Fortinet FortiAnalyzer® 7.2

Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 05-729-1129995-20250625
Version: 1.4
25 June 2025

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

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.

Section 9, Annex A, identifies the TOE hardware models and guides.

1.2 SECURITY TARGET REFERENCE

ST Title:	Fortinet FortiAnalyzer® 7.2 Security Target
ST Version:	1.4
ST Date:	25 June 2025

1.3 TOE REFERENCE

TOE Identification:	Fortinet FortiAnalyzer® 7.2.9 (Build # 6429)
TOE Developer:	Fortinet, Incorporated
TOE Type:	Log Collection and Reporting

1.4 TOE OVERVIEW

The TOE is an integrated network appliance that provides log collection and reporting tools. The TOE keeps records of emails, File Transfer Protocol (FTP), web browsing, security events and other network activity and subsequently analyzes them to aid in the identification of security issues and to reduce network misuse and abuse.

The TOE has two modes of operation: Analyzer and Collector mode.[1] The Analyzer mode, which is the default mode, supports all the monitoring features of the FortiAnalyzer for analysis and reporting. The Collector mode supports the storage and distribution of the logs and save states.

With its logging capabilities, the TOE can act as an audit server. The TOE can also be used as a Quarantine repository for files that are suspected to have been infected with a virus.

The TOE also provides Vulnerability Management by analyzing logs collected from target hosts for known vulnerabilities and open ports. Upon scan completion, the FortiAnalyzer creates a report that describes the security issues it found and their known solution. Packet Capture works in a similar way, where the TOE checks the logs for areas of the network that may require policy adjustment for the firewall or traffic.

Administrative domains (ADOMs) offer further security by assigning separate parts of the network to different administrators. The TOE maintains a separation between the different domains, but a single administrator may be assigned to multiple ADOMs. There are three levels of Users for the system: Restricted users, Standard Users, and Super Users. A Restricted User has only read permissions for certain parts of the system. A Standard User has all the read-write options a Super User has except for changing the Server Settings.

[1] Application Note: Only the Analyzer mode of operation is included in the evaluated configuration.

Administrators must be successfully authenticated before being granted access to the TOE.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Management Workstation	Windows 11 supporting a web browser and terminal application	General purpose computing hardware
Managed Devices	FortiGate v7.2.9[1] FortiManager v7.2.9[2]	Fortinet FortiWiFi 60F Fortinet Manager 200G

Table 1 – Non-TOE Hardware/Firmware/Software

Note 1: FortiAnalyzer supports connectivity with FortiGate and FortiWiFi versions (6.2.0->6.2.16, 6.4.0->6.4.15, 7.0.0->7.0.17, 7.2.0->7.2.10)

Notes 2: FortiAnalyzer supports connectivity with FortiManager versions (6.4.0->6.4.19, 7.0.0->7.0.17, 7.2.0->7.2.10)

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The FortiAnalyzer 7.2 firmware is deployed on a stand-alone FortiAnalyzer appliance.

Model	CPU/Entropy Source
FAZ-300G	Intel Core i3-8100 Fortinet CPU Jitter Entropy Library 1.0

Table 2 – TOE Hardware Models

Figure 1 – TOE Diagram shows the TOE in the evaluated configuration.

