WatchGuard Technologies, Inc.

XTM Firewalls and Fireware XTM Operating System v11.5.1

Security Target

Evaluation Assurance Level: EAL4+

Document Version: 0.8

Prepared for:

WatchGuard Technologies, Inc.
505 Fifth Avenue South, Suite 500
Seattle, WA 98104
United States of America

Phone: +1 206 613 6600
http://www.watchguard.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the XTM Firewalls and Fireware XTM Operating System v11.5.1 from WatchGuard Technologies, Inc., and will hereafter be referred to as the TOE throughout this document. The TOE is composed of hardware (specific models of XTM[1] Firewalls product family) and software (Fireware XTM Operating System). There are a total of 23 instances of the TOE, as shown in Table 4.

This ST conforms to the following two protection profiles:

- U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007
- U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007.

The above two protection profiles will be referred to throughout this ST using these shortened names and acronyms.

- Short name: Application-level Firewall PP[2]; Acronym: ALF
- Short name: Traffic Filter Firewall PP; Acronym: TFF

Both protection profiles require assurance at Evaluation Assurance Level (EAL) 2, augmented by ALC_FLR.2. This evaluation has been augmented to meet the assurance requirements for EAL 4 augmented with ALC_FLR.2, while still meeting all of the functional requirements to conform to the protection profiles listed above.

[1] XTM – eXtensible Threat Management

[2] PP – Protection Profile

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	WatchGuard Technologies, Inc. XTM Firewalls and Fireware XTM Operating System v11.5.1 Security Target
ST Version	Version 0.8
ST Author	Corsec Security
ST Publication Date	4/13/2012

PP Identification	U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007; U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007.
TOE Reference	WatchGuard XTM Firewalls and Fireware XTM Operating System v11.5.1, Build Number: 331198
Keywords	Firewall, Network Security

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

WatchGuard Technologies, Inc. offers a suite of hardware devices that provide all-in-one network and content security solutions. These devices (known as XTM Firewalls) are equipped with a proprietary operating system called Fireware XTM, developed by WatchGuard.

XTM Firewall device (running the Fireware XTM Operating System) separates 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 XTM Firewall device. It uses access policies to identify and filter different types of information. It can also control which policies or ports the protected computers can use on the Internet (outbound access).

It should be noted that Fireware XTM Operating System comes in two varieties: Fireware XTM OS[3], and Fireware XTM Pro OS. Fireware XTM Pro OS is the superset of Fireware XTM OS as it offers more features, but both operating systems are contained in the same binary code. Customers can unlock either the Fireware XTM OS or Fireware XTM Pro OS, according to the license they purchased.

In referring to the software component (operating system) of the TOE, this document uses the following convention.

[3] OS – Operating System

Table 2 – Naming Convention used for Fireware XTM Software

Term	Scope of the Term
Fireware XTM Operating System	Indicates the whole software (TOE) that contains the two licenses below.
Fireware XTM OS	Refers to the XTM OS license
Fireware XTM Pro OS	Refers to the XTM Pro OS license

In summary, XTM Firewall devices that run the Fireware XTM Operating System incorporate packet filtering and application proxy techniques to inspect, control, and protect the flow of network traffic that travels in and out of the organization's internal networks.

Table 3 below summarizes product offerings from WatchGuard, under the product family name of XTM Firewalls.

Table 3 – XTM Firewalls Product List

Product Family Name	Individual Product Name	Recommended No. of Users	Ideal For	OS
	XTM 2 Series	Up to 50 users	Small Business	Fireware XTM OS, Fireware XTM Pro OS
	XTM 3 Series	Up to 300 users	Medium Business	Fireware XTM Pro OS
	XTM 5 Series	Up to 1500 users	Main office, headquarters	Fireware XTM OS, Fireware XTM Pro OS
	XTM 8 Series	Up to 5,000 users	Main office, headquarters	Fireware XTM Pro

				OS
	XTM 1050	Up to 10,000 users	Headquarters, Datacenters	Fireware XTM Pro OS
	XTM 2050	Up to 20,000 users	Enterprises, corporate, and university campuses	Fireware XTM Pro OS

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a combination of a particular model of XTM Firewall device and the corresponding Fireware XTM OS or Fireware XTM Pro OS. The table below (Table 4) lists all the instances of the TOE that operate in the CC-configuration mode.

Table 4 – List of TOE Instances

Product Family Name	Individual Product Name	Model Number	OS	TOE Instance
	XTM 2 Series	XTM21	Fireware XTM OS	✓
		XTM22	Fireware XTM OS	✓
		XTM23	Fireware XTM Pro OS	✓
		XTM21-W[4]	Fireware XTM OS	✓
		XTM22-W	Fireware XTM OS	✓
		XTM23-W	Fireware XTM Pro OS	✓

[4] "W" in the model number indicates the support for wireless connection. It should be noted that the Wireless interface is not included in the TOE boundary.

Product Family Name	Individual Product Name	Model Number	OS	TOE Instance
		XTM25	Fireware XTM OS	✓
		XTM25-W	Fireware XTM OS	✓
		XTM26	Fireware XTM Pro OS	✓
		XTM26-W	Fireware XTM Pro OS	✓
	XTM 3 Series	XTM33	Fireware XTM Pro OS	✓
		XTM33-W	Fireware XTM Pro OS	✓
		XTM330	Fireware XTM Pro OS	✓
	XTM 5 Series	XTM505	Fireware XTM OS	✓
		XTM510	Fireware XTM OS	✓
		XTM520	Fireware XTM OS	✓
		XTM530	Fireware XTM OS	✓
	XTM 8 Series	XTM810	Fireware XTM Pro OS	✓
		XTM820	Fireware XTM Pro OS	✓
		XTM830	Fireware XTM Pro OS	✓
		XTM830-F	Fireware XTM Pro OS	✓
	XTM 1050	XTM1050	Fireware XTM Pro OS	✓
	XTM 2050	XTM2050	Fireware XTM Pro OS	✓

It should be noted that all the TOE instances listed in Table 4 offer the same core functionalities of Application-level Firewall and Traffic Filter Firewall. As noted before, the Fireware XTM Pro OS is the superset and the Fireware XTM OS is the subset. However, both operating systems provide all the functionalities of packet filtering (Traffic Filter Firewall) and application proxy techniques (Application-level Firewall).

Figure 1 shows the detailed view of the CC-evaluated deployment configuration of the TOE.

Acronyms that appear in Figure 1:

- CLI – Command Line Interface
- Mgmt – Management
- SSH – Secure Shell
- TCP/IP – Transmission Control Protocol/Internet Protocol
- TLS – Transport Layer Security
- UI – User Interface

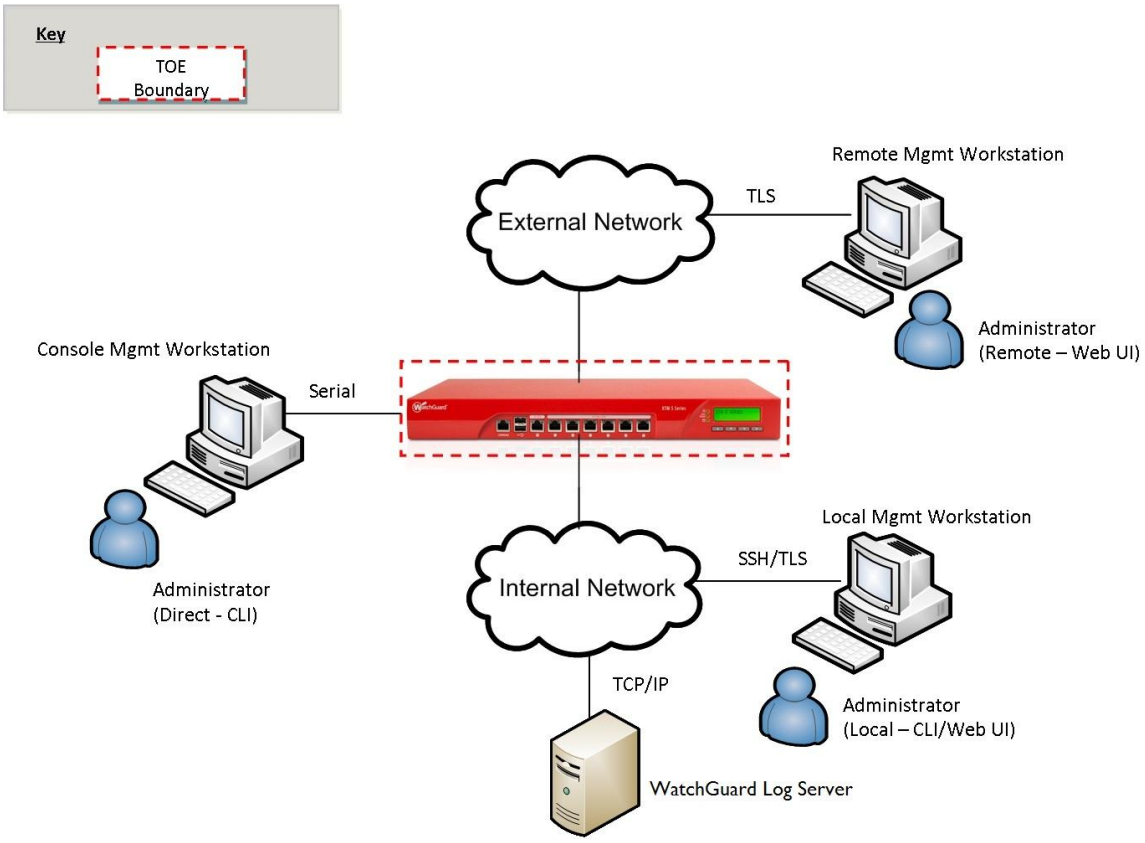

Figure 1 – Deployment Configuration of the TOE

The TOE boundary is drawn around the XTM Firewall device which contains and runs the Fireware XTM Operating System. In the CC-configuration of the TOE, access to administrative functions of the TOE is provided through the following two interfaces:

- Fireware XTM Command Line Interface – Administrator of the TOE can connect to the CLI of the TOE from either the console management workstation or the local management workstation. In case of local connection (from the internal network), the TOE protects information as it is transmitted between the TOE and the local management workstation, using SSH.

- Fireware XTM Web UI – Administrator of the TOE can connect to the TOE either locally or remotely, using a standard web browser. The web browser must point to the IP address of the TOE over the correct port number. The TOE protects information when it is transmitted between the TOE and the local management workstation, and also when it is transmitted between the TOE and the remote management workstation, using TLS.

1.4.1 Brief Description of the Components of the TOE

As stated in Section 1, the TOE is composed of software (Fireware XTM Operating System) and hardware (specific model of XTM Firewalls product family). The following paragraphs provide a brief description of the components of the TOE.

1.4.1.1 Fireware XTM Operating System (Software)

Fireware XTM Operating System is a proprietary OS developed by WatchGuard that runs on the XTM Firewall devices. Customers can unlock either the Fireware XTM OS or Fireware XTM Pro OS, according to the license they purchased.

1.4.1.2 Major Interfaces of XTM Firewall Device (Hardware)

All models of XTM Firewalls product family share the same types of hardware components. Below lists the different types of interfaces that are available on these devices.

1.4.1.2.1 Ethernet Ports

Each device in the WatchGuard XTM Firewalls product family provides a group of RJ[5]-45 Ethernet ports on the front panel of its chassis. These ports can be configured as follows:

[5] RJ – Registered Jack

1.4.1.2.1.1 External Interfaces

Administrators of the TOE can configure these ports as External Interfaces. External Interfaces are used to connect to external networks that may be untrusted (i.e. the Internet).

1.4.1.2.1.2 Trusted Interfaces

Administrators of the TOE can also configure the Ethernet ports of the XTM Firewall device to be Trusted Interfaces. Trusted Interfaces are used to connect to the private LAN[6] or internal network that needs to be protected.

1.4.1.2.2 Serial Interface

The Serial Interface, which is located on the back panel of the XTM Firewall device, is used to directly connect the XTM Firewall device to a console.

1.4.1.2.3 Liquid Crystal Display (LCD)

The LCD located in front of the chassis is used to display information about the status of the device.

1.4.1.2.4 LCD Keypad Scrolling Buttons

There are four buttons (Up Arrow, Down Arrow, Left Arrow, Right Arrow) on the front of the chassis, which users of the TOE use to select menus and options displayed in the LCD.

1.4.2 TOE Environment

In the CC-evaluated deployment of the TOE as shown in Figure 1 above, the software and hardware configuration of the TOE and its environment are as follows:

As shown in Table 4, there are 23 unique instances of the TOE.

In the CC-evaluated deployment, the following are the TOE environment components.

[6] LAN – Local Area Network

- Console Management Workstation – Any computer that is capable of supporting terminal application in VT[7]100 mode.

- Local Management Workstation – Any computer that supports either or both:

  - Web browsers (for Web UI) – IE[8] (6.x or 7.x); Firefox 2.x; Safari 2.0
  - SSH2 (for CLI)

- Remote Management Workstation – Any computer that supports running the web browsers mentioned above.

- WatchGuard Log Server– Any Linux or Unix machine running the WatchGuard Log Server software. In the CC-evaluation of the TOE, the TOE is configured to send the audit data to a WatchGuard Log Server.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

The TOE boundary is drawn around the physical WatchGuard XTM Firewall device. All individual models (listed in Table 4) of the WatchGuard XTM Firewalls product family contain the following common components on the front of the chassis. They are:

- LCD
- LCD Keypad Scrolling Buttons

[7] VT – Virtual Terminal

[8] IE – Internet Explorer

- Ethernet ports (RJ-45)
- USB[9] ports

Figure 2 below shows the components listed above.

Figure 2 – Front View of the XTM 8 Series Firewall Device

In CC-configuration of the TOE, Ethernet ports on each model of the WatchGuard XTM Firewalls can be configured in two different ways, as stated in Section 1.4.1. These configurations are:

- External Interface – used to connect to external network (typically the Internet) that is not trusted.
- Trusted Interface – used to connect to the private LAN or internal network that needs to be protected.

In the rear of the chassis, all individual models of the WatchGuard XTM Firewalls provide the following common components. They are:

- AC receptacle – Accepts a detachable AC power cord supplied with the device.

[9] USB – Universal Serial Bus

- Power switch – Controls the power supplied to the device.
- Fans – The fans decrease the internal temperature of the device.
- Serial Interface (Console) – A DB9 connector for the serial interface to the console.

Figure 3 below shows the components listed above.

Figure 3 – The Rear View of the XTM 8 Series Firewall

The TOE is designed to filter traffic coming through the TOE based on a set of rules that are created by a system administrator. Figure 4 below illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

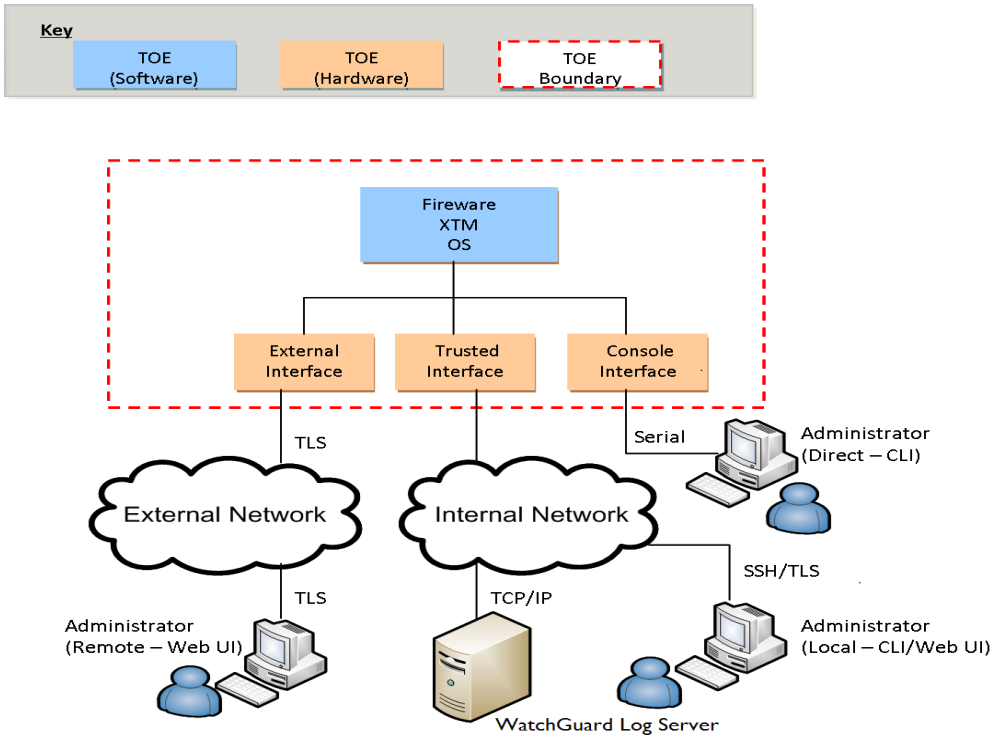

Figure 4 – Physical TOE Boundary

It should be noted that in the CC-evaluated deployment of the TOE, there are three modes of the TOE administration. These are:

- Direct Administration – in which the TOE administrator accesses the TOE from the CLI over Serial cable connection.

- Local Administration – in which the TOE administrator accesses the TOE from either CLI or Web UI on a workstation on an internal network that is located along with the TOE in the same physically secure location. The connection is secured by the use of SSH (for CLI) and TLS (for Web UI).

- Remote Administration – in which the TOE administrator accesses the TOE from an external network via TLS connection, using a Web UI.

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)

1.5.2.1 Security Audit

The TOE audits events in the form of logs. All audit records include at least the following information: identity of the subject that caused the event, the outcome of the event, and the date and time of the event. Audits can be viewed using both the CLI and the Web User Interface. Reviewing the audit records is an activity limited to TOE's administrative accounts (*status* and *admin* accounts). Both accounts can perform searches and sorting of the audit data.

The TOE contains small amount of internal memory which it utilizes to temporarily save the audit records. In addition, the TOE can be configured to send audit data to a WatchGuard Log Server. The TOE protects the unauthorized deletion of the audit data[10].

1.5.2.2 Cryptographic Support

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 SSH and TLS which perform the encryption and the decryption of data that is being passed.

Cryptographic operations are performed by a FIPS[11] 140-2-validated cryptographic module, certificate #XXX.

---

[10] Application Note: The TOE only protects the logs saved to internal memory and relies on the environment to provide protection for audit data sent to the WatchGuard Log Server.

1.5.2.3 User Data Protection

The TOE acts as a barrier between an organization's internal network (that is to be protected) and the external network (i.e., Internet). The TOE enables the information to flow through the TOE, both from inside and outside an organization's network by inspecting and allowing, denying and/or redirecting the flow of information (in forms of IP packets). The TOE achieves this by the use of policies and policy enforcement.

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

- 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)

It should be noted that for a product such as this TOE (i.e. Firewall device), it is critical that the memory used in assembling network packets is free of any residual information. The TOE achieves this by zeroizing the memory bits before reuse of the memory for assembling additional packets. This ensures that any previous information content of the memory is not revealed.

1.5.2.4 Identification and Authentication

The TOE provides two built-in administrative accounts: *admin*, and *status*. Since the *status* account is limited to read permission only, the term "TOE administrator" applies to the human user who holds the *admin* account. With the account (and the role) of *admin*, the TOE administrator can make changes to the TOE configuration and be able to save these changes.

[11] FIPS – Federal Information Processing Standard

Nevertheless, the *status* account is considered an administrative account as it is able to view all the TOE configuration data, including all policies and audit data.

Table 5 below summarizes the accounts, roles, and permissions for the administrative accounts of the TOE.

Table 5 – Accounts, Roles, Permissions for TOE administrative accounts

Account Name	Role	Permission	Initial Passphrase
admin	admin	Read, Write, Execute	readwrite
status	status	Read	read-only

Both the *admin* and *status* accounts are associated with human users. The TOE requires that human users associated with these accounts to be identified and authenticated before they are given access to the TOE.

1.5.2.5 Security Management

As shown in Table 5 above, the TOE supports two roles of administrative users: s*tatus* and *admin*. In addition, the TOE limits the ability to change the password of both the *status* account and the *admin* account to the TOE administrator.

Only the TOE administrator (*admin* role) is able to add, modify, delete and save the policies, thereby controlling the information flow through the TOE. Also, the TOE limits the ability to enable, disable, or modify the behavior of audit trail management to the TOE administrator.

The TOE provides restrictive default values for information flow control security attributes, and allows only the authorized administrator to set different values.

The ability to set the date and time (used to form timestamps) is limited to the TOE administrator. Also, the ability to reboot or shut down the TOE is limited to the TOE administrator.

1.5.2.6 Protection of the TOE Security Functionality

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

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionalities that are not part of the evaluated configuration of the TOE are:

- WatchGuard System Manager (WSM) – An application for network management with XTM Firewall devices. Administrators can use WSM to manage many different models of WatchGuard XTM Firewalls product family. This application provides a user management interface that is ideal for managing multiple instances of WatchGuard XTM Firewalls in a network. Use of WatchGuard System Manager is excluded in the CC-evaluated version of the TOE.

- WatchGuard Server Center – WatchGuard Server Center is another application that provides a user management interface. As it is a more robust application with a large installation footprint, it provides more administrative functionalities than the thin clients such as Fireware XTM Command Line Interface and Fireware XTM Web UI. Use of WatchGuard Server Center is excluded in the CC-evaluated version of the TOE.

- Optional Interface – Optional Interface is used to connect to a mixed trust area of the internal network, such as servers in a DMZ (demilitarized zone). Use of Optional Interface is excluded in the CC-evaluated version of the TOE.

- Wireless Interface – In Table 4, there are six instances of the TOE (XTM21-W, XTM22-W, XTM23-W, XTM25-W, XTM26-W, and XTM33-W) that offers the Wireless Interface. In the CC-evaluated version of the TOE, use of Wireless Interface is excluded.

- FTP Proxy – The TOE can be configured to act as a FTP proxy. When acting as a FTP proxy, the TOE establishes connection between the client and the real server on the protected side of the network, and allows or denies traffic according the policy set for the FTP service. In the CC-evaluated version of the TOE, use of FTP service is excluded.

- Telnet – In the CC-evaluated version of the TOE, use of Telnet protocol is excluded.

- USB ports – In the CC-evaluated version of the TOE, use of USB ports are excluded.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 6 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (Application-level Firewall; Traffic Filter Firewall); Parts 2 and 3 Interpretations from the CEM as of 2010/04/30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007; U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007.
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. Threats may be addressed either by the TOE or by the TOE's intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.1.1 Threats Addressed by the TOE

The TOE addresses all threats delineated in Table 7 from the Application-Level Firewall PP and Traffic Filter Firewall PP. These threats are restated from these protection profiles. All threats are common to both protection profiles with an exception of T.LOWEXP, which only applies to the Application-Level Firewall PP.

Table 7 – Threats Addressed by the TOE

Name	Description
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

T.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
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.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
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.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

3.1.2 Threat to be addressed by Operating Environment

The threat possibility discussed in Table 8 below must be countered by procedural measured and/or administrative methods.

Table 8 – Threats to be Addressed by Operating Environment

Name	Description
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with the Application-level Firewall PP are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB[12] 140-2 (level 1).

In CC-deployment of the TOE, remote administration is done through the external interface of the TOE by a TOE administrator accessing the TOE from an external network over a connection protected by TLS.

The following OSP in Table 9 is presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC-evaluated configuration:

[12] PUB – Publication

Table 9 – Organizational Security Policies

Name	Description
P.CRYPTO	Where the TOE requires FIPS-approved security functions, only National Institute of Standards and Technology (NIST) FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. 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. All of the assumptions are common to both Application-level and Traffic Filter protection profiles.

Table 10 – Assumptions

Name	Description
A.PHYSEC	TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the external networks.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows. All security objectives are common to both Application-level and Traffic Filter protection profiles with exception of O.EAL, which is unique to Application-level Firewall PP.

Table 11 – Security Objectives for the TOE

Name	Description
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security

	functionality by an authorized external IT entity.
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, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functionality, and must ensure that only authorized administrators are able to access such functionality.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
O.SECSTA	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

4.2 Security Objectives for the IT Environment

The following IT security objectives are to be satisfied by the environment:

Table 12 – Security Objectives for the IT Environment

Name	Description
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the

	TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	The TOE must be delivered, installed, and operated in a manner that maintains security.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
OE.PHYSEC	The TOE is physically secure.
OE.PUBLIC	The TOE does not host public data.
OE.REMACC	Authorized administrators may access the TOE remotely from the external networks.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE.

6.1 Conventions and Terminologies

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These are explained below:

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in the Application-level Firewall PP and Traffic Filter Firewall PP.

- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Deviations in phrasing of the SFRs that are required for compliance with the PP in this ST are indicated by the word **Refinement:**

In addition, the refinements done by the ST author to the SFRs from protection profiles are indicated in Table 13.

Omissions in phrasing of the SFRs that are required for compliance with the PP in this ST are indicated by strike through ~~as shown~~.

As the SFRs are taken from the Application-level Firewall PP and Traffic Filter Firewall PP, there are a number of terms that these protection profiles use. These terms are defined in Common Criteria, in Section 2.3 of Part 1:

- ***User*** – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- ***Human user*** – Any person who interacts with the TOE.
- ***External IT entity*** – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
- ***Role*** – A predefined set of rules establishing the allowed interactions between a user and the TOE.
- ***Identity*** – A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
- ***Authentication data*** – Information used to verify the claimed identity of a user.

From the above definitions given by the CC, both protection profiles derive the following terms and use them.

- ***Authorized external IT entity***[13] – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE are therefore trusted to not compromise the security policy enforced by the TOE.

- ***Authorized Administrator***[14] – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access

[13] In the CC-deployment of the TOE, there is no IT product or system that administers the TOE. Thus, there is no ***Authorized external IT entity*** in the TOE boundary. This term appears in the SFR statements only for completeness. It is not applicable to the CC-evaluation of the TOE.

[14] In CC-evaluation of the TOE, the human user who holds the *admin* account is the ***Authorized Administrator*** of the TOE.

control requirements once authenticated to the TOE are therefore trusted to not compromise the security policy enforced by the TOE.

6.2 Security Functional Requirements

The security functional requirements for this ST are the following components from Part 3 of the CC, summarized in Table 13. There are three SFRs (FCS_COP.1, FIA_UAU.4, FIA_UAU.5) on which the refinement by the ST author has been made. The explanation for the refinement of these SFRs is given in Section Protection Profile Rationale.

The SFRs listed in Table 13 are a subset of security functional requirements from Application-level Firewall protection profile and Traffic Filter Firewall protection profile, as the following SFRs are not applicable to this ST. These SFRs are:

- FDP_IFC.1(2)
- FDP_IFF.1(2)
- FMT_MSA.1(2)
- FMT_MSA.1(4)
- FPT_RVM.1

The explanation for not including these SFRs in this ST is given in Section Protection Profile Rationale.

Table 13 – TOE Security Functional Requirements

Name	Description	S	A	R	I
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	✓	✓	✓	
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic generation		✓	✓	
FDP_IFC.1 (1)	Subset information flow control (1)		✓		
FDP_IFF.1 (1)	Simple security attributes (1)		✓	✓	
FDP_RIP.1	Subset residual information protection	✓	✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.4	Single-use authentication		✓	✓	
FIA_UAU.5	Multiple authentication mechanisms		✓	✓	
FIA_UID.2	User identification before any action				
FMT_MOF.1 (1)	Management of security functions behavior (1)	✓	✓		✓
FMT_MOF.1 (2)	Management of security functions behavior (2)	✓	✓		✓
FMT_MSA.1 (1)	Management of security attributes (1)	✓	✓		
FMT_MSA.1 (3)	Management of security attributes (3)	✓	✓		

FMT_MSA.3	Static attribute initialization		✓	✓	
FMT_MTD.1 (1)	Management of TSF data (1)	✓	✓		
FMT_MTD.1 (2)	Management of TSF data (2)	✓	✓		
FMT_MTD.2	Management of limits on TSF data		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_STM.1	Reliable time stamps				

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [the events listed in Table 14].

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, [information specified in the third column of Table 14 (Auditable Event)].

Dependencies: FPT_STM.1 Reliable time stamps

Table 14 – Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Minimal	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.

FIA_UID.2	Basic	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.2	Basic	All use of the authentication mechanism.	The user identities provided to the TOE.
FIA_AFL.1	Minimal	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users' capability to authenticate.	The identity of the offending user and the authorized administrator.
FDP_IFF.1	Basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Minimal	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Minimal	Whenever policy rules are created, modified, edited, or deleted	The authorized administrator's role.
FMT_MOF.1	Extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [an authorized administrator] 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.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to perform [searches and sorting] of audit data based on:

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses].

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

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

FAU_STG.4.1

The TSF shall *prevent audited events, except those taken by the authorized* ***administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1

The TSF generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [the cryptographic key generation algorithm as listed in Table 15] and specified key sizes [the key sizes listed in Table 15] that meet the following: [the standards listed in Table 15]

Table 15 – Cryptographic Key Generation

Key Generation Method	Cryptographic Key Size	Standards
PRNG[15]	128 bit, 192 bit, 256 bit	ANSI X9.31 (certificate # 885)

Dependencies: FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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 140-2 zeroization requirements].

[15] PRNG – Pseudo-Random Number Generator

Dependencies: **FCS_CKM.1 Cryptographic key generation**

FCS_COP.1 **Cryptographic operation**

Hierarchical to: **No other components.**

FCS_COP.1.1

Refinement: The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with specified cryptographic algorithms [the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 16] and cryptographic key sizes [the cryptographic key sizes listed in the Key Sizes (bits) column of Table 16] that meets the following: [the list of standards in the Standards (Certificate #) column of Table 16].

Table 16 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Appliance / Module	Part # / Firmware	Standards (Certificate #)
Symmetric encryption and decryption	AES[16] CBC	128, 192, 256	XTM Cryptographic Processor XTM 3	P1020NSE	FIPS 197 (certificate # 1829)
			XTM Cryptographic Processor XTM 2	P1011NSE	FIPS 197 (certificate # 1828)
			XTM Cryptographic Processor XTM 330	P2020NSE	FIPS 197 (certificate # 1827)

[16] AES – Advanced Encryption Standard

			XTM Cryptographic Module Version 11.5.1	Firmware	FIPS 197 (certificate # 1662)
			XTM Cryptographic Processor XTM 8, XTM 1050, and XTM 2050	400BG233-P-G	FIPS 197 (certificate # 1660)
			XTM Cryptographic Processor XTM 5	350BG233-G	FIPS 197 (certificate # 1659)
			XTM Cryptographic Processor XTM 2	NHIXP435AE	FIPS 197 (certificate # 1658)
	Triple-DES[17] CBC[18]	112, 168	XTM Cryptographic Processor XTM 3	P1020NSE	FIPS 46-3 (certificate # 1182)
			XTM Cryptographic Processor XTM 2	P1011NSE	FIPS 46-3 (certificate # 1181)
			XTM Cryptographic Processor XTM 330	P2020NSE	FIPS 46-3 (certificate # 1180)

[17] DES – Data Encryption Standard

[18] CBC – Cipher Block Chaining

			XTM Cryptographic Module Version 11.5.1	Firmware	FIPS 46-3 (certificate # 1082)
			XTM Cryptographic Processor XTM 8, XTM 1050, and XTM 2050	400BG233-P-G	FIPS 46-3 (certificate # 1080)
			XTM Cryptographic Processor XTM 5	350BG233-G	FIPS 46-3 (certificate # 1079)
			XTM Cryptographic Processor XTM 2	NHIXP435AE	FIPS 46-3 (certificate # 1078)
Message Authentication	HMAC[19] with SHA[20]-1	20 bytes[21]	XTM Cryptographic Processor XTM 330	P2020NSE	FIPS 198 (certificate # 1083)
			XTM Cryptographic Processor XTM 3	P1020NSE	FIPS 198 (certificate # 1082)
			XTM Cryptographic Processor XTM 2	P1011NSE	FIPS 198 (certificate # 1081)

[19] HMAC – Hash-based Message Authentication Code

[20] SHA – Secure Hashing Algorithm

[21] Truncated to 12 bytes per RFC 2402

			XTM Cryptographic Module Version 11.5.1	Firmware	FIPS 198 (certificate # 977)
			XTM Cryptographic Processor XTM 8, XTM 1050, and XTM 2050	400BG233-P-G	FIPS 198 (certificate # 975)
			XTM Cryptographic Processor XTM 5	350BG233-G	FIPS 198 (certificate # 974)
			XTM Cryptographic Processor XTM 2	NHIXP435AE	FIPS 198 (certificate # 973)

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

6.2.3 Class FDP: User Data Protection

FDP_IFC.1 (1) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [UNAUTHETICATED INFORMATION FLOW CONTROL SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: pass information].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1 (2)[22] Subset information flow control (Not applicable to this ST)

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [AUTHETICATED INFORMATION FLOW CONTROL SFP] on:

[22] FDP_IFC.1(2) is not applicable to this ST. It is listed here for completeness of the Application-level Firewall PP.

a) [subjects: a human user or external IT entity that sends and receives FTP[23