Read-Only	Read-Only
Revert Configuration from Revision History	Read-Write	Read-Write	Read-Only	Read-Only
Terminal Access	Read-Write	Read-Write	Read-Only	Read-Only
Manage Device Configurations	Read-Write	Read-Write	Read-Only	Read-Write
Provisioning Templates	Read-Write	Read-Write	Read-Only	Read-Write
SD-WAN	Read-Write	Read-Write	Read-Only	Read-Write
Policy & Objects	Read-Write	Read-Write	Read-Only	Read-Write
Global Policy Packages & Objects	Read-Write	Read-Write	None	Read-Write
Assignment	Read-Write	None	None	Read-Only
Policy Packages & Objects	Read-Write	Read-Write	Read-Only	Read-Write
Policy Check	Read-Write	Read-Write	Read-Only	Read-Only
Install Policy Package or Device Configuration	Read-Write	Read-Write	Read-Only	Read-Write
Import Policy Package	Read-Write	Read-Write	Read-Only	Read-Write
Interface Mapping	Read-Write	Read-Write	Read-Only	Read-Write
AP Manager	Read-Write	Read-Write	Read-Only	Read-Write
FortiClient Manager	Read-Write	Read-Write	Read-Only	Read-Write
FortiSwitch Manager	Read-Write	Read-Write	Read-Only	Read-Write
VPN Manager	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Super User	Standard User	Restricted User	Package User
Log View/ FortiView/NOC	Read-Write	Read-Write	Read-Only	Read-Write
Event Management	Read-Write	Read-Write	Read-Only	Read-Only
Reports	Read-Write	Read-Write	Read-Only	Read-Only
CLI only realtime-monitor	Read-Write	Read-Write	Read-Only	None
CLI only read-passwd	Read-Write	None	None	Read-Only

Table 17 – Predefined Administrator Profiles

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

The TOE is able to send policy and object information to managed devices. Policy and object information includes configuration information, antivirus definitions, intrusion protection signatures, access rules and firmware updates. All information is sent over a connection protected using TLS version 1.1 (RFC4346) or TLS 1.2 (RFC 5246). The supported ciphersuites are described in Section 7.8.

Time is provided by the TSF and can only be changed by an authorized administrator. The supporting hardware devices include a hardware clock which is used to generate reliable time stamps which in turn are used by the TOE for audit records and to provide scheduling features for flow control policies.

TOE Security Functional Requirements addressed: FPT_ITC.1, FPT_STM.1.

7.7 TOE ACCESS

An administrative session with the GUI or the CLI is closed after fifteen minutes of inactivity. The Administrator must log in again to regain access. This applies to an Administrator with any profile.

TOE Security Functional Requirements addressed: FTA_SSL.3.

7.8 TRUSTED PATH / CHANNELS

The TOE provides trusted paths and trusted channels, protected by encryption to guard against disclosure and protected by cryptographic signature to detect modifications.

7.8.1 Trusted Path

A trusted path is used to protect authentication of Administrators, and administration activities. This channel is logically distinct from other communication channels and provides assured identification of the end points and protection of the channel data from disclosure. TLS version 1.1 (RFC 4346) and TLS 1.2 (RFC 5246) are used to encrypt and authenticate administration sessions between the remote browser and TOE. The TOE supports the following ciphersuites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES _128_SHA
- TLS_RSA_WITH_AES _256_SHA

Secure hash functions SHA-1provides support to the TLS protocol.

SSH is used to protect remote connections to the CLI. The SSH implementation complies with RFCs 4251, 4252, 4253, and 4254. Administrators use password based or SSH-RSA public key authentication. AES-CBC-128 and AES-CBC-256 symmetric algorithms are used. Data integrity is provided using HMAC-SHA1, HMAC-SHA-256 and HMAC-SHA-384. Secure hash functions SHA-1, SHA-256 and SHA-384 provide support to the HMAC functions. Diffie-Hellman-Group 14 is used for key exchange. Rekeying occurs following the transfer of 1GB of data. Packets greater than 32768 bytes are automatically dropped.

TOE Security Functional Requirements addressed: FTP_TRP.1

7.8.2 Trusted Channel

The trusted channel is established between the TOE and the managed Fortinet device, or between the TOE and the FortiGuard service.

In the evaluated configuration, the TOEalways initiates the communications to the managed devices. The trusted channel provides security for communications between the TOE and the managed devices using TLS 1.1 or 1.2, and the ciphersuites described above. This channel is logically distinct from other communication channels and provides assured identification of the end points and protection of the channel data from disclosure.

In the evaluated configuration, the TOE always initiates the communications to receive updates from the FortiGuard service. Updates may be loaded manually over an air gap using a USB token, or an update request may be sent manually from the TOE to the FortiGuard service. In this case, the updates are sent over a protected link using TLS 1.1 or 1.2, and the ciphersuites described above for the trusted path. This channel is also logically distinct from other communication channels and provides assured identification of the end points and protection of the channel data from disclosure.

TOE Security Functional Requirements addressed: FTP_ITC.1

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
FortiGuard	FortiGuard provides up-to-date security threat information services, including antivirus definitions and intrusion prevention signatures.
Local Console	A management console (may be a computer workstation or VT100 type terminal) connected directly to the TOE. Although the Local Console falls outside the TOE Boundary it is located in the same physical location as the TOE and therefore is provided with the same physical protection as is provided for the TOE.
Management Workstation	A computer located remotely from the TOE but which is able to establish a network connection to the TOE. The Management workstation falls outside the TOE Boundary.
Person	A person is a human being. A person can be, but is not necessarily, an authorized user.
Administrators	The term 'Administrators' is used to refer to all TOE administrative users assigned to any profile. Where capabilities are distinguished by administrator profile, the individual profile name is specified.
User	A user may be a person or an IT entity.

Table 18 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ADOM	Administrative Domain
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-block Chaining
CC	Common Criteria

Acronym	Definition
CLI	Command Line Interface
CM	Configuration Management
CTR	Counter-mode
DH or DHE	Diffie-Hellman Key Exchange
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Keyed Hash Message Authentication Code
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PKCS	Public-Key Cryptography Standards
PP	Common Criteria Protection Profile
RAM	Random Access Memory
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
RSASSA-PKCS1	RSA Signature Scheme with Appendix PKCS1
SDK	Software Development Kit
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TLS	Transport Layer Security

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
XML	eXtensible Markup Language

Table 19 – Acronyms