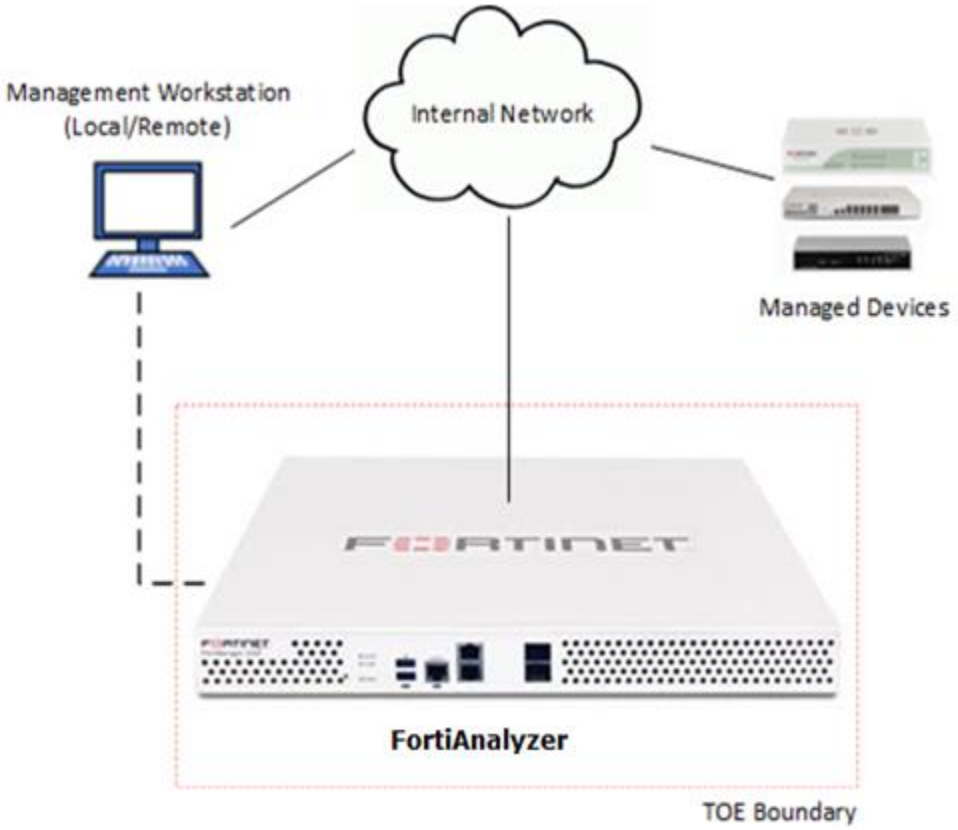

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

FortiAnalyzer units are shipped directly to customers with the FortiAnalyzer software pre-installed. If the version of FortiAnalyzer is not the CC-evaluated version, customers can download the correct version by logging into the Fortinet

Customer Support website (https://support.fortinet.com) and navigating to **Download** > **Firmware Images**.

Due to having different device drivers, each model offered in the FortiAnalyzer Series has its own unique firmware image created from the same common firmware build. For each series, the hardware model identifier changes (i.e. *100A*).

Customers can download the software based on their FortiAnalyzer hardware model. The software is provided to customers as an .out file. An example of a filename is as follows:

- *FAZ-300G-v7.2.9-build6429-FORTINET.out*

1.5.1.2 TOE Guidance

The following lists the TOE Guidance Documentation to install, configure, and maintain the TOE:

- FortiAnalyzer v7.2.9 Administration Guide, January 14, 2025
  - *FortiAnalyzer-7.2.9-Administration_Guide.pdf*
- FortiAnalyzer v7.2.9 CLI Reference, December 11, 2024
  - *FortiAnalyzer_7.2.9_CLI_Reference.pdf*
- FortiManager & FortiAnalyzer 7.2.9 Log Reference, December 11, 2024
  - *FortiManager_&_FortiAnalyzer_7.2.9_Log_Reference.pdf*
- FortiAnalyzer v7.2.9 Release Notes, February 4, 2025
  - *fortiAnalyzer-7.2.9-release-notes.pdf,*

These documents can be found in Portable Document Format (PDF) format and downloaded at https://docs.fortinet.com/product/fortianalyzer/7.2.

In addition to the above, a series of Information Supplement and QuickStart Guides are included as part of the TOE. Each of these guides is specific to the hardware model it references. A list of these guides is provided in Table 20.

The following FIPS and Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- FortiAnalyzer 7.2, EAL4 Common Criteria Technote, June 25, 2025
  - *FAZ 7.2 EAL4 CC Technote.pdf*

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. 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 may view the contents of the audit records; however, this functionality is restricted to those users authorized to view the records. The TOE uses aggregated audit events to recognize potential security violations. All audit records are protected from modification and unauthorized deletion.
Cryptographic Support	The TOE provides cryptographic operation functions supported by Cryptographic Algorithm Validation Program (CAVP) - validated algorithms with Fortinet FortiAnalyzer SSL Cryptographic Library Version: 7.2, which are part of the TOE.
User Data Protection	The TOE controls access to the security data required to perform security management functions including management of devices.
Identification and Authentication	Users must be identified and authenticated prior to gaining access to the TOE.
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	Reliable time stamps are provided to support the audit function.
TOE Access	The TOE is capable of terminating local and remote administrative sessions upon detection of administrator inactivity. The TOE is capable of terminating a remote session upon request from a remote administrator such as when a request to logout is received.
Trusted Path	The TOE requires an encrypted trusted channel for communication between the TOE and the managed devices in support of the collection of logs. A trusted path communication is required in support of remote administration.
Data Collection and Reporting	Data is collected from the TOE and monitored devices protected by the TOE, aggregated and analyzed. Based on the analysis, potential violations are identified, and reports are generated.

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. Automated updates that do not require administrative action were not evaluated.
- The following Representational State Transfer (REST) Application Programming Interfaces (APIs) are not included in the evaluation:
  - JavaScript Object Notation (JSON)
  - eXtensible Markup Language (XML)
  - Software Development Kit (SDK)
- FortiManager acting as a Management system for a FortiAnalyzer using the FGFM protocol is currently excluded from the evaluation.
- The following protocol/interfaces are excluded from this evaluation:

  SSH Client, DDNS, DHCP, HTTP, NTP, SNMP, SMTP, Telnet, TFTP Client, LDAP, USB, RADIUS, SYSLOG and High Availability.
- FortiView module
- FortiSoC Service
- Collector Mode
- The Trusted Platform Module (TPM)
- FortiAnalyzer Cloud

1.5.4 Disabled Features

The following TOE features are disabled by default and are excluded from the scope of this evaluation:

- Web UI over HTTP (HTTPS must be used)
- The TOE acting as a telnet client or server
- The TOE acting as a TFTP client

1.5.5 Vendor Supported but not Evaluated Hardware Models

The following table lists the Hardware models supported for this release but were not evaluated:

