SECURITY TARGET

FOR

FORTIANALYZER™ V4.0 MR3 CENTRALIZED REPORTING

Document No. 1735-005-D0001

Version: 1.0, 3 June 2014

Prepared for:

Fortinet, Incorporated

326 Moodie Drive

Ottawa, Ontario

Canada, K2H 8G3

Prepared by:

Electronic Warfare Associates-Canada, Ltd.

1223 Michael Street, Second Floor

Ottawa, Ontario

K1J 7T2

SECURITY TARGET

FOR

FORTIANALYZER™ V4.0 MR3 CENTRALIZED REPORTING

Document No. 1735-005-D0001

Version: 1.0, 3 June 2014

<Original> Approved by:

Project Engineer:	Greg Lague	3 June 2014
Project Manager:	M. Gauvreau	3 June 2014
Program Director:	E. Connor	3 June 2014
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) 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 Information Technology (IT) environment.

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

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

1.2 SECURITY TARGET REFERENCE

This document, version 1.0, dated 3 June 2014, is the Security Target for the FortiAnalyzer™ v4.0 MR3 Centralized Reporting.

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation for this Security Target is identified in Table 1. The FortiAnalyzer™ v4.0 MR3 Centralized Reporting is a combined hardware and software TOE.

Product	Firmware Version	Hardware ID
FortiAnalyzer	v4.0 MR3 build 3059,130918	100C
		200D
		400B
		400C
		1000C
		2000B
		4000B

Table 1 - TOE Identification Details

1.4 TOE OVERVIEW

The TOE is a log collection and reporting device. FortiAnalyzer units are network appliances that provide integrated log collection and reporting tools. Logs for network traffic, email, File Transfer Protocol (FTP), web browsing, security events, and other network activity are analyzed to aid in the identification of security issues and to reduce network misuse and abuse.

In addition to logging and reporting, FortiAnalyzer units also have several features that augment or enable certain FortiGate unit functionalities, such as Data Leak Prevention (DLP) archiving and quarantining, and make information about the state of the network available to administrators.

- Logging and reporting: The FortiAnalyzer unit is able to aggregate and analyze log data from Fortinet and other Syslog-compatible devices. Customizable reports may be used to filter and review records, including traffic, event, virus, attack, Web content, and email data, mining the data to determine the security stance. This may be used to ensure regulatory compliance.

- DLP archiving: Both FortiGate DLP archive logs and their associated copies of files or messages may be stored on and viewed from a FortiAnalyzer unit. Data filtering may be used to track and locate specific email or instant messages, or to examine the contents of archived files.

- Quarantine repository: The FortiAnalyzer unit can act as a central repository for suspicious files, or files known to be infected by a virus.

- Vulnerability management: The FortiAnalyzer unit may be used to scan designated target hosts for known vulnerabilities and open Transmission Control Protocol (TCP) and/or User Datagram Protocol (UDP) ports. When the vulnerability scan is complete, the FortiAnalyzer unit generates a report that describes the discovered security issues and their known solutions. FortiAnalyzer may use the FortiGuard subscription service to update the vulnerability database. This functionality is not included in the evaluated version of the TOE.

• Packet capture: FortiAnalyzer units may be used to log observed packets to diagnose areas of the network where firewall policies may require adjustment, or where traffic anomalies occur.

• File explorer: An interface allows administrators to browse through the list of content archive/DLP, quarantine, log, and report files on the FortiAnalyzer unit.

Administration of the system may be performed locally through the Command Line Interface (CLI) using an administrator console or remotely via a remote administrator station through the FortiAnalyzer Web-based manager (https) or the CLI through an SSH connection. Access to the FortiAnalyzer administrative functions, including the viewing of audit data, is restricted to authenticated Administrators.

The FortiAnalyzer supports local authentication and authentication using Remote Authentication Dial In User Service (RADIUS). Administrators are authenticated locally in the evaluated version.

The FortiAnalyzer unit must be connected to the network with access to all of the devices to be monitored. FortiAnalyzer also supports Internet Protocol Security (IPSec) for encryption between the unit and the monitored devices. FortiAnalyzer also requires appropriate hardware and software to support the console or web-based/CLI administrative capabilities.

The TOE type is a log collection and reporting device.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

1.5.1.1 Physical Configuration

The FortiAnalyzer unit is a stand-alone appliance that does not require supporting hardware. The FortiAnalyzer unit consists of custom hardware and firmware, including the following major components: firmware, processor, memory, disk storage and I/O interfaces.

1.5.1.2 Physical Interfaces

The FortiAnalyzer unit has the interfaces defined in Table 2.

Product	Interfaces			
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-100C	Console	RJ-45	RS-232	Connection to the management computer. Provides access to the CLI
	PORT1 and PORT2	RJ-45	10/100/1000 Ethernet	Connection to the network
	PORT3	RJ-45	10/100 Ethernet	Connection to the network. The speed cannot be changed
	USB	USB		Two optional connections for the USB key, modem or

Product	Interfaces			
	Interface	**Type**	**Protocol**	**Purpose**
				backup operation
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-200D	PORT1, PORT2, PORT3, PORT4	RJ-45	1000 Ethernet	Network connection
	Console	RJ-45	RS-232	Optional connection to the management computer. Provides access to the CLI
	USB1 USB2	USB		Reserved for future use
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-400B	PORT1, PORT2, PORT3, PORT4	RJ-45	10/100/1000 Ethernet	Up to three connections to the internal network
	Console	RJ-45	RS-232	Optional connection to the management computer. Provides access to the CLI
	USB	USB		Reserved for future use
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-400C	PORT1, PORT2, PORT3, PORT4	RJ-45	10/100/1000 Ethernet	Up to three connections to the internal network
	Console	RJ-45	RS-232	Optional connection to the management computer. Provides access to the CLI
	USB	USB		Reserved for future use
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-1000C	PORT1, PORT2, PORT3 and PORT4	RJ-45	10/100/1000 Ethernet	Network connection
	USB	USB		Four optional connections reserved for future use
	Console	DB9	RS-232	Optional connection to the management computer. Provides access to the CLI
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-2000B	PORT1, PORT2, PORT3, and PORT4,	RJ-45	10/100 Ethernet	Network connection
	PORT5 and		1000 Ethernet	Network connection

