WatchGuard Firebox Security Appliances with Fireware v11.11 Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 1917-000-D102
Version: 1.3
17 October 2016

WatchGuard Technologies Inc.
505 Fifth Ave South, Suite 500
Seattle, Washington, USA
98104

Prepared by:

Electronic Warfare Associates - Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

1 SECURITY TARGET INTRODUCTION 1
1.1 DOCUMENT ORGANIZATION 1
1.2 SECURITY TARGET REFERENCE 1
1.3 TOE REFERENCE 2
1.4 TOE OVERVIEW 2
1.5 TOE DESCRIPTION 2
1.5.1 Physical Scope 2
1.5.2 Logical Scope 7
1.5.3 Functionality Excluded from the Evaluated Configuration 8
2 CONFORMANCE CLAIMS 9
2.1 COMMON CRITERIA CONFORMANCE CLAIM 9
2.2 EVALUATION ASSURANCE LEVEL 9
2.3 PROTECTION PROFILE CONFORMANCE CLAIM 9
3 SECURITY PROBLEM DEFINITION 10
3.1 THREATS 10
3.1.1 Threats Addressed by the TOE 10
3.2 ORGANIZATIONAL SECURITY POLICIES 11
3.3 ASSUMPTIONS 11
4 SECURITY OBJECTIVES 12
4.1 SECURITY OBJECTIVES FOR THE TOE 12
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 13
4.3 SECURITY OBJECTIVES RATIONALE 13
4.3.1 Security Objectives Rationale Related to Threats 14
4.3.2 Security Objectives Rationale Related to OSPs 18
4.3.3 Security Objectives Rationale Related to Assumptions 20
5 EXTENDED COMPONENTS DEFINITION 22
5.1 SECURITY FUNCTIONAL REQUIREMENTS 22
5.2 SECURITY ASSURANCE REQUIREMENTS 22
6 SECURITY REQUIREMENTS 23
6.1 CONVENTIONS 23

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 23
6.2.1 Security Audit (FAU) 24
6.2.2 Cryptographic Support (FCS) 26
6.2.3 User Data Protection 27
6.2.4 Identification and Authentication (FIA) 29
6.2.5 Security Management 30
6.2.6 Protection of the TSF 31
6.2.7 Trusted Path/Channels 31
6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 31
6.3.1 SFR Rationale Related to Security Objectives 32
6.3.2 Dependency Rationale 36
6.4 TOE SECURITY ASSURANCE REQUIREMENTS 37
7 TOE SUMMARY SPECIFICATION 39
7.1 TOE SECURITY FUNCTIONS 39
7.1.1 Security Audit 39
7.1.2 Cryptographic Support 40
7.1.3 User Data Protection 41
7.1.4 Identification and Authentication 42
7.1.5 Security Management 43
7.1.6 Protection of the TSF 44
7.1.7 Trusted Path/Channels 44
8 TERMINOLOGY AND ACRONYMS 45
8.1 TERMINOLOGY 45
8.2 ACRONYMS 45

LIST OF TABLES

Table 1 – TOE Instances 3
Table 2 – Non-TOE Hardware and Software 6
Table 3 - TOE Guidance Documentation 7
Table 4 – Logical Scope of the TOE 8
Table 5 – Security Threats 11
Table 6 – Organizational Security Policies 11

Table 7 – Assumptions 11
Table 8 – Security Objectives for the TOE 13
Table 9 – Security Objectives for the Operational Environment 13
Table 10 – Mapping Between Objectives and Threats, Policies, and Assumptions 14
Table 11 – Summary of Security Functional Requirements 24
Table 12 – Auditable Events 25
Table 13 – Cryptographic Key Generation 26
Table 14 – Cryptographic Operation 27
Table 15 – Mapping of SFRs to Security Objectives 32
Table 16 – Security Functional Requirement Dependencies 37
Table 17 – Security Assurance Requirements 38
Table 18 – Cryptographic Algorithms 41
Table 19 – Administrative Accounts for the TOE 42
Table 20 – Terminology 45
Table 21 – Acronyms 47

LIST OF FIGURES

Figure 1 – WatchGuard Firebox Appliance 3
Figure 2 – Deployment Configuration of the TOE 5

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 ST reference, the 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 operational 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

ST Title:	WatchGuard Firebox Security Appliances with Fireware v11.11 Security Target
ST Version:	1.3
ST Date:	17 October 2016

1.3 TOE REFERENCE

TOE Identification: WatchGuard Firebox Security Appliances with Fireware v11.11.2.508770 with WatchGuard Dimension 2.1 Software

TOE Developer: WatchGuard Technologies, Inc.

TOE Type: Firewall, Network Security

1.4 TOE OVERVIEW

The TOE is a suite of hardware devices that provide all-in-one network and content security solutions. These devices (known as Firebox Security Appliances) are equipped with a WatchGuard proprietary operating system (OS) called Fireware v11.11.

Firebox appliances (running the Fireware OS) separate the organization's internal networks from external network connections to decrease the risk of an external attack. It protects the internal, private networks from unauthorized users on the Internet. Traffic that enters and leaves the protected networks is examined by the Firebox appliances. They use access policies to identify and filter different types of information and can also control which policies or ports the protected computers can use on the Internet (outbound access).

WatchGuard Dimension 2.1 provides for viewing and sorting of audit logs.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

1.5.1.1 Physical Configuration

The TOE is a software and hardware TOE. It is a combination of a particular model Firebox appliance and the Fireware v11.11 OS software. Table 1 lists all the instances of the TOE that operate in the CC-evaluated configuration mode. All listed TOE instances offer the same core functionalities.

TOE Series	Hardware Model	Fireware OS Version
Firebox M Series	Firebox M200	Fireware OS v11.11
	Firebox M300	
	Firebox M400	
	Firebox M440	
	Firebox M500	
	Firebox M4600	
	Firebox M5600	

TOE Series	Hardware Model	Fireware OS Version
Firebox T10 Series	Firebox T10	Fireware OS v11.11
	Firebox T10-W	
Firebox T30 Series	Firebox T30	Fireware OS v11.11
	Firebox T30-W	
Firebox T50	Firebox T50	Fireware OS v11.11
	Firebox T50-W	

Table 1 – TOE Instances

Additionally, the TOE includes the WatchGuard Dimension 2.1 software.

1.5.1.2 Network Interfaces

In the CC-evaluated configuration of the TOE, secure access to administrative functions is provided through the following network interfaces:

Ethernet Ports - Each instance of the TOE (identified in Table 1 above) provides a group of RJ-45 Ethernet ports. Administrators can configure these ports to be either internal (trusted) or external (untrusted) network interfaces. Trusted interfaces permit authorized administrators to perform remote administration using the Network Command Line Interface (CLI) and Web-Based Graphical User Interface (GUI). These network ports must be configured by an authorized administrator to allow Secure Hypertext Transfer Protocol (HTTPS) and (Transport Layer Security (TLS) (v1.2) for the Web-Based GUI and Secure Shell (SSH) (v2.0) for the Network CLI.

Serial Interface - The Serial Interface is used to directly connect the Firebox appliances to a console management workstation. This port allows access to CLI when connected to a terminal which supports VT100 emulation. This local Console CLI permits an authorized administrator to configure the TOE, monitor its operation, and examine the audit logs.

Figure 1 provides a typical front view of the TOE hardware.

Figure 1 – WatchGuard Firebox Appliance

1.5.1.3 TOE Boundary

The WatchGuard Firebox appliance is designed to filter traffic based on a set of rules that are created by a system administrator. WatchGuard Dimension provides a platform for sorting and viewing the log files that are produced by the appliance.

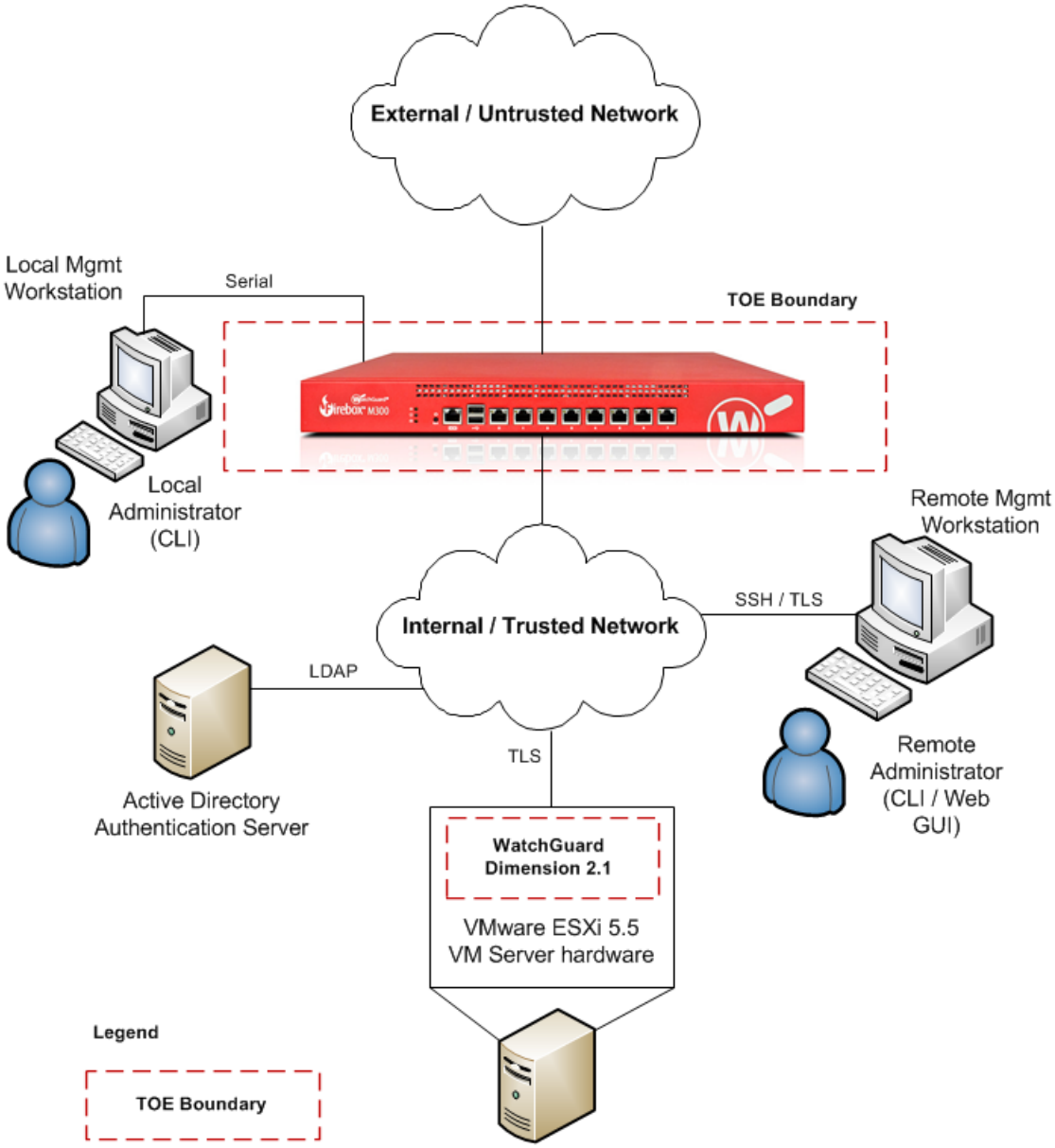

Figure 2 below illustrates the physical boundary of the overall solution and ties together all of the administrative components of the TOE and the constituents of the operational environment.

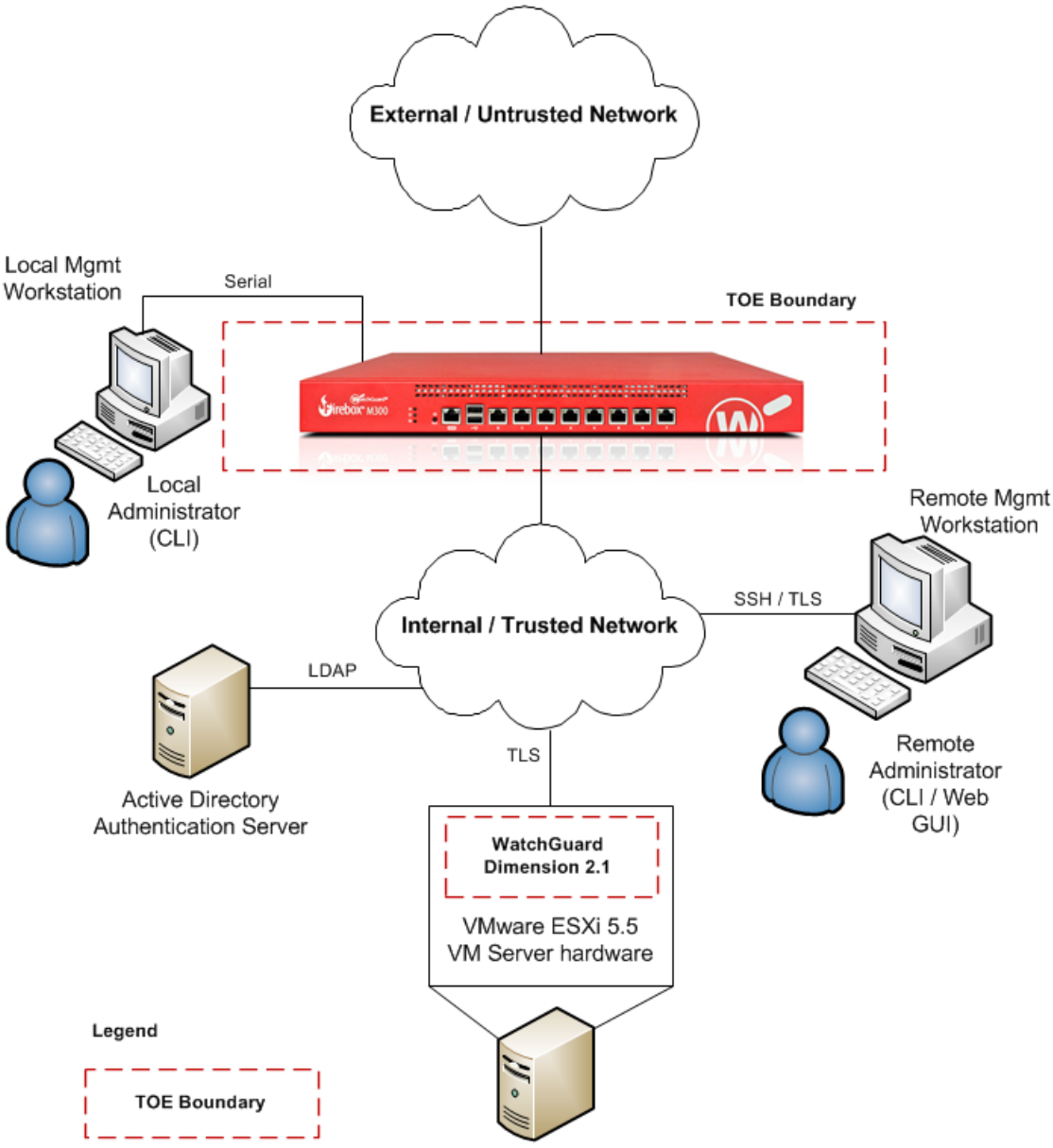

Figure 2 – Deployment Configuration of the TOE

1.5.1.4 Operational Environment

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

Operational Environment Component	Supporting Components

Operational Environment Component	Supporting Components
Local Management Workstation	Terminal Application operating in VT100 emulation mode
Remote Management Workstation	Any computer that supports the following: • Internet Explorer v11, or later • Firefox v42.0, or later • SSH v2.0 (for CLI) • TLS v1.2 (for GUI)
Active Directory Authentication Server	Windows Server 2008 R2 General purpose computer hardware
WatchGuard Dimension environmental support	Any appropriate VM hardware VMware ESXi 5.5, or later 40GB allocated for data (default)

Table 2 – Non-TOE Hardware and Software

1.5.1.5 TOE Guidance

The TOE includes the following guidance documentation:

Document Type	Document Title
Hardware and Help Guides	Fireware Help (includes Dimension)
	Fireware Command Line Interface Reference
	WatchGuard Firebox M200/M300 Hardware Guide
	WatchGuard Firebox M400/M500 Hardware Guide
	WatchGuard Firebox M440 Hardware Guide
	WatchGuard Firebox M4600 Hardware Guide
	WatchGuard Firebox M5600 Hardware Guide
	WatchGuard Firebox T10 Hardware Guide
	WatchGuard Firebox T30/T50 Hardware Guide

Document Type	Document Title
Quick Start Guides	WatchGuard Firebox M200/M300 Quick Start Guide
	WatchGuard Firebox M400/M500 Quick Start Guide
	WatchGuard Firebox M440 Quick Start Guide
	WatchGuard Firebox M4600 Quick Start Guide
	WatchGuard Firebox M5600 Quick Start Guide
	WatchGuard Firebox T10/T10-W Quick Start Guide
	WatchGuard Firebox T30, T30-W/T50, T50-W Quick Start Guide

Table 3 - TOE Guidance Documentation

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.

Functional Classes	Description
Security Audit	The Firebox devices generate audit entries for security related events which are stored as audit logs in the WatchGuard Dimension server. The audit logs are protected from unauthorized modification and deletion and may only be reviewed by authorized administrators.
Cryptographic Support	The TOE depends on FIPS validated cryptographic algorithms, as detailed in Table 18. The TOE protects the confidentiality and integrity of all information when it passes between the TOE and the remote management workstation, and also when it passes between the TOE and the local management workstation. The TOE achieves this by using validated cryptographic algorithms to perform encryption and the decryption of data according to the SSH and TLS protocols.
User Data Protection	Information flow control is achieved through the use of policy and policy enforcement.
Identification and Authentication	The TOE provides two pre-configured administrative accounts. The TOE requires that users associated with these accounts be identified and authenticated before permitted access to the TOE and TOE security functions. Users may authenticate using either local password authentication, or Active Directory.

Functional Classes	Description
Security Management	The TOE provides local management capabilities via serial connection and remote management capabilities via workstation CLI and/or Web-Based GUI. Management functions allow the administrators to configure users, roles, and security policy attributes.
Protection of the TSF	The operating system clock inside the TOE provides all of the timestamps for the audits.
Trusted Path/Channels	The communications links between the TOE and its remote administrators are protected using HTTPS (TLS v1.2) for the Web-based GUI and SSH (v2.0) for workstation CLI.

Table 4 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are not included in the evaluated configuration:

External Network Interface – The external network interface allows for remote administration of the TOE. Authorized administrators can connect to the TOE through the external network and configure the TOE, monitor its operation, and examine the audit logs via remote workstation by logging into a Web-based GUI. To protect the confidentiality and integrity of information the external network connection must be configured to allow HTTPS and TLS (v1.2) at the network port and the remote web browser respectively. The External Network Interface is not to be used in the evaluated configuration.

Telnet – Use of Telnet protocol is not permitted in the evaluated configuration of the TOE.

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-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

2.2 EVALUATION ASSURANCE LEVEL

This Security Target claims conformance to Evaluation Assurance Level 4 augmented with ALC_FLR.2 – Flaw Reporting Procedures.

2.3 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

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1.1 Threats Addressed by the TOE

Table 5 lists the threats addressed by the TOE. Potential threat agents are unauthorized persons or external IT entities not authorized to use the TOE itself. The threat agents are assumed to have a low to moderate attack potential and are assumed to have a moderate level of resources and access to all publicly available information about the TOE and potential methods of attacking the TOE. It is expected that the WatchGuard Firebox units will be protected to the extent necessary to ensure that they remain connected to the networks they protect.

Threat	Description
T.ACCESS	An unauthorized person on an external network may attempt to by-pass the information flow control policy to access protected resources on the internal network.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, or records have been compromised, thus allowing an attacker to escape detection.
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non- security functions provided by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

Threat	Description
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

Table 5 – Security Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. The TOE must address the organizational security policies described in Table 6.

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, access, or malicious activity must be collected.
P.MANAGE	The TOE shall be manageable only by authorized administrators.

Table 6 – Organizational Security Policies

3.3 ASSUMPTIONS

Table 7 describes the security aspects of the intended environment for the evaluated TOE. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Assumptions	Description
A.LOCATE	The TOE hardware and software will be located within controlled access facilities and protected from unauthorized physical modification.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.SECALG	Administrators will ensure that their browsers and SSH client applications use only approved cryptographic algorithms.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

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.ACCESS	The TOE must allow only authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide accountability for the application of rules to user data as it flows through the TOE and for authorized administrator use of security functions by providing a means to record and securely store a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator using cryptographic functions.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.

Security Objective	Description
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 domain or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSEC	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.SECALG	Only approved cryptographic algorithms will be used in the browsers and SSH client applications of authorized administrators.

Table 9 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

Table 10 maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.AUDACC	T.COMDIS	T.MEDIAT	T.NOAUTH	T.NOHALT	T.PRIVIL	T.PROCOM	P.ACCACT	P.DETECT	P.MANAGE	A.LOCATE	A.MANAGE	A.SINGEN	A.SECALG
O.ACCESS			X			X	X				X				
O.ADMIN		X									X				
O.AUDIT		X							X	X					

	T.ACCESS	T.AUDACC	T.COMDIS	T.MEDIAT	T.NOAUTH	T.NOHALT	T.PRIVIL	T.PROCOM	P.ACCACT	P.DETECT	P.MANAGE	A.LOCATE	A.MANAGE	A.SINGEN	A.SECALG
O.ENCRYP					X			X							
O.IDAUTH			X		X	X	X		X	X	X				
O.MEDIAT	X			X											
O.PROTCT			X			X	X				X				
O.TIME									X	X					
OE.ADMIN						X					X		X		
OE.PHYSEC						X						X			
OE.SINGEN														X	
OE.SECALG															X

Table 10 – Mapping Between Objectives and Threats, Policies, 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.ACCESS**	An unauthorized person on an external network may attempt to by-pass the information flow control policy to access protected resources on the internal network.	
Objectives:	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
Rationale:	O.MEDIAT mitigates this threat by ensuring that all information between clients and servers located on internal and external networks is mediated by the TOE.	

Threat: **T.AUDACC**	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, or records have been compromised, thus allowing an attacker to escape detection.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are

		able to access such functionality.
	O.AUDIT	The TOE must provide accountability for the application of rules to user data as it flows through the TOE and for authorized administrator use of security functions by providing a means to record and securely store a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
Rationale:	O.ADMIN provides for security management functionality, including the functionality for reviewing the audit trail. O.AUDIT requires that users are accountable for information flows through the TOE based on the application of rules to that traffic, and that authorized administrators are accountable for the use of security functions related to audit. O.AUDIT also ensures that the audit records are stored securely.	

Threat: **T.COMDIS**	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.	
Objectives:	O.ACCESS	The TOE must allow only authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.	

Threat:	An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the

T.MEDIAT	internal network.	
Objectives:	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
Rationale:	O.MEDIAT requires that all information that passes through the networks is mediated by the TOE, blocking unauthorized users, and impermissible information.	

Threat: **T.NOAUTH**	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator using cryptographic functions.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
Rationale:	O.IDAUTH requires that users be uniquely identified before accessing the TOE. O.ENCRYP ensures the confidentiality and integrity of data passed between the TOE and the authorized administrator for management purposes.	

Threat: **T.NOHALT**	An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to

		legitimate users.
	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
	OE.PHYSEC	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by requiring the TOE to protect itself against bypass, or to deny access to legitimate users. OE.ADMIN and OE.PHYSEC also address this threat by ensuring that the TOE is properly installed and operated.	

Threat: **T.PRIVIL**	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
Rationale:	The O.IDAUTH objective addresses this threat by requiring authentication of users prior to accessing TOE functions. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-	

	protection.

Threat: **T.PROCOM**	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator using cryptographic functions.
Rationale:	O.ENCRYP counters this threat by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.ACCACT**	Users of the TOE shall be accountable for their actions.	
Objectives:	O.AUDIT	The TOE must provide accountability for the application of rules to user data as it flows through the TOE and for authorized administrator use of security functions by providing a means to record and securely store a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	The O.AUDIT objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. O.TIME supports the audit trail with reliable time stamps.	

Policy:	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be

P.DETECT	collected.	
Objectives:	O.AUDIT	The TOE must provide accountability for the application of rules to user data as it flows through the TOE and for authorized administrator use of security functions by providing a means to record and securely store a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	The O.AUDIT objective supports this policy by ensuring the collection of data on security relevant events. O.IDAUTH ensures that users are appropriately identified, thereby supporting this policy. O.TIME supports this policy by ensuring that the audit functionality is able to include reliable timestamps.	

Policy: P.MANAGE	The TOE shall be manageable only by authorized administrators.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.
	O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed,

		and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	The O.ACCESS objective supports this policy by ensuring that authorized administrators have appropriate access to manage the TOE. O.ADMIN supports this policy by ensuring that the TOE provides the appropriate security management functionality to authorized administrators. O.IDAUTH supports this policy by ensuring that administrators must be identified and authenticated prior to being granted access to TOE security management functions. O.PROTCT supports this policy by ensuring that the TOE security functions may not be bypassed to allow unauthorized access. OE.ADMIN supports this policy by ensuring that only competent, trained administrators have access to the TOE security functions.	

4.3.3 Security Objectives Rationale Related to Assumptions

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

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

Assumption: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.

Rationale:	The OE.ADMIN objective supports the assumption by ensuring that all authorized administrators are qualified and trained to manage the TOE.

Assumption: A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	
Objectives:	OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
Rationale:	This objective supports the assumption by requiring that the information flow subject to security policy is made to pass through the TOE.	

Assumption: A.SECALG	Administrators will ensure that their browsers and SSH client applications use only approved cryptographic algorithms.	
Objectives:	OE.SECALG	Only approved cryptographic algorithms will be used in the browsers and SSH client applications of authorized administrators.
Rationale:	This objective supports the assumption by requiring that authorized administrators use only approved cryptographic algorithms from their browsers and SSH client applications.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

This section provides the 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 **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 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the Common Criteria and extended components defined in Section 5.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation

Class	Identifier	Name
(FCS)	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
Trusted Path/Channels (FTP)	FTP_TRP.1	Trusted path

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

Functional Component	Auditable Event	Additional Audit Record Contents
FDP_IFF.1	All decision on requests for information flow	The presumed addresses of the source and destination
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users' capability to authenticate	The user identity provided to the TOE The identity of the administrator restoring the user account
FIA_UAU.1	All use of the user authentication mechanism	The user identity provided to the TOE
FIA_UID.1	All use of the user identification mechanism	The user identity provided to the TOE
FMT_SMF.1	Notice of creation, modification or deletion of policy rules, user account information, authentication mechanisms or audit logs	The identity of the authorized administrator
FPT_STM.1	Changes to the time	The identity of the administrator performing this action

Table 12 – Auditable Events

6.2.1.2 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 [*users in the Device Administrator and Device Monitor roles for the Firebox device, and users in the Super Administrator and Report Administrator roles for the Dimension server*] with the capability to read [*all audit trail data*] 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.

6.2.1.3 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*searches*] of audit data based on [*log type, key words*].

6.2.1.4 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.

6.2.1.5 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [prevent audited events, except those taken by the authorised ~~user~~ **administrator** with special rights] and [*shall limit the number of audit records lost*] if the audit trail is full.

6.2.2 Cryptographic Support (FCS)

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 [*Random Number Generation*] and specified cryptographic key sizes [*listed in Table 13*] that meet the following: [*American National Standards Institute (ANSI) X9.31*].

Key Usage	Key Size
Triple Data Encryption Algorithm	80, 112 (assessed security strength)
AES	128, 192, 256
Asymmetric (RSA signature/verification)	2048, 3072, 4096

Table 13 – 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 [*zeroization*] 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.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in* Table 14] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in* Table 14] and cryptographic key sizes [*cryptographic key sizes specified in* Table 14] that meet the following: [*standards listed in* Table 14].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Encryption and Decryption	Triple Data Encryption Algorithm (TDEA) (TCBC mode)	112 (assessed security strength)	NIST Special Publication 800-67 NIST Special Publication 800-20	2171
Encryption and Decryption	AES (Advanced Encryption Standard) (CBC and CTR modes[1])	128, 192, 256	FIPS PUB 197 NIST Special Publication 800-38A	3960
Cryptographic Signature Services	RSA	2048, 3072, 4096	PKCS #1 v. 2.1 RSASSA-PKCS1-v1_5	2023
Hashing	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	n/a	FIPS PUB 180-4	3266
Keyed Hash	HMAC-SHA-1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	n/a	FIPS PUB 198	2580

Table 14 – Cryptographic Operation

6.2.3 User Data Protection

6.2.3.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*Unauthenticated Information Flow SFP*] on

[1] AES is used in both CBC and CTR modes.

[*Subjects: unauthenticated users and IT entities*[2]*;*

Information: network traffic[3]*;*

Operations: pass information].

6.2.3.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*Unauthenticated Information Flow SFP*] based on at least the following types of subject and information security attributes:

[*Subjects: unauthenticated users and external entities*

Subject security attributes:

- *presumed address*

Information: network traffic

Information security attributes:

- *presumed address of source subject;*
- *presumed address of destination subject;*
- *port number;*
- *type (protocol);*
- *schedule*].

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

[*Subjects can cause information to flow through the TOE to another connected network if all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes*].

FDP_IFF.1.3 The TSF shall ~~enforce~~ ~~the~~ **ensure that** [*users in the Device Administrator role shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied*].

[2] Unauthenticated users and IT entities that send and receive information through the TOE to one another

[3] Any network traffic sent through the TOE from one subject to another

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

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

[*the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., Request for Comments (RFC)). This shall be accomplished through protocol filtering proxies that are designed for that purpose*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*0 and 1000*]] of unsuccessful authentication attempts occur related to [*authorized TOE administrator*[4] *access*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock out the account until access is restored by a user in the Device Administrator role*].

Application Note: This SFR applies to the Command Line Interface (CLI) and serial interface only.

6.2.4.2 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.

6.2.4.3 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*local and support for Active Directory authentication*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following rules:*

a. administrators may authenticate to any interface using a locally held username and password;
b. administrators may authenticate to any interface via specified Active Directory domain.]

[4] 'TOE Administrator' refers to a user in the Device Administrator or Device Monitor role.

6.2.4.4 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

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Unauthenticated Information Flow SFP*] to restrict the ability to [[*delete attributes from a rule, modify attributes in a rule, add attributes to a rule*]] the security attributes [*source address, destination address, port number, type, schedule*] to [*users in the Device Administrator role*].

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 [*Unauthenticated Information Flow SFP*] to provide [restrictive] default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users in the Device Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a. *administer unauthenticated information flow rules;*
b. *administer user account information;*
c. *administer authentication mechanisms and authentication failure handling policy;*
d. *review audit logs.]*

6.2.5.4 FMT_SMR.1(1) Security roles (Firebox)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Device Administrator, Device Monitor*] **for the Firebox device**.

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

6.2.5.5 FMT_SMR.1(2) Security roles (Dimension)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Super Administrator, Report Administrator*] **for the Dimension Server**.

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

6.2.6 Protection of the TSF

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

6.2.7.1 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].

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

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

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Table 15 provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.PROTCT	O.TIME
FAU_GEN.1			X					
FAU_SAR.1	X	X	X					
FAU_SAR.3		X	X					
FAU_STG.1			X				X	

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.PROTCT	O.TIME
FAU_STG.4			X				X	
FCS_CKM.1				X				
FCS_CKM.4				X				
FCS_COP.1				X				
FDP_IFC.1						X		
FDP_IFF.1						X		
FIA_AFL.1							X	
FIA_UAU.1	X				X			
FIA_UAU.5					X			
FIA_UID.1	X				X			
FMT_MSA.1	X	X					X	
FMT_MSA.3		X					X	
FMT_SMF.1		X					X	
FMT_SMR.1					X			
FPT_STM.1								X
FTP_TRP.1				X				

Table 15 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each Security Functional Requirement (SFR) back to the security objectives for the TOE.

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
	FMT_MSA.1	Management of security attributes
Rationale:	FAU_SAR.1 meets this objective by ensuring that only	

	authorized administrators are able to access and read audit records. FIA_UID.1 and FIA_UAU.1 support the objective by ensuring that users are identified and authenticated prior to being allowed access to TOE security management functionality. FMT_MSA.1 addresses the objective by ensuring that only authorized administrators have access to the security attributes associated with the information flow security function policy.

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
	FAU_SAR.3	Selectable audit review
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	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, and FAU_SAR.3 meets the objective by allowing administrators to search those records. FMT_MSA.1meets the objective by providing the functionality to manage the parameters associated with the information flow control security functional policy. FMT_MSA.3 meets the objective by providing the initial values required to manage the information flow control security functional policy. FMT_SMF.1 meets the objective by providing the management functions supporting the specific security management claims, and limiting access to that functionality to authorized administrators.	

Objective: O.AUDIT	The TOE must provide accountability for the application of rules to user data as it flows through the TOE and for authorized administrator use of security functions by providing a means to record and securely store a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.	
Security	FAU_GEN.1	Audit data generation

Functional Requirements:	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
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_SAR.1 supports the objective by providing authorized administrators the means to read the audit information, and FAU_SAR.3 supports the objective by providing a means to search the audit trail. FAU_STG.1 and FAU_STG.4 supports the objective by preventing unauthorized modification of logs, and ensuring that the proper actions are taken if the audit trail becomes full.	

Objective: O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FTP_TRP.1	Trusted path
Rationale:	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 support the objective by providing the cryptographic functionality required to support trusted links. FTP_TRP.1 supports the objective by specifying the use of that cryptography between the TOE and the remote administrator.	

Objective: O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions.	
Security Functional Requirements:	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
	FMT_SMR.1	Security roles

Rationale:	FIA_UID.1 and FIA_UAU.1 ensure that users are identified and authenticated prior to being granted access to TOE security management functions. FIA_UAU.5 provides multiple possible authentication mechanisms that may be used to support the objective. FMT_SMR.1 supports the objective by providing roles which are used to provide users access to TOE security functionality.

Objective: O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.	
Security Functional Requirements:	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Rationale:	FDP_IFC.1 and FDP_IFF.1 support the objective by detailing how the TOE mediates the flow of information for the unauthenticated information flow policy.	

Objective: O.PROTCT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.	
Security Functional Requirements:	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
	FIA_AFL.1	Authentication failure handling
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
Rationale:	FAU_STG.1 and FAU_STG.4 support this objective by ensuring that the records in the audit trail are securely stored, and appropriately protected in the case of the storage becoming full. FIA_AFL.1 supports the objective by locking a user account after a specified number of unsuccessful authentication attempts, thereby protecting the TOE against a brute force attack. The security management SFRs, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 support the objective by ensuring that access to TOE	

	security functions is limited to authorized users.

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 requiring that the TOE be able to provide reliable time stamps.	

6.3.2 Dependency Rationale

Table 16 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FAU_SAR.3	FAU_SAR.1	✓
FAU_STG.1	FAU_GEN.1	✓
FAU_STG.4	FAU_STG.1	✓
FCS_CKM.1	FCS_COP.1	✓
	FCS_CKM.4	✓
FCS_CKM.4	FCS_CKM.1	✓
FCS_COP.1	FCS_CKM.1	✓
	FCS_CKM.4	✓
FDP_IFC.1	FDP_IFF.1	✓
FDP_IFF.1	FDP_IFC.1	✓
	FMT_MSA.3	✓
FIA_AFL.1	FIA_UAU.1	✓
FIA_UAU.1	FIA_UID.1	✓
FIA_UAU.5	None	N/A
FIA_UID.1	None	N/A

SFR	Dependency	Dependency Met
FMT_MSA.1	FDP_IFC.1	✓
	FMT_SMR.1	✓
	FMT_SMF.1	✓
FMT_MSA.3	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	✓
FPT_STM.1	None	N/A
FTP_TRP.1	None	N/A

Table 16 – Security Functional Requirement Dependencies

6.4 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2). EAL4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL4.

The Security Assurance Requirements (SARs) are summarized in Table 17.

Assurance Class	Assurance Components	
	Identifier	Name
Class ADV: Development	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
Class AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ALC:	ALC_CMC.4	Production support, acceptance procedures and automation

Assurance Class	Assurance Components	
	Identifier	**Name**
Life-cycle support	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Class ASE: 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
Class ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Table 17 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. This serves to rationalize that the security functionality satisfies the necessary requirements.

7.1.1 Security Audit

7.1.1.1 Audit Generation

The TOE generates log files with information about security related events that the Administrator of the TOE can review to monitor the network security and activity, identify security risks, and address them.

A *log file* is a list of events along with information about those events. An *event* is a single activity that occurs on the TOE. For example, TOE's denying of a packet based on a policy set is an *event*. The TOE also captures information about allowed events to give a more complete picture of the activities on the network.

The TOE audits events in the form of logs. It generates and saves the following types of log messages:

Traffic log messages – The TOE generates traffic log messages as it applies packet filter and proxy rules to traffic that goes through the device.

Alarm log messages – Alarm log messages are sent when an event occurs that triggers the TOE to run a command. When the alarm condition is matched, the device sends an alarm log message to the WatchGuard Dimension Server, and then it does the specified action.

Event log messages – The TOE sends event log messages because of user activity. Actions that can cause the TOE to send an event log message are:

- Device start up and shut down
- Device authentication
- Process start up and shut down
- Problems with the device hardware components
- Any task done by the administrator

Debug log messages – Debug log messages include diagnostic information that can be used to troubleshoot problems.

Statistic log messages – Statistic log messages include information about the performance of the TOE.

All audit records include at least the following information:

- The type of event
- The identity of the subject that caused the event
- The outcome of the event
- The date and time of the event.

7.1.1.2 Audit Review

Audits can be viewed using the CLI, the Web User Interface, and the Dimension Mgmt Interface. Reviewing the audit records stored on the TOE is an activity limited to the TOE's administrative accounts (*status* and *admin* accounts). Reviewing the audit records stored on the Dimension server is an activity limited to users assigned the Super Administrator and Report Administrator roles. Users assigned these account types and/roles can perform searches and sorting of the audit data by key word and log type.

7.1.1.3 Audit Storage

The Firebox device contains a small amount of internal memory which it utilizes to temporarily save the audit records. In addition, the Firebox device is configured to send audit data to a WatchGuard Dimension Server. The TOE protects the unauthorized deletion and modifications of the audit data. No user may modify or delete the audit data. However, the audit records may be rotated out based on age. For example, audit records may be rotated out after ninety days. The rotation parameters are administrator-configurable.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4.

7.1.2 Cryptographic Support

Using cryptographic algorithms , the TOE protects the confidentiality and integrity of information when it passes between the TOE and the remote management workstation, when it passes between the TOE and the local management workstation, and when it passes between the TOE and the WatchGuard website for firmware upgrades. The TOE achieves this by using SSH (v2.0) and TLS (v1.2) which perform the encryption and the decryption of data that is being passed.

All cryptographic functions used in SSH and TLS are performed by FIPS 140-2 validated cryptographic algorithms. Certificate information is provided in Table 18.

TOE Series	Model Number	Operating System	CAVP Certificate Numbers
Firebox M Series	Firebox M200	Fireware OS v11.11.2	AES: 3960 RSA: 2023 SHS: 3266 TDES: 2171 HMAC: 2580 DRBG: 1160
	Firebox M300		
	Firebox M400		
	Firebox M440		
	Firebox M500		
	Firebox M4600		
	Firebox M5600		

TOE Series	Model Number	Operating System	CAVP Certificate Numbers
Firebox T10 Series	Firebox T10		
	Firebox T10-W		
Firebox T30 Series	Firebox T30		
	Firebox T30-W		
Firebox T50 Series	Firebox T50		
	Firebox T50-W		

Table 18 – Cryptographic Algorithms

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 User Data Protection

By default, the TOE denies all packets that are not specifically allowed. Through the use of policy, the administrator configures a set of rules that direct the TOE to allow or deny traffic based on source and destination of the packet, type of data (based on protocol), the port or schedule. The TOE allows an authorized administrator to view all information flows allowed by the policy rules before the rules are applied.

The TOE uses two categories of policies to filter network traffic: *packet filters* and *proxies*. A packet filter policy examines each packet's Internet Protocol (IP) and Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP) header. If the packet header information is legitimate, then the TOE allows the packet. Otherwise, the TOE drops the packet. A proxy policy examines both the header information and the content of each packet to make sure that connections are secure. If the packet header information is legitimate and the content of the packet is not considered a threat, then the TOE allows the packet. Otherwise, the TOE drops the packet.

Proxy policies also include settings that are related to the specified network protocol. For example, the administrator can configure an SMTP proxy to deny email if the headers are not properly set. The TOE supports proxy policies for many common protocols, including DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP, SMTP, and TCP/UDP.

The TOE includes many pre-configured packet filter policies and proxy policies that can be readily used. The administrator can use these pre-configured policies as they are, or modify them to suit the need of the network environment. The administrator can also create a custom policy based on the following security attributes:

- Source address of the information
- Destination address of the information
- What service the traffic is using
- The source port of the information
- The destination port of the information
- Interface the traffic arrives or exits on (Trusted/External)
- Schedule (the time period for which information flow is explicitly allowed)

TOE Security Functional Requirements addressed: FDP_IFC.1, FDP_IFF.1.

7.1.4 Identification and Authentication

No administrative actions may be performed prior to login to one of the TOE interfaces.

The Firebox device provides two built-in administrative accounts: *admin* and *status*. The default passphrases are changed during the TOE configuration.

Table 19 summarizes the characteristics of these accounts.

Account Name	Initial Passphrase	Note
admin	readwrite	The “admin” account is a default account in the Device Administrator role which allows full access to the TOE. This account and the associated passphrase may be used to save configuration changes to the TOE. It is also the account that can be used to change the passphrases for both the “admin” and the “status” accounts.
Status	read-only	The “status” account is a default account in the Device Monitor role which allows read-only access to the TOE. With this account and the associated passphrase, a user can review the TOE configuration but cannot make changes to the TOE.

Table 19 – Administrative Accounts for the TOE

Both the *admin* and *status* accounts must be associated with users. The TOE requires that users associated with these accounts be identified and authenticated before they are given access to the TOE. Additional user accounts may be created, allowing a user in the Device Administrator or Device Monitor role to authenticate to any interface using a locally held username and password or via a specified Active Directory domain.

The TOE provides protection against unauthorized users gaining access to the TOE CLI or serial interface by allowing a configurable number of unsuccessful login attempts before being locked out. When the *status* account is locked out, it can be unlocked by the individual who holds the *admin* account.

Users accessing the Dimension Server management interface must also be identified and authenticated prior to accessing the TSF. A default account, *admin*, is provided in the Super Administrator role and this account must be assigned a password during installation.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1.

7.1.5 Security Management

7.1.5.1 Roles

The Firebox device supports role-based user account credentials with two default role types: Device Monitor and Device Administrator. The Device Monitor role is provided with read-only access to the TOE. The Device Administrator role has full authorization of the TOE including user account administrative functions such as account creation, password resets, and authentication failure handling policies.

The TOE performs a number of management functions that are only available to Device Administrators. It administers unauthenticated information flow control rules by allowing the administrator to add, delete, modify, and save configuration policies for the following security attributes:

- Source address of the information
- Destination address of the information
- What service the traffic is using
- The source port of the information
- The destination port of the information
- Interface the traffic arrives or exits on (Trusted/External)
- Schedule (the time period for which information flow is explicitly allowed)

The TOE provides restrictive default values for information flow control security attributes and only allows the authorized administrator to override them. Below lists some of the restrictive default values:

- Ping requests received on the external network are denied.
- All incoming policies are denied and the outgoing policy allows all outgoing traffic.
- The TOE is set up for direct administration and local administration from the trusted network only. Additional configuration changes must be made to allow remote administration from the external network.

The TOE also limits the ability to review logs to users in the Device Administrator and Device Monitor roles.

The Dimension Server supports the Super Administrator and Report Administrator roles. The Super Administrator role supports access to all Dimension functionality. Users with the Report Administrator role may schedule reports, manage groups, view logs, and view reports.

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

7.1.6 Protection of the TSF

The operating system clock inside of the TOE provides all of the time stamps for the audits. The system clock can only be set through the CLI by a user assuming an authorized administrator role for the device.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.1.7 Trusted Path/Channels

The TOE provides trusted paths protected by encryption to guard against disclosure and are protected by cryptographic signature to detect modifications. The trusted paths are logically distinct from other communication paths and provide assured identification of their end points.

The TOE protects information when it is transmitted between the TOE and the remote management workstation. The TOE achieves this by using SSH and TLS which perform the encryption and the decryption of data that is being passed.

Administrators initiate communications with the TOE by selecting the known TOE URL, thus ensuring identification of the interface. The administrators must authenticate with a username and password combination to access the modules, thereby providing assurance of the user identity. Remote administration authentication is performed over HTTPS (TLS v1.2) for the Network Web-based GUIs and SSH (v2.0) for the Network CLI. In the evaluated configuration, the administrator's browser or SSH client must be configured to ensure that only approved algorithms are used.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
authorized administrator or administrator	These are generic terms that mean someone who administers the TOE.
TOE Administrator	A TOE Administrator is a user in the Device Administrator or Device Monitor role who administers the TOE.

Table 20 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CSEC	Swedish Certification Body for IT Security
CTR	Counter
DNS	Domain Name Server
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol

Acronym	Definition
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
Mgmt	Management
NIST	National Institute of Standards and Technology (USA)
OS	Operating System
OSP	Organizational Security Policy
POP3	Post Office Protocol version 3
PP	Protection Profile
PUB	Publication
RFC	Request For Comments
RJ	Registered Jack
RSA	Rivest-Shamir-Adleman
SFR	Security Functional Requirement
SFP	Security Function Policy
SHA	Secure Hashing Algorithm
SIP	Session Initiated Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
ST	Security Target
TCBC	TDEA Cipher Block Chaining
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

Acronym	Definition
UDP	User Datagram Protocol
VM	Virtual Machine
VT	Virtual Terminal

Table 21 – Acronyms