Model	CPU/Entropy Source
FAZ-150G	ATOM E3940

FAZ-300F	Intel G4400 Skylake
FAZ-400E	Intel Core i3-4350T
FAZ-800F	Intel Core i3-6100
FAZ-800G	Intel Core i5-8500
FAZ-810G	Intel Core i5-8500
FAZ-1000F	Intel Xeon Bronze 3106
FAZ-1000G	AMD EPYC 3251
FAZ-2000E	Intel Xeon E5-2620v3
FAZ-3000F	2 x Intel Xeon E5-2630v3
FAZ-3000G	2 x Intel Xeon Silver 4215
FAZ-3100G	2 x Intel Xeon Silver 4215
FAZ-3500E	2 x Intel Xeon E5-2630v2
FAZ-3500F	2 x Intel Xeon E5-2650v2
FAZ-3500G	2 x Intel Xeon Gold 5118
FAZ-3510G	AMD EPYC 3251
FAZ-3700F	2 x Intel Xeon E5-2640v4
FAZ-3700G	2 x Intel Xeon Gold 5218

Table 4 – Vendor Supported but not Evaluated Hardware Models

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 extended
- 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 CONFORMANCE CLAIM

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

2.3 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 PP; therefore, a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats addressed by the TOE. Potential threat agents are unauthorized users 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 FortiAnalyzer 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.

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

Threat	Description
T.AUDACC	TOE Users may not be accountable for the actions that they conduct because the audit records are not created and reviewed, thus allowing an unauthorized user to escape detection.
T.LACKDATA	Unauthorized users or external IT entities may initiate widespread attacks on the TOE or devices protected by the TOE, which may go unnoticed due to a lack of data.
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.PRIVILEGE	An unauthorized user 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 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 5 - Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 6 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 to the TOE must be collected.
P.MANAGE	The TOE shall be manageable only by authorized administrators.

Table 6 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 7.

Assumption	Description
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 7 – 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 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 record audit records for use of the TOE functions and protect those records from unauthorized deletion or modification.
O.ENCRYPT	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.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
O.PROTECT	The TOE must protect itself against attempts by unauthorized users or unauthorized entities 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.REPORT	The TOE must gather, analyze and create reports on all events indicating a breach in the policy related to use of the TOE or resources protected by the TOE.
O.TIME	The TOE shall provide reliable time stamps.

Table 8 – 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.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.

Table 9 – 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.LACKDATA	T.NOAUTH	T.PRIVILEGE	T.PROCOM	P.ACCACT	P.DETECT	P.MANAGE	A.LOCATE	A.NOEVIL	A.MANAGE
O.ADMIN	X			X				X			
O.AUDIT	X					X	X				
O.ENCRYPT					X						
O.IDENTAUTH			X	X		X		X			
O.PROTECT			X	X				X			
O.REPORT		X		X							
O.TIME	X					X	X				
OE.ADMIN										X	X
OE.PHYSICAL									X		

Table 10 – 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 and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.AUDACC**	TOE Users may not be accountable for the actions that they conduct because the audit records are not created and reviewed, thus allowing an unauthorized user 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 record audit records for use of the TOE functions and protect those records from unauthorized deletion or modification.
	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. O.TIME ensures that audit records provide the detail required to demonstrate when an action took place.	

Threat: **T.LACKDATA**	Unauthorized users or external IT entities may initiate widespread attacks on the TOE or devices protected by the TOE, which may go unnoticed due to a lack of data.	
Objectives:	O.REPORT	The TOE must gather, analyze and create reports on all events indicating a breach in the policy related to use of the TOE or resources protected by the TOE.
Rationale:	O.REPORT ensures that attacks do not go unnoticed by gathering data and allowing the creation reports.	

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.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTECT	The TOE must protect itself against attempts by unauthorized users or unauthorized entities 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.IDENTAUTH requires that users be uniquely identified before accessing the TOE. O.PROTECT prevents unauthorized access to TOE security functions and data.	

Threat: **T.PRIVILEGE**	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
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.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTECT	The TOE must protect itself against attempts by unauthorized users or unauthorized entities 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.REPORT	All events that are indicative of inappropriate activity that may have resulted from misuse, malicious activity, or unintended access to the TOE must be collected.

Rationale:	O.IDENTAUTH provides authentication of users prior to access of TOE functions. O.ADMIN ensures that only authorized administrators are able to access TOE security functions. O.PROTECT addresses this threat by providing TOE self-protection. O.REPORT provides responses to breaches in policy such as unauthorized access to the TOE.

Threat: **T.PROCOM**	An unauthorized person or 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.ENCRYPT	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.ENCRYPT requires that an authorized administrator uses encryption when performing administrative functions on the TOE remotely. O.ENCRYPT 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 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 record audit records for use of the TOE functions and protect those records from unauthorized deletion or modification.
	O.IDENTAUTH	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:	O.AUDIT supports this policy by requiring auditing of the use of TOE functions. O.IDENTAUTH 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 record audit records for use of the TOE functions and protect those records from unauthorized deletion or modification.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	O.AUDIT 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.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.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTECT	The TOE must protect itself against attempts by unauthorized users or unauthorized entities 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.ADMIN supports this policy by ensuring that the TOE provides the appropriate security management functionality to authorized administrators. O.IDENTAUTH supports this policy by ensuring that administrators must be identified and authenticated prior to being granted access to TOE security management functions. O.PROTECT supports this policy by ensuring that the TOE security functions may not be bypassed to allow unauthorized access.	

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 TOE's operational environment.

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities and protected from unauthorized physical modification.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by ensuring the physical protection of the TOE.	