Product	Interfaces			
	Interface	**Type**	**Protocol**	**Purpose**
	PORT6			
	USB	USB		Four optional connections reserved for future use
	Console	DB9	RS-232	Optional connection to the management computer. Provides access to the CLI
	Interface	**Type**	**Protocol**	**Purpose**
FortiAnalyzer-4000B	PORT1 and PORT2	RJ-45	10/100/1000 Ethernet	Network connection
	PORT3 and PORT4	small form-factor pluggable	1 Gbps/auto Ethernet	Small form-factor pluggable transceiver
	USB	USB		Two optional connections reserved for future use
	Console	DB9		Optional connection to the management computer. Provides access to the CLI
	Serial		RS-232 serial	Two serial ports connect a serial device to the system
	VGA			One port to connect to a monitor

Table 2 - FortiAnalyzer Interfaces

The FortiAnalyzer units may be securely administered over the external or internal networks or locally within the secure area. The FortiAnalyzer unit provides the following administration options:

- The FortiAnalyzer unit has a dedicated console (RS232 port with RJ-45 or DB9 connector). When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiAnalyzer unit via the CLI. This Local Console CLI permits an authenticated Administrator to configure the FortiAnalyzer unit, monitor its operation and examine the audit logs that are created.
- Remote administration may be performed via any network port that has been configured by an Administrator to allow Hypertext Transfer Protocol Secure (HTTPS) (for the Network Web-Based Graphical User Interface (GUI)) and SSH (for the Network CLI) traffic. When connected to a remote administrator station, this port provides remote access to the Network CLI or to the Network Web-Based GUI and allows an authenticated Administrator to configure the FortiAnalyzer unit, monitor its operation and examine the audit logs that are created.

1.5.1.3 Logging, Analyzing and Reporting Workflow

Figure 1 shows the logging, analyzing and reporting workflow of the FortiAnalyzer. These functions provide the basis of the TOE aggregation, analysis, and reporting functionality.

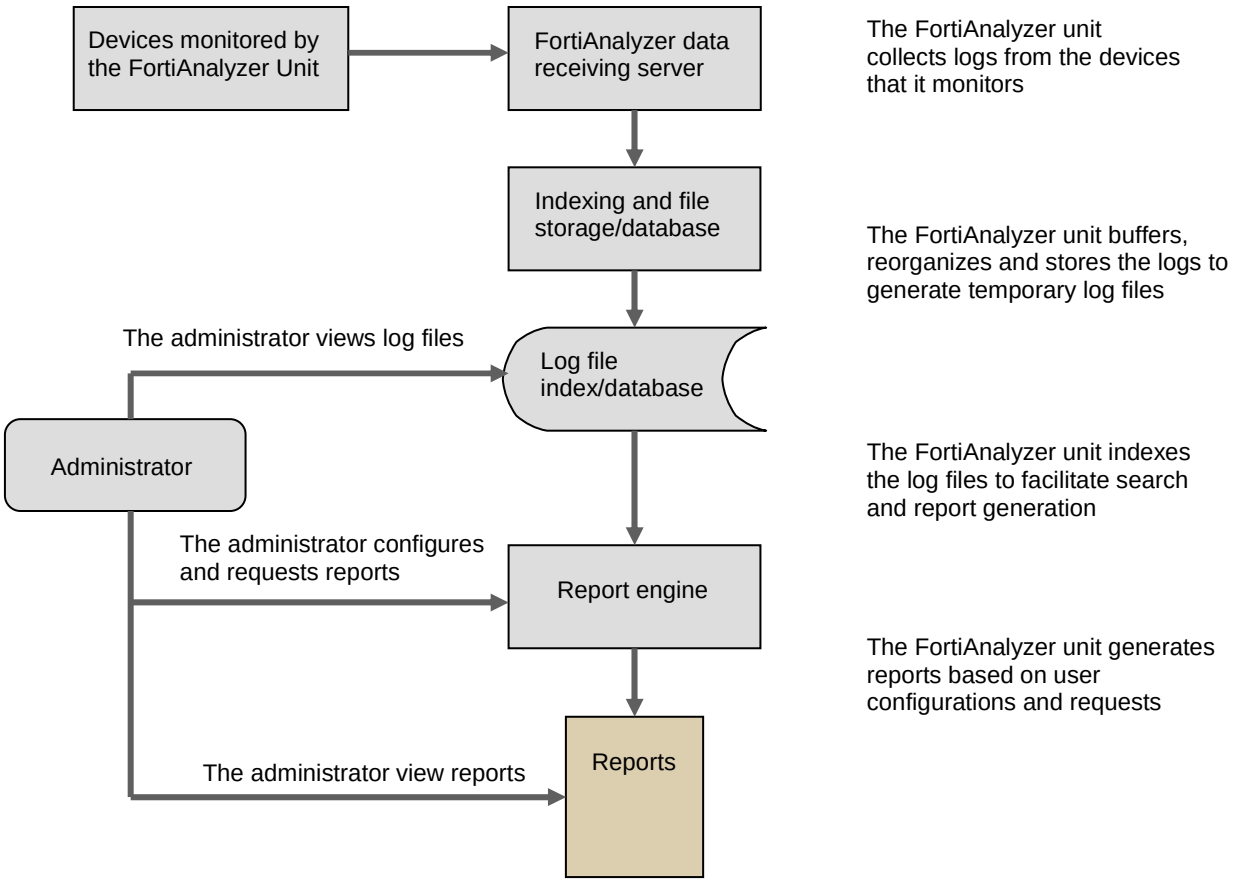


Figure 1 - FortiAnalyzer Logging, Analyzing and Reporting Workflow

1.5.1.4 TOE Environment

The FortiAnalyzer units are designed to be installed and used in an operational environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

1.5.1.5 Physical Boundary

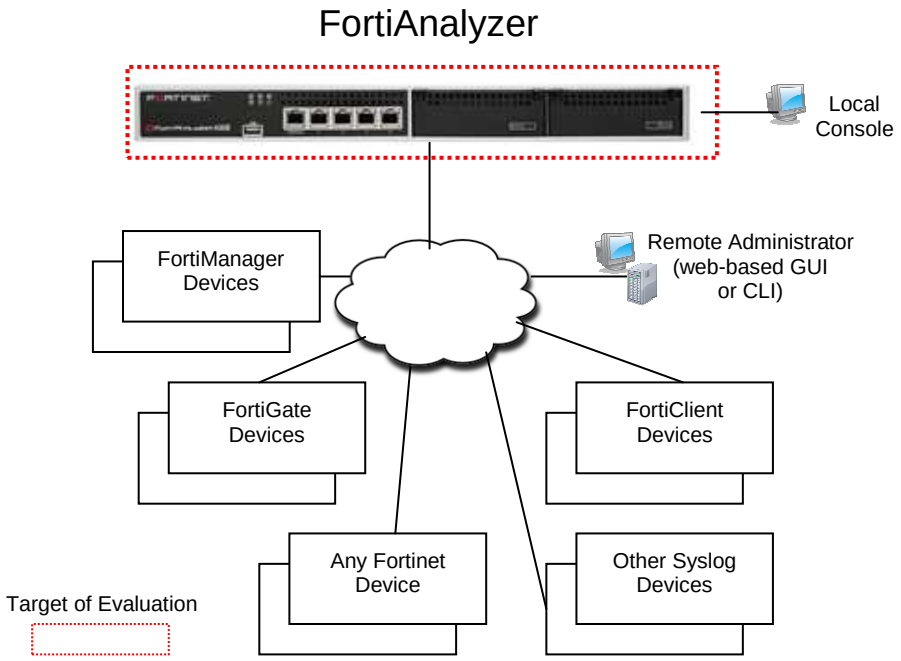


Figure 2 - FortiAnalyzer Deployment Configuration

Figure 2 shows the TOE in deployment configuration. The Local Console, located within a secure area, is a terminal or general purpose computer with a standard serial interface and optional ethernet interfaces. A serial port is used to administer the TOE via the Local Console CLI.

The Remote Administrator station is a terminal or general purpose computer with a standard network interface which is used to administer the TOE remotely using the Network Web-Based GUI or Network CLI.

1.5.1.5.1 Required Non-TOE Hardware / Software / Firmware

The TOE is a standalone appliance and does not require any non-TOE hardware, software, or firmware.

1.5.1.6 TOE Guidance Documentation

The following guidance documentation is an integral part of the TOE:

- FortiAnalyzer Administration Guide Version 4.0 MR3
- FortiAnalyzer CLI Reference Version 4.0 MR3
- FortiAnalyzer Log Message Reference Version 4.0 MR3
- FortiAnalyzer Install Guide Version 4.0 MR3

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. The following breakdown also provides the description of the security features of the TOE, and loosely follows the security functional classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs are stored in a protected from unauthorized modification and deletion and may be reviewed by authorized administrators. Timestamp information is provided to support auditing.
Protection (Cryptographic Support and Trusted Path/Channel)	Cryptographic functionality is provided to allow the communications links between the TOE and the monitored devices, and between the TOE and its remote administrators to be protected, as appropriate.
Access Control	The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE. Authorized administrators may be restricted to administering certain data types (specifically system data, network data, admin data, alerts data, devices data, log data, quarantine data, DLP archive data, and report data), for specific devices or virtual domains. Access by devices is limited to those registered with the TOE, and may be further limited by data type (logs, DLP archives, quarantined files, IPS Packet Logs, Reports) and disk allocation limits.
Identification and Authentication	Users must identify and authenticate prior to TOE access.
Security Management	The TOE provides management capabilities via a text-based Local Console CLI, via a text-based Network CLI interface, and via a Network Web-Based GUI, accessed via HTTPS. Management functions allow the administrators to configure system and network settings (including connections to monitored devices), configure log storage and query features, perform backups, manage the log and archive functionality, and configure and browse reports.
Data Collection and Reporting	Data is collected from monitored devices, aggregated and analyzed. Based on that analysis, potential violations may be identified, alarms may be raised and reports may be generated.

Table 3 - Logical Scope of the TOE

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, CCMB-2006-09-001 July 2009 Revision 3, CCMB-2009-07-002 July 2009 Revision 3 and CCMB-2007-09-003 July 2009 Revision 3.

The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in Part 2, as well as any explicitly-defined functional requirements. The Target of Evaluation (TOE) for this ST, the FortiAnalyzer™ v4.0 MR3 Centralized Reporting, is therefore conformant with CC Part 2 extended.

The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 2, augmented with ALC_FLR.1 Basic flaw remediation.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS, POLICIES AND ASSUMPTIONS

3.1.1 Threats

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

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.BYPASS	A user may bypass the organization's policy resulting in breaches of regulations.
T.LACKDATA	Unauthorized users may initiate widespread attacks on the system, which may go unnoticed due to a lack of data.
T.COMPDATA	An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by circumventing security.

3.1.2 Organizational Security Policies

The TOE must address the organizational security policies described below.

P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall be managed only by authorized users.

3.1.3 Assumptions

The following specific conditions are assumed to exist in the TOE operational environment.

A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.ACCESS	The TOE is connected to the network in such a way that it is able to access all of the monitored resources.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). The mapping of security objectives to assumptions, threats and organizational security policies along with the rationale for this mapping is found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE and its environment.

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
O.REPORT	The TOE must gather, analyze, provide appropriate response and create reports on all events indicating a breach in the policy related to use of the resources protected by the TOE.
O.SECURE	The TOE must ensure the security of all audit and system data.
O.TIME	The TOE must provide reliable timestamps.
O.TRUST	The TOE will maintain a mechanism for transmitting select data in a trusted manner.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.AVAIL	The TOE environment must ensure that the monitored network is available and accessible to the TOE at all times.

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.PRIVILEGE	T.BYPASS	T.LACKDATA	T.COMPDATA	P.ACCOUNT	P.INTEGRITY	P.MANAGE	A.LOCATE	A.MANAGE	A.ACCESS	A.NOEVIL
O.ACCESS				X			X				
O.AUDIT			X		X						
O.IDENTAUTH	X			X	X		X				
O.ADMIN	X						X				
O.PROTECT	X	X				X					
O.SECURE	X	X				X					
O.REPORT	X	X	X								
O.TIME		X	X								
O.TRUST				X							
OE.PERSON									X		X
OE.PHYSICAL								X			
OE.AVAIL										X	

Table 4 - Mapping Between Objectives, Threats, Organizational Security Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
	O.SECURE	The TOE must ensure the security of all audit and system data.
	O.REPORT	The TOE must gather, analyze, provide appropriate response and create reports on all events indicating a breach in the policy related to use of the resources protected by the TOE.
Rationale:	O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. O.PROTECT mitigates this threat by ensuring the integrity of system and audit data. O.PROTECT mitigates this threat by ensuring that system and audit data are not accessible. O.SECURE mitigates the threat by ensuring that system data is protected. O.REPORT helps to detect this threat, and respond appropriately.	
Threat: T.BYPASS	A user may bypass the organization's policy resulting in breaches of regulations.	
Objectives:	O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
	O.SECURE	The TOE must ensure the security of all audit and system data.

	O.REPORT	The TOE must gather, analyze, provide appropriate response and create reports on all events indicating a breach in the policy related to use of the resources protected by the TOE.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.PROTECT mitigates this threat by protecting the integrity of the audit data that provides evidence of any irregularities. O.SECURE ensures that the system and audit data are secure, so that it may be used to provide evidence of a policy breach. O.REPORT provides for the reports that point to any breach in policy, and where appropriate, the response. O.TIME ensures that audit and report data are supported with accurate time information.	
Threat: T.LACKDATA	Unauthorized users may initiate widespread attacks on the system, which may go unnoticed due to a lack of data.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	O.REPORT	The TOE must gather, analyze, provide appropriate response and create reports on all events indicating a breach in the policy related to use of the resources protected by the TOE.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT mitigates this threat by ensuring the provision of the data that may be used to discover an assault on the protected system. O.REPORT provides for the reports that will uncover an attack on the system. O.TIME ensures that audit and report data are supported with accurate time information.	
Threat: T.COMPDATA	An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by circumventing security.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the

		TOE.
	O.TRUST	The TOE will maintain a mechanism for transmitting select data in a trusted manner.
Rationale:	O.ACCESS ensures that only authorized users have access to the TOE functions and data. O.IDENTAUTH restricts access to authorized users by allowing access only after proper identification and authorization has been verified. O.TRUST ensures that data is appropriately protected in transit.	

4.3.2 Security Objectives Rationale Related to Organizational Security Policies

Policy: P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.IDENTAUTH supports this policy by ensuring that the TOE has a clear identity for any user granted access to TOE functionality. O.AUDIT ensures that the use of the TOE is recorded. This may be used to provide evidence of a user's actions.	
Policy: P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.	
Objectives:	O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
	O.SECURE	The TOE must ensure the security of all audit and system data.
Rationale:	O.PROTECT supports this policy by preventing unauthorized access which could allow the integrity of the system or audit data to be compromised. O.SECURE further protects the security of the audit and system data.	
Threat: P.MANAGE	The TOE shall be managed only by authorized users.	

Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
Rationale:	O.ACCESS supports this policy by restricting authorized users to the functions and data to which they have been granted access. O.IDENTAUTH ensures that only credentialed users have access to the TOE. O.ADMIN ensures that access to the security functions of the TOE are restricted to authorized users.	

4.3.3 Security Objectives Rationale Related to Assumptions

Assumption: A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	
Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that trained individuals are in place to manage the TOE.	
Assumption: A.ACCESS	The TOE is connected to the network in such a way that it is able to access all of the monitored resources.	

Objectives:	OE.AVAIL	The TOE environment must ensure that the monitored network is available and accessible to the TOE at all times
Rationale:	OE.AVAIL supports this assumption by ensuring the availability of the network being monitored.	
Assumption: A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that the individuals managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

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

a. Aggregation (EXT_DCR_AGG.1);

b. Data Collection (EXT_DCR_COL.1);

c. Quarantine (EXT_DCR_QUA.1); and

d. Reporting (EXT_DCR_REP.1).

5.1 CLASS EXT_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 collection, aggregation, quarantine and reporting. The Data Collection and Reporting class was modelled after the classes FAU: Security audit and FDP: User data protection. Aggregation (EXT_DCR_AGG.1) was modelled after FDP_SDI.1 Stored data integrity monitoring. Data Collection (EXT_DCR_COL.1) was modelled after FAU_GEN.1 Audit data generation. Quarantine (EXT_DCR_QUA.1) was modelled after FDP_SDI.1 Stored data integrity monitoring. Reporting (EXT_DCR_REP) was modelled after FAU_SAA.1 Potential violation analysis. Component levelling is shown in Figure 3.

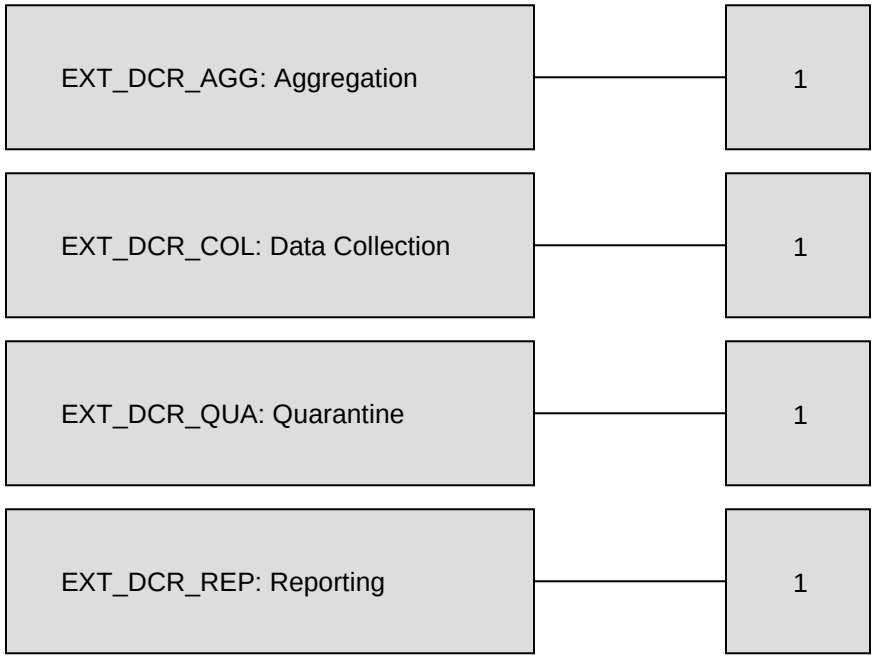


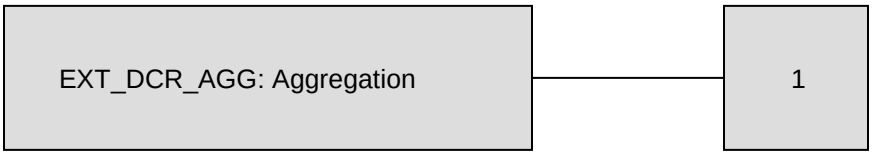
Figure 3 - EXT_DCR: Data Collection and Reporting Class Decomposition

5.1.1 EXT_DCR_AGG 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



Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

EXT_DCR_AGG.1 Data Aggregation

Hierarchical to: No other components

Dependencies: EXT_DCR_COL.1 Data Collection

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

5.1.2 EXT_DCR_COL 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

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.

EXT_DCR_COL Data Collection

Hierarchical to: No other components

Dependencies: No dependencies

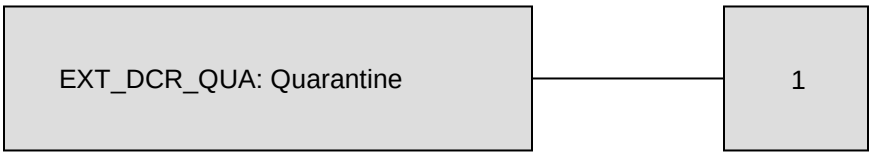
EXT_DCR_COL.1.1 The TSF shall be able to collect the following information types from the targeted IT system resource(s): [assignment: *information types*].

5.1.3 EXT_DCR_QUA Quarantine

Family Behaviour

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

Component Levelling



Management

There are no management activities foreseen.

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.)

EXT_DCR_QUA Quarantine

Hierarchical to: No other components

Dependencies: No dependencies

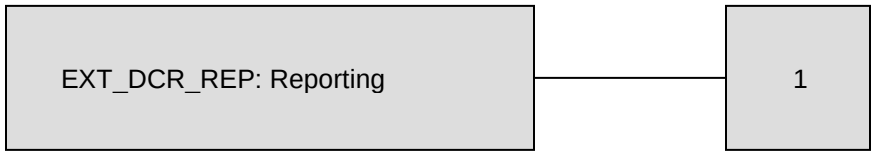
EXT_DCR_QUA.1.1 The TOE shall be able to isolate selected data to a container controlled by the TSF where it may be examined, deleted or restored.

5.1.4 EXT_DCR_REP 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



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.

EXT_DCR_REP Reporting

Hierarchical to: No other components

Dependencies: EXT_DRC_AGG.1 Aggregation

EXT_DCR_REP.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]. To improve readability selections of [none] are generally not shown.
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown.
- Refinement: Refined components are identified by using underlining 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 TOE 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 5 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_ARP.1	Security audit automatic response
	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_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACC.1(2)	Subset access control (devices)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FDP_ACF.1(2)	Security attribute based access control (devices)
Identification and Authentication (FIA)	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
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_STM.1	Reliable time stamps
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Data Collection and Reporting (EXT_DCR)	EXT_DCR_AGG.1	Aggregation
	EXT_DCR_COL.1	Data Collection
	EXT_DCR_QUA.1	Quarantine
	EXT_DCR_REP.1	Reporting

Table 5 - Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall ~~take~~ [*send a notification to an email address, SNMP trap or Syslog server*] upon detection of a potential security violation.

6.2.1.2 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 6*].

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

d) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
e) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*information specified in Table 6 Auditable Events*.]

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1	Action taken due to detection	Condition that was matched and message details
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_STG.1	None	
FCS_CKM.1	Failure of the activity	
FCS_CKM.4	None	
FCS_COP.1	Failure of the cryptographic operation	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information

Requirement	Auditable Events	Additional Audit Record Contents
FDP_ACC.1(1)	None	
FDP_ACC.1(2)	None	
FDP_ACF.1(1)	Successful requests to apply the administrator access control SFP[1]	
FDP_ACF.1(2)	Successful requests to apply the device access control SFP[2]	
FIA_UAU.1	Use of the authentication mechanism	Claimed identity of the user
FIA_UID.1	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	Modifications to the TSF data	The identity of the Administrator performing the function
FMT_SMF.1	Use of any of the management functions	
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	
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	Identification of the initiator and target of all

[1] The administrator access control SFP controls administrator access to the TOE.

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

Requirement	Auditable Events	Additional Audit Record Contents
	trusted path functions	trusted channels
EXT_DCR_AGG.1	No additional entries	
EXT_DCR_COL.1	No additional entries	
EXT_DCR_QUA.1	Quarantine event	Source of data being quarantined
EXT_DCR_REP.1	No additional entries	

Table 6 - Auditable Events

6.2.1.3 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.

6.2.1.4 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*].

6.2.1.5 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.

6.2.1.6 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)

The FortiAnalyzer FIPS evaluation for FortiAnalyzer is a FIPS 140-2 Level 1 validation for the OS/firmware and a FIPS 140-2 Level 2 validation for the FortiAnalyzer 4000B platform. The Cryptographic Module Validation Program (CMVP) certificate numbers are #2105 and #2115 respectively.

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*FIPS-approved Random Number Generator ANSI X9.31 Appendix A.2.4*] and specified cryptographic key sizes [*listed in Table 7*] that meet the following: [*standards listed in Table 7*].

Key Usage	Key Size	Standard	Cryptographic Algorithm Validation Program (CAVP) Certificate Number
Symmetric Cryptography			
AES	128, 192 or 256	FIPS 197	2681
Triple-DES	168	FIPS 46-3	1608, 1609
Asymmetric Cryptography			
RSA	2048	PKCS1	1030

Table 7 - Cryptographic Key Generation

6.2.2.2 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 [*keys are zeroized when a factory reset is performed via the CLI (local console or remote)*] that meets the following: [*FIPS PUB 140-2 Key Management Security Level 1*].

6.2.2.3 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 8*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 8*] and cryptographic key sizes [*cryptographic key sizes specified in Table 8*] that meet the following: [*standards listed in Table 8*].

Operation	Algorithm	Key Size or Digest Length	Standard	CAVP Certificate Number
Encryption and Decryption	Triple-DES	168	FIPS 46-3	1608, 1609
	AES	128, 192, 256	FIPS 197	2681
Message authentication coding	HMAC SHA-1 HMAC SHA-256	160	FIPS 198	1667, 1668
Hashing	SHA-1 SHA-2	160	FIPS 180-3	2251, 2252
Random Number Generation	ANSI X9.31 Appendix A	2048	ANSI X9.31 Appendix A.2.4	1251
Digital Signatures	RSA	2048	PKCS1	1030

Table 8- 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: Security data

Operations: read only, read/write]

Application Note: Security data refers to system data, network data, admin data, alert data, devices data, log data, quarantine data, DLP archive data, and reports.

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(2).1 The TSF shall enforce the [*device access control SFP*] on [

Subjects: devices

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

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

Objects: Security data

Security attributes

Data type (system, network, admin, alerts, devices, logs, quarantine, DLP archive, report).]

FDP_ACF.1(1).2 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 security data if the administrator's access profile contains the permission to perform that function for that data type*].

FDP_ACF.1(1).3 The TSF shall explicitly authorize access of subject to objects based on the following additional rules: [*the administrator is the admin administrator (default administrator account)*].

FDP_ACF.1(1).4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*Administrative domain, which may be used to constrain access privileges to a subset of devices or virtual domains*].

Application note: Administrative domains may be used with the FortiAnalyzer 400B, 400C and 4000B models, but not the 100C.

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(2).1 The TSF shall enforce the [*device access control SFP*] to objects based on the following: [

Subjects: devices

Security attributes

Registered device indication

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

Security attributes

Data type]

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 device privileges have been established for that data type*].

FDP_ACF.1(2).3 The TSF shall explicitly authorize access of subject to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1(2).4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*the disk allocation limit has been reached and the action indicated is 'Stop Logging'*].

Application Note: The 'data type' in this case, is the data type of the object, i.e. DLP archive, quarantined file, IPS Packet log, or Report. All of these data types would be available if the registered device was running FortiGate firmware 4.0 or later. Fewer data type options are available for other device types.

6.2.3.5 Iteration Rationale

Two iterations of FDP_ACC.1 and FDP_ACF.1 were included to address access control for both administrators and devices.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is authenticated.

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

6.2.4.2 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 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 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access 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 [query, modify, delete] the security attributes [*access profile*] to [*authorized administrators*].

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 [*no one*] 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 [*perform the operations identified in Table 9 on*] the [*TSF data identified in Table 9*] to [*authorized administrators*].

Operation	TSF Data
Read only, read/write	System setting data
Read only, read/write	Network configuration data
Read only, read/write	Admin data
Read only, read/write	Alerts
Read only, read/write	Device data
Read only, read/write	Logs
Read only, read/write	Quarantine
Read only, read/write	DLP Archive
Read only, read/write	Reports

Table 9 - Management of TSF Data

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 [*query the system status (using the dashboard and widgets), configure network settings, configure network shares, configure administrator related settings, configure log storage and query features, perform backups, configure connections to devices monitored by the TOE, manage the log and archive functionality, and configure and browse reports*].

6.2.5.5 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 [*admin administrator and other administrators with customizable access profiles*].

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 Trusted path/channels (FTP)

6.2.7.1 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 ~~for~~ [*to transmit or receive logs, DLP archives, quarantined files, IPS Packet Logs, and Reports, where this data would otherwise traverse an untrusted network*].

6.2.8 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 [initial user authentication, *use of the Command Line Interface, use of the web-based management interface*].

6.2.9 Data Collection and Reporting (EXT_DCR)

6.2.9.1 EXT_DCR_AGG.1 Aggregation

Hierarchical to: No other components.

Dependencies: EXT_DCR_COL.1 Data Collection

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

6.2.9.2 EXT_DCR_COL.1 Data Collection

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_DCR_COL.1.1 The TSF shall be able to collect the following information types from the targeted IT system resource(s): [*log data, DLP archive files, quarantine files, IPS Packet Data, Reports*].

Application Note: Reports are generated rather than collected.

6.2.9.3 EXT_DCR_QUA.1 Quarantine

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_DCR_QUA.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.

6.2.9.4 EXT_DCR_REP.1 Reporting

Hierarchical to: No other components.

Dependencies: EXT_DRC_AGG.1 Aggregation

EXT_DCR_REP.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, forensic analysis, threat analysis, and web filtering activity*].

6.3 SECURITY REQUIREMENTS RATIONALE

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

	O.ACCESS	O.AUDIT	O.IDENTAUTH	O.ADMIN	O.PROTECT	O.REPORT	O.SECURE	O.TIME	O.TRUST
FAU_ARP.1						X			
FAU_GEN.1		X							
FAU_GEN.2		X							
FAU_SAA.1						X			
FAU_SAR.1		X							
FAU_STG.1		X			X		X		
FCS_CKM.1									X
FCS_CKM.4									X
FCS_COP.1									X
FDP_ACC.1(1)	X		X		X		X		
FDP_ACC.1(2)					X		X		
FDP_ACF.1(1)	X		X		X		X		
FDP_ACF.1(2)					X		X		
FIA_UAU.1	X		X						
FIA_UID.1	X		X						
FMT_MSA.1			X	X	X				
FMT_MSA.3			X						
FMT_MTD.1			X	X					
FMT_SMF.1				X					
FMT_SMR.1			X	X					
FPT_STM.1								X	

	O.ACCESS	O.AUDIT	O.IDENTAUTH	O.ADMIN	O.PROTECT	O.REPORT	O.SECURE	O.TIME	O.TRUST
FTP_ITC.1									X
FTP_TRP.1									X
EXT_DCR_AGG.1						X			
EXT_DCR_COL.1		X				X			
EXT_DCR_QUA.1					X				
EXT_DCR_REP.1						X			

Table 10 - Mapping of SFRs to Security Objectives

6.3.1 Security Functional Requirements Rationale Related to Security Objectives

Table 11 shows the Security Functional Requirements Rationale related to Security Objectives.

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
Rationale:	FIA_UAU.1 and FIA_UID.1 support this objective by ensuring that users are identified and authenticated prior to access. FDP_ACC.1(1) and FDP_ACF.1(1) ensure that access to functions and data are strictly controlled.	
Objective: O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected audit trail storage

	EXT_DCR_COL.1	Data Collection
Rationale:	FAU_GEN.1 and FAU_GEN.2 support the creation of audit records. FAU_STG.1 ensures that they are protected. FAU_SAR.1 ensures that the records are usable, in that they may be read. EXT_DCR_COL.1 supports the collection of audit data from monitored devices.	
Objective: O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMR.1	Security roles
	FMT_MTD.1	Management of TSF data
Rationale:	FIA_UID.1 and FIA_UAU.1 support the identification and authentication of users, respectively. FDP_ACC.1(1) and FDP_ACF.1(1) control access to administrative functions. FMT_MSA.1 restricts access to security data, and FMT_MSA.3 provides restrictive default values. FMT_SMR.1 allows for roles to be used, and FMT_MTD.1 allows access to be controlled based on those roles.	
Objective: O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MTD.1	Management of TSF data
	FMT_SMR.1	Security roles
	FMT_SMF.1	Specification of management functions
Rationale:	FMT_SMF.1 ensures that management functions exist to support the management of the TOE. FMT_SMR.1 supports FMT_SMF.1 by allowing for the administrative roles to be used, and FMT_MTD.1 allows access to be controlled based on those roles. FMT_MSA.1 further supports this objective by restricting access to security data.	

Objective: O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.	
Security Functional Requirements:	FAU_STG.1	Protected audit trail storage
	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACC.1(2)	Subset access control (devices)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FDP_ACF.1(2)	Security attribute based access control (devices)
	FMT_MSA.1	Management of security attributes
	EXT_DCR_QUA.1	Quarantine
Rationale:	FAU_STG.1 protects the audit data from unauthorized modification or deletion. FDP_ACC.1(1) and FDP_ACF.1(1), and FDP_ACC.1(2) and FDP_ACF.1(2) protect the TOE from access by unauthorized administrators and devices, respectively. FMT_MSA.1 restricts access to data to authorized administrators. EXT_DCR_QUA.1 allows for files to be isolated, thereby protecting the system from potentially malicious files.	
Objective: O.REPORT	The TOE must gather, analyze, provide appropriate response and create reports on all events indicating a breach in the policy related to use of the resources protected by the TOE.	
Security Functional Requirements:	FAU_ARP.1	Security alarms
	FAU_SAA.1	Potential violation analysis
	EXT_DCR_AGG.1	Aggregation
	EXT_DCR_COL.1	Data collection
	EXT_DCR_REP.1	Reporting
Rationale:	EXT_DCR_COL.1 supports the collection of data; EXT_DCR_AGG.1 supports the aggregation of that data, and FAU_SAA.1 allows for analysis of that data to discover potential violations. FAU_ARP.1 allows for a response on detection of a potential security violation, and EXT_DCR_REP.1 supports the creation of reports.	
Objective: O.SECURE	The TOE must ensure the security of all audit and system data.	

Security Functional Requirements:	FAU_STG.1	Protected audit trail storage
	FDP_ACC.1(1)	Subset access control (administrators)
	FDP_ACC.1(2)	Subset access control (devices)
	FDP_ACF.1(1)	Security attribute based access control (administrators)
	FDP_ACF.1(2)	Security attribute based access control (devices)
Rationale:	FAU_STG.1 supports the security of audit data by ensuring that it is protected from unauthorized modification and deletion. FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), and FDP_ACF.1(2), ensure the protection of data objects by controlling access to these objects.	
Objective: O.TIME	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 ensures the provision of reliable timestamps.	
Objective: O.TRUST	The TOE will maintain a mechanism for transmitting select data in a trusted manner.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Rationale:	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 provide for the cryptography required to support trusted communications. FTP_ITC.1 supports trusted communications, where required, between devices, including those required to meet the content archive requirements. FTP_TRP.1 supports trusted communications between users and the TOE, where required.	

Table 11 - Security Functional Requirements Rationale

6.4 DEPENDENCY RATIONALE

Table 12 - Functional Requirement Dependencies 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	Dependencies	Dependency Satisfied?
FAU_ARP.1	FAU_SAA.1	Yes
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes
FAU_SAA.1	FAU_GEN.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Yes
FCS_CKM.4	FCS_CKM.1	Yes
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Yes
FDP_ACC.1(1)	FDP_ACF.1	Yes
FDP_ACC.1(2)	FDP_ACF.1	Yes
FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	Yes
FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	Yes
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes

SFR	Dependencies	Dependency Satisfied?
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	None	Yes
FTP_ITC.1	None	Yes
FTP_TRP.1	None	Yes
EXT_DCR_AGG.1	EXT_DCR_COL.1	Yes
EXT_DCR_COL.1	None	Yes
EXT_DCR_QUA.1	None	Yes
EXT_DCR_REP.1	EXT_DCR_AGG.1	Yes

Table 12 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Basic Flaw Remediation (ALC_FLR.1). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.1 augmentation since there are a number of areas where current Fortinet practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in the Table 13 - EAL 2 Assurance Requirements.

Assurance Class	Assurance Components	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures

Assurance Class	Assurance Components	
	Identifier	**Name**
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target Evaluation	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_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 13 - EAL 2 Assurance Requirements

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 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

The TOE creates audit records for administrative events, and access control decisions. The TOE records time of the event, the identity of the administrator or user who caused the event and details of the event as they occur. The administrator may review the audit records. The audit records are stored locally. Audit records cannot be modified and may only be deleted by the administrators with appropriate privileges. In addition to being time stamped, each audit record is also assigned a sequential event ID. The TOE provides reliable timestamps using an internal clock that may be set by an administrator. Changes to the date/time are audited.

The TSF is able to monitor the audit events and recognize a potential security violation based on the severity of an event, or a number of events occurring within a preset time period. Upon detection of a potential security violation, the TSF may be configured to send a notification to an email address, and SNMP trap or a Syslog server. For these two functions, the TSF uses the aggregate audit events, and not just those generated by the TOE itself.

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

7.1.2 Protection (Cryptographic Support and Trusted Path/Channel)

The TOE maintains an isolated security domain for its own execution. No other applications may be loaded onto the TOE. Administrators and users do not have access to the operating system or the file system (i.e. there are no root/system level users). The TOE stores all security and configuration data in segregated configuration files. The TOE also provides a quarantine storage area to isolate potentially dangerous files for examination. The TOE only provides identification, authentication and access control services to administrative users. The TOE uses cryptography to ensure the integrity and privacy of data transmitted between devices and between administrative users and devices.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, EXT_DCR_QUA.1, FTP_ITC.1, and FTP_TRP.1

7.1.3 User Data Protection

The TOE provides for two distinct access control TSFs – 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 devices that are monitored by the TOE must first be registered with the TOE in order to communicate with the TOE. Communications with other devices may be further restricted by data type and disk allocation

limits. Communications between devices may be encrypted, where this is considered appropriate. For example, transmission of content archive data may be encrypted.

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

7.1.4 Identification and Authentication

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

TOE Security Functional Requirements addressed: FIA_UAU.1 and FIA_UID.1.

7.1.5 Security Management

Administration may be performed locally through the console using the CLI, or through the web-based GUI. Remote administration may also be conducted through the CLI or web-based GUI. Communications between the TOE and remote administrators are protected by an encrypted path.

Administrative access to the TOE is restricted to authorized administrators and is controlled through defined roles and access profile information. When a new user is created, that user does not have administrative privileges until those privileges are specifically granted. Access must be specifically granted to read from and/or write to System setting data, Network configuration data, Admin data, Alerts, Device data, Logs, Quarantined data, DLP Archive files, and Reports.

The TOE provides administrators with the ability to query the system status (using the dashboard and widgets), configure network settings, configure network shares, configure administrator related settings, configure log storage and query features, perform backups, configure connections to devices monitored by the TOE, manage the log and archive functionality, and configure and browse reports.

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

7.1.6 Data Collection and Reporting

The TOE has the ability to collect log information from a number of devices, aggregate that data, analyse it and provide reports. Additionally, the TSF is able to monitor the audit events and recognize a potential security violation based on the severity of an event, or the number of events occurring within a preset time period. Upon detection of a potential security violation, the TSF may be configured to send a notification to an email address, an SNMP trap or a Syslog server.

TOE Security Functional Requirements addressed: EXT_DCR_AGG.1, EXT_DCR_COL.1, EXT_DCR_REP.1, FAU_ARP.1 and FAU_SAA.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Admin administrator	This is the default administrator account. All administrative permissions have been granted to this account, and this account may not be deleted.
Quarantine	Data is quarantined when it is isolated within a controlled container from where it may be examined, deleted or restored.
Syslog	Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
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
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
NTP	Network Time Protocol

PKCS	Public-Key Cryptography Standards
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest, Shamir and Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Secure Network Mail Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
USB	Universal Serial Bus