Assumption: **A.MANAGE**	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:	OE.ADMIN supports the assumption by ensuring that all authorized administrators are qualified and trained to manage the TOE.	

Assumption: **A.NOEVIL**	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:	OE.ADMIN supports this assumption by ensuring that administrators are properly trained, not malicious, and follow all administrative guidance.

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFR)s used in this ST. The following extended SFRs have been created to address additional security features of the TOE:

a. Aggregation (DCR_AGG_EXT.1);
b. Data Collection (DCR_COL_EXT.1);
c. Quarantine (DCR_QUA_EXT.1); and
d. Reporting (DCR_REP_EXT.1).

5.1 CLASS DCR: DATA COLLECTION AND REPORTING

Data Collection and Reporting addresses the collection of security information from monitored devices, and the actions performed on that information. These actions include data collection and aggregation. The Data Collection and Reporting class was modelled after the classes FAU: Security audit and FDP: User data protection. Aggregation (DCR_AGG_EXT.1) was modelled after FDP_SDI.1 Stored data integrity monitoring. Data Collection (DCR_COL_EXT.1) was modelled after FAU_GEN.1 Audit data generation. Quarantine (DCR_QUA_EXT.1) was modelled after FDP_SDI.1 Stored data integrity monitoring. Reporting (DCR_REP_EXT.1) was modelled after FAU_SAA.1 Potential violation analysis.

5.1.1 DCR_AGG_EXT Aggregation

Family Behaviour

This family defines the requirements for the aggregation of data. This family may be used to specify that data be aggregated for the purposes of analysis and reporting.

Component Levelling

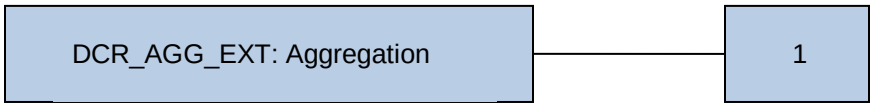

Figure 2 – DCR_AGG_EXT: Aggregation Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

DCR_AGG_EXT.1 Aggregation

Hierarchical to: No other components.

Dependencies: DCR_COL_EXT.1 Data collection

DCR_AGG_EXT.1.1 The TSF shall be able to aggregate data collected from monitored devices for further analysis and reporting.

5.1.2 DCR_COL_EXT Data Collection

Family Behaviour

This family defines the requirements for the collection of data. This family may be used to specify the information types to be collected.

Component Levelling

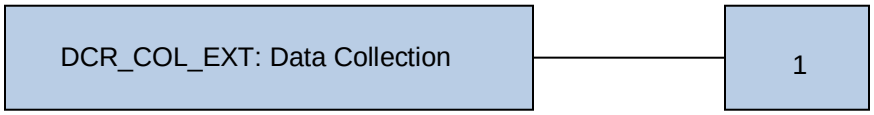

Figure 3 – DCR_COL_EXT: Data Collection Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a. Configuring the targeted IT system resources; and

b. Configuring the information types to be collected.

Audit

There are no auditable events foreseen.

DCR_COL_EXT.1 Data collection

Hierarchical to: No other components.

Dependencies: No dependencies

DCR_COL_EXT.1.1 The TSF shall be able to collect the following information types from the targeted IT system resource(s): [assignment: *information types*].

5.1.3 DCR_QUA_EXT Quarantine

Family Behaviour

This family defines the requirements for quarantining data. This family may be used to specify this function.

Component Levelling

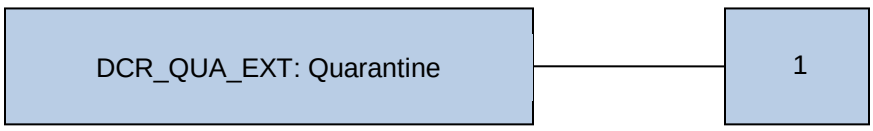

Figure 4 – DCR_QUA_EXT: Quarantine Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a. Configuring the targeted IT system resources; and

b. Configuring the information types to be collected.

Audit

The following action should be auditable if FAU_GEN Security audit data generation is included in the ST:

a. Minimal: Data quarantine event (data saved to quarantine, examination of quarantined data, data removed from quarantine.)

DCR_QUA_EXT.1 Quarantine

Hierarchical to: No other components.

Dependencies: No dependencies

DCR_QUA_EXT.1.1 The TOE shall be able to isolate selected data to a container controlled by the TSF where it may be examined, deleted or restored.

5.1.4 DCR_REP_EXT Reporting

Family Behaviour

This family defines the requirements for the creation of reports. This family may be used to describe the specific events, activities and patterns or trends that are to be addressed by the reports.

Component Levelling

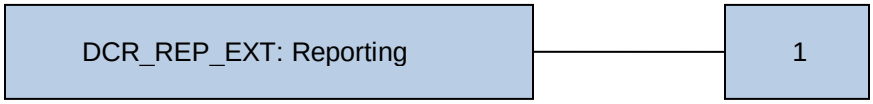

Figure 5 – DCR_REP_EXT: Data Collection Component Levelling

Management

The following action could be considered for the management function in FMT:

a. modification of report parameters.

Audit

There are no auditable events foreseen.

DCR_REP_EXT.1 Reporting

Hierarchical to: No other components.

Dependencies: DCR_AGG_EXT.1

DCR_REP_EXT.1.1 The TSF shall be able to apply a set of rules to the aggregated data to create reports relating to the following events, activities or patterns: [assignment: *specific events, activities and patterns*].

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, 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 11.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (administrators)

Class	Identifier	Name
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FDP_ACC.1(2)	Subset access control (devices)
	FDP_ACF.1(2)	Security attribute based access control (devices)
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (administrators)
	FMT_MSA.1(2)	Management of security attributes (devices)
	FMT_MSA.3(1)	Static attribute initialisation (administrators)
	FMT_MSA.3(2)	Static attribute initialisation (devices)
	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_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Data Collection and Reporting (EXT_DCR)	DCR_AGG_EXT.1	Aggregation
	DCR_COL_EXT.1	Data Collection
	DCR_QUA_EXT.1	Quarantine
	DCR_REP_EXT.1	Reporting

Table 11 – 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) [*All auditable events listed in Table 12*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in Table 12*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of audit	
FAU_GEN.2	None	
FAU_SAA.1	Changes to the monitoring rules	
	Detection of violation	Condition that was matched and action performed
FAU_SAR.1	None	
FAU_STG.1	None	
FDP_ACC.1(1)	None	
FDP_ACC.1(2)	None	
FDP_ACF.1(1)	None	
FDP_ACF.1(2)	Successful requests to apply the device access control SFP[2]	
FIA_UAU.2	Use of the authentication mechanism	Claimed identity of the user

[2] The device access control SFP controls access from monitored devices to the TOE.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UID.2	Use of the identification mechanism	Claimed identity of the user
FMT_MSA.1	Modification of the security attributes	The identity of the Administrator performing the function
FMT_MSA.3	Modification of the security attributes	The identity of the Administrator performing the function
FMT_MTD.1	None	
FMT_SMF.1	None	
FMT_SMR.1	Modifications to an access profile or user	The identity of the Administrator performing the function
FPT_STM.1	Changes to the time	The identity of the Administrator performing the function **Note**: This event is recorded when the system clock is changed using the CLI.
FTA_SSL.3	The termination of a remote session by the session locking mechanism	
FTA_SSL.4	The termination of an interactive session	
FTP_ITC.1	All attempted uses of the trusted channel functions	Identification of the initiator and target of all trusted channels
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of the initiator and target of all trusted channels
DCR_AGG_EXT.1	None	
DCR_COL_EXT.1	None	
DCR_QUA_EXT.1	Quarantine event	Source of data being quarantined
DCR_REP_EXT.1	None	

Table 12 - 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_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*events causing an alert event's trigger(s) to reach the specified threshold frequency*] known to indicate a potential security violation;

b) [*Match on a condition defined by log type and severity of event, match on a specified word in the log message*].

6.2.1.4 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.

6.2.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 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 (bits)	Standard	CAVP Certificate Number
Encryption and Decryption	AES (Advanced Encryption Standard in CBC mode for TLS)	128, 256	FIPS PUB 197 (AES) and NIST SP 800-38A	A6837
Encryption and Decryption	AES-GCM (Advanced Encryption Standard with GCM used for TLS)	128, 256	FIPS PUB 197 and NIST SP 800-38D	A6837
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS-v1_5 using SHA-256)	2048, 3072, 4096	PKCS #1.5, PSS	A6837
	Elliptic Curve Digital Signature Algorithm (ECDSA)	P-256 P-384 P-521	FIPS 186-5 (Digital Signature Standard)	A6837
Key Agreement in support of TLS & SSH	Key Agreement Schemes (KAS) and Key Confirmation (Diffie-Hellman)	2048. 4096, 8192	NIST SP800-56A	A6837
	EC DH	P-256 P-384 P-521		A6837

Operation	Algorithm	Key Size or Digest (bits)	Standard	CAVP Certificate Number
Hashing	SHA-1	160	FIPS PUB 180-3	A6837
	SHA-256	256		
	SHA-384	384		
	SHA-512	512		
Keyed Hash	HMAC-SHA-1	160 key 160 digest	FIPS PUB 198	A6837
	HMAC-SHA2-256	256 key 256 digest		
	HMAC-SHA2-384	384 key 384 digest		
	HMAC-SHA2-512	8 ~ 1024 bit key 512 bit digest		
Random Bit Generation	CTR_DRBG	N/A	NIST SP800-90A	A6839

Table 13 – Cryptographic Operation

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1(1) Subset access control (administrators)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*administrative access control SFP*] on [

Subjects: Administrators

Objects: TSF data

Operations: read only, read/write]

6.2.3.2 FDP_ACC.1(2) Subset access control (devices)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*device access control SFP*] on [

Subjects: Devices

Objects: Logs, DLP archives, quarantined files, IPS Packet Logs

Operations: receive]

6.2.3.3 FDP_ACF.1(1) Security attribute based access control (administrators)

Hierarchical to: No other components.

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

FDP_ACF.1.1(1) The TSF shall enforce the [*administrative access control SFP*] to objects based on the following: [

Subjects: Administrators

Security attributes: Username, Access Profile, Administrative Domain

Objects: TSF data

Security attributes: none].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an authorized administrator may read only or read/write TSF data if the administrator's access profile contains the permission to perform that function for that data type*].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*Super Users have read-write access to all TSF data*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [Administrative users associated with a given administrative domain **are** denied access to devices or virtual domains which are not assigned to that given administrative domain].

6.2.3.4 FDP_ACF.1(2) Security attribute based access control (devices)

Hierarchical to: No other components.

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

FDP_ACF.1.1(2) The TSF shall enforce the [*device access control SFP*] to objects based on the following: [

Subjects: Devices

Security attributes: IP Address, Serial Number (SN), Device Name, Device Model, Firmware Version

Objects: Logs, DLP archives, quarantined files, IPS Packet Logs

Security attributes: none].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *the TOE may receive data from a registered device if the device is authorized].*

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 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.

6.2.4.2 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.

FIA_UID.2.2 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(1) Management of security attributes (administrators)

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(1) The TSF shall enforce the [*administrative access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*username, access profile, Administrative Domain*] to [*Super Users*].

6.2.5.2 FMT_MSA.1(2) Management of security attributes (devices)

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(2) The TSF shall enforce the [*device access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Device Name*] to [*Super Users, Standard Users*].

6.2.5.3 FMT_MSA.3(1) Static attribute initialisation (administrator)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(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(1) The TSF shall allow the [*Super Users*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_MSA.3(2) Static attribute initialisation (devices)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*device access control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*Super Users*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 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 [*perform the operations identified in Table 14 on*] the [*TSF data identified in Table 14*] to [*authorized administrators identified in Table 14*].

TSF DATA	**Predefined Administrator Profile**		
	Super user	**Standard User**	**Restricted User**
System Settings	Read-Write	None	None
Administrative Domain	Read-Write	None	None
Device Manager	Read-Write	Read-Write	Read-Only
Add/Delete/Edit Devices/Groups	Read-Write	Read-Write	None
Log View/FortiView/SOC	Read-Write	Read-Write	Read-Only
Incidents & Events	Read-Write	Read-Write	Read-Only
Reports	Read-Write	Read-Write	Read-Only

Table 14 – Management of TSF Data

6.2.5.6 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: [*query the system status, adding/editing users and profiles, configure network settings, configure administrator related settings, configure local log storage and query features, perform system configuration backups, add or remove devices to be monitored by the TOE, manage the log and archive functionality, and configure and run reports*].

6.2.5.7 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 [*Restricted User, Standard User, and Super User*].

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_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 [a*dministrator-configurable time interval of session inactivity*].

6.2.7.2 FTA_SSL.4 User-initiated Termination

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

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

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 [another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel [*to receive logs, DLP archives, quarantined files, and IPS Packet Logs*].

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 [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 [*remote administration*].

6.2.9 Data Collection and Reporting (DCR)

6.2.9.1 DCR_AGG_EXT.1 Aggregation

Hierarchical to: No other components.

Dependencies: EXT_DCR_COL.1 Data Collection

DCR_AGG_EXT.1.1 The TSF shall be able to aggregate data collected from monitored devices for further analysis and reporting.

6.2.9.2 DCR_COL_EXT.1 Data Collection

Hierarchical to: No other components.

Dependencies: No dependencies.

DCR_COL_EXT.1.1 The TSF shall be able to collect the following information types from the targeted IT system resource(s): [*logs, DLP events, quarantined files, and IPS Packet Logs*].

6.2.9.3 DCR_QUA_EXT.1 Quarantine

Hierarchical to: No other components.

Dependencies: No dependencies.

DCR_QUA_EXT.1.1 The TOE shall be able to isolate selected data to a container controlled by the TSF where it may be downloaded and examined.

6.2.9.4 DCR_REP_EXT.1 Reporting

Hierarchical to: No other components.

Dependencies: EXT_DCR_AGG.1 Aggregation

DCR_REP_EXT.1.1 The TSF shall be able to apply a set of rules to the aggregated data to create reports relating to the following events, activities or patterns: [*bandwidth analysis, Admin and System Events Analysis, threat analysis, and web filtering activity*].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 15.

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 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 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 15 – 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.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.PROTECT	O.REPORT	O.TIME
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAA.1					X	X	
FAU_SAR.1	X	X					
FAU_STG.1		X					
FCS_COP.1			X				
FDP_ACC.1(1)	X				X		
FDP_ACC.1(2)						X	
FDP_ACF.1(1)	X				X		
FDP_ACF.1(2)						X	
FIA_UAU.2	X			X			
FIA_UID.2	X			X			
FMT_MSA.1(1)	X				X		
FMT_MSA.1(2)	X				X		
FMT_MSA.3(1)					X		
FMT_MSA.3(2)					X		
FMT_MTD.1	X				X		
FMT_SMF.1	X				X		
FMT_SMR.1				X	X		
FPT_STM.1							X
FTA_SSL.3					X		

	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.PROTECT	O.REPORT	O.TIME
FTA_SSL.4					X		
FTP_ITC.1			X				
FTP_TRP.1			X				
DCR_AGG_EXT.1						X	
DCR_COL_EXT.1						X	
DCR_QUA_EXT.1					X		
DCR_REP_EXT.1						X	

Table 16 – 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.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(1)	Subset access control (administrators)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FMT_MSA.1(1)	Management of security attributes (administrators)
	FMT_MSA.3(1)	Static attribute initialisation (administrators)
	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(1) and FDP_ACF.1(1) meet this objective by restricting access to the security data required to perform administrative functions. FMT_MSA.1(1) meets the objective by providing the functionality to manage the parameters associated with the administrative access control SFP. FMT_MSA.3(1) 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.	

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 review
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage

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_STG.1 ensures that the audit logs are protected against unauthorised modifications or deletion.

Objective: **O.ENCRYPT**	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_COP.1	Cryptographic operation
	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Rationale:	FCS_COP.1 supports this objective by providing the cryptographic functionality required to support trusted links. FTP_ITC.1 and FTP_TRP.1 support the objective by specifying the use of encryption between the TOE and the remote administrator, and between the TOE and the managed devices.	

Objective: **O.IDENTAUTH**	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.PROTECT**	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:	FAU_SAA.1	Potential violation analysis
Security Functional Requirements: **Rationale:**	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FMT_MSA.1(1)	Management of security attributes (administrators)
	FMT_MSA.1(2)	Management of security attributes (devices)
	FMT_MSA.3(1)	Static attribute initialisation (administrators)
	FMT_MSA.3(2)	Static attribute initialisation (devices)
	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
	FTA_SSL.4	User-initiated Termination
	DCR_QUA_EXT.1	Quarantine
	FAU_SAA.1 will ensure the monitoring of audited events will indicate any potential violation of SFR enforcement. FDP_ACC.1(1) and FDP_ACF.1(1) ensure the TOE data is protected by limiting data and administrative access to authorized administrators. FMT_MSA.1(2), and FMT_MSA.3(2) ensure the TOE device data is only accessible by authorized users on authorized devices. FMT_MSA.1(1), FMT_MSA.3(1), 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. 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. DCR_QUA_EXT.1 Supports this objective with the ability to isolate files to examine and delete if determined to be malicious.	

Objective: **O.REPORT**	The TOE must gather, analyze and create reports on all events indicating a breach in the policy related to use of the TOE or resources protected by the TOE.

Security Functional Requirements:	FAU_SAA.1	Potential violation analysis
	FDP_ACC.1(2)	Subset access control (devices)
	FDP_ACF.1(2)	Security attribute based access control (devices)
	DCR_AGG_EXT.1	Aggregation
	DCR_COL_EXT.1	Data Collection
	DCR_REP_EXT.1	Reporting
Rationale:	FAU_SAA.1 will ensure the monitoring of audited events will indicate any breach in the policy related to use of the TOE or resources protected by the TOE. FDP_ACC.1(2), FDP_ACF.1(2) ensure the TOE has access to the data and functions necessary to create reports. DCR_AGG_EXT.1, DCR_COL_EXT.1 and DCR_REP_EXT.1 support this objective by reporting on the data collected from the TOE and monitored devices by the TOE.	

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 17 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_SAA.1	FAU_GEN.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	FCS_CKM.1 is considered satisfied as per guidance from the Canadian Common Criteria Scheme.
	FCS_CKM.4	✓	FCS_CKM.4 is considered satisfied as per guidance from the Canadian Common Criteria Scheme.
FDP_ACC.1(1)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1)
FDP_ACF.1(2)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2)
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(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1)
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2)
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
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	
DCR_AGG_EXT.1	DCR_COL_EXT.1	✓	
DCR_COL_EXT.1	None	N/A	
DCR_QUA_EXT.1	None	N/A	
DCR_REP_EXT.1	DCR_AGG_EXT.1	✓	

Table 17 – 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 and access control decisions. The TOE records the time of the event, the identity of the administrator who caused the event and the details of the event. The administrator may review the audit records. The audit records are stored locally, cannot be modified, and may only be deleted by administrators with appropriate privileges. In addition to being time stamped, each audit record is also assigned a sequential event ID.

The TOE monitors the audit events and recognizes potential security violations based on the severity of an event or a number of events occurring within a pre-set time period. The number of events and the time period frequency can be configured by the administrator using event handlers. The TOE uses the aggregate audit events, and not just those generated by the TOE itself.

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

7.2 CRYPTOGRAPHIC SUPPORT

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. This generates cryptographic keys whose strengths are modified by available entropy. Entropy is provided using the Fortinet CPU Jitter Entropy Library to seed the DRBG during the boot process and to periodically reseed the DRBG. The entropy source for each hardware model can be found in Table(s) 2 & 4 above.

RSA asymmetric keys and Diffie-Hellman key exchange are used in support of TLS and SSH.

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_COP.1.

7.3 USER DATA PROTECTION

The TOE provides for two distinct access control SFPs – one for administrators and one for devices. Administrative users are granted access to data based on the permissions in their access profiles. Users may also be constrained by administrative domains, which are used to limit access privileges to a subset of devices or virtual domains. The TOE-monitored devices must first be registered

with the TOE in order to communicate with the TOE. These devices have the ability to send logs and quarantined files as granted by the TOE.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2).

7.4 IDENTIFICATION AND AUTHENTICATION

In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access to the web GUI and CLI. The identification and authentication mechanism is a username and password combination. The TOE maintains administrator accounts locally.

TOE Security Functional Requirements addressed: FIA_UAU.2 and 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 FortiAnalyzer administrative users, and review of audit records.

Management of the security attributes that control access to user management functions is limited to users who have been assigned the Super User profile. 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 remotely managed devices. Although all of the predefined profiles include some device manager privileges, users with Restricted 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 three 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. Restricted users are limited to read-only access to most data, and no access to the data related to system level functionality.

TSF Data	**Predefined Administrator Profile**		
	Super user	**Standard User**	**Restricted User**
System Settings	Read-Write	None	None

Administrative Domain	Read-Write	None	None
Device Manager	Read-Write	Read-Write	Read-Only
Add/Delete/Edit Devices/Groups	Read-Write	Read-Write	None
Log View/FortiView/SOC	Read-Write	Read-Write	Read-Only
Incidents & Events	Read-Write	Read-Write	Read-Only
Reports	Read-Write	Read-Write	Read-Only

Table 18 – Predefined Administrator Profiles

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.6 PROTECTION OF THE TSF

The TOE provides reliable timestamps for audit records using an internal clock that may be set by an authorized administrator. Audit records are generated for changes to the date and time.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.7 TOE ACCESS

An authorized administrator can configure the TOE to terminate inactive local and remote sessions following a specified period of time. In the evaluated configuration the timeout value is set to 10 minutes by default. Administrators may also terminate their own session at any time while using the web GUI or CLI.

TOE Security Functional Requirements addressed: FTA_SSL.3 and FTA_SSL.4.

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 1.2 and 1.3 are used to encrypt and authenticate administration sessions between the remote browser and TOE.

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.

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 devices. In the evaluated configuration, the managed devices always initiate the communication while the TOE acts as the server. The trusted channel provides security for communications between the TOE and the managed devices using TLS 1.2 or 1.3. 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.

TOE Security Functional Requirements addressed: FTP_ITC.1.

7.9 DATA COLLECTION AND REPORTING

The TOE has the ability to collect log information from a number of devices (including itself), aggregate that data, analyse it and provide reports. Additionally, the TSF is able to monitor the audit events (for itself and monitored devices) and recognize a potential security violation based on the severity of an event, or the number of events occurring within a pre-set time period. If necessary, the TOE can isolate files for download and examination in order to determine if they are malicious.

TOE Security Functional Requirements addressed: DCR_AGG_EXT.1, DCR_COL_EXT.1, DCR_QUA_EXT.1, and DCR_REP_EXT.1.

8 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CLI	Command Line Interface
DLP	Data Leak Prevention
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
IPS	Intrusion Prevention System
IT	Information Technology
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SN	Serial Number
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

Table 19 – Acronyms

9 ANNEX A – FORTIANALYZER MODELS AND GUIDES

Model	QuickStart/Information Supplement
FAZ-150G	Guide: FortiAnalyzer 150G QuickStart Guide File: FAZ-150G-QSG.pdf
FAZ-300F	Guide: FortiAnalyzer 300F QuickStart Guide File: FAZ-300F-QSG.pdf
FAZ-300G	Guide: FortiAnalyzer 300G QuickStart Guide File: FAZ-300G-QSG.pdf
FAZ-400E	Guide: FortiAnalyzer 400E QuickStart Guide File: FAZ-400E-QSG.pdf
FAZ-800F	Guide: FortiAnalyzer 800F QuickStart Guide File: FAZ-800F-QSG.pdf
FAZ-800G	Guide: FortiAnalyzer 800G QuickStart Guide File: FAZ-800G-QSG.pdf
FAZ-810G	Guide: FortiAnalyzer 810G QuickStart Guide File: FAZ-810G-QSG.pdf
FAZ-1000F	Guide: FortiAnalyzer 1000F QuickStart Guide File: FortiAnalyzer-1000F-QSG.pdf
FAZ-1000G	Guide: FortiAnalyzer 1000G QuickStart Guide File: FortiAnalyzer-1000G-QSG.pdf
FAZ-2000E	Guide: FortiAnalyzer 2000E QuickStart Guide File: FortiAnalyzer-2000E-QSG.pdf
FAZ-3000F	Guide: FortiAnalyzer 3000F QuickStart Guide File: FAZ-3000F-QSG.pdf
FAZ-3000G	Guide: FortiAnalyzer 3000G QuickStart Guide File: FAZ-3000G-QSG.pdf
FAZ-3100G	Guide: FortiAnalyzer 3100G QuickStart Guide File: FAZ-3100G-QSG.pdf
FAZ-3500E	Guide: FortiAnalyzer 3500E QuickStart Guide File: FAZ-3500E-QSG.pdf
FAZ-3500F	Guide: FortiAnalyzer 3500F QuickStart Guide File: FAZ-3500F-QSG.pdf

Model	QuickStart/Information Supplement
FAZ-3500G	Guide: FortiAnalyzer 3500G QuickStart Guide File: FAZ-3500G-QSG.pdf
FAZ-3510G	Guide: FortiAnalyzer 3510G QuickStart Guide File: FAZ-3510G-QSG.pdf
FAZ-3700F	Guide: FortiAnalyzer 3700F QuickStart Guide File: FortiAnalyzer-3700F-QSG.pdf
FAZ-3700G	Guide: FortiAnalyzer 3700G QuickStart Guide File: FortiAnalyzer-3700G-QSG.pdf

Table 20 - FortiAnalyzer Quick Start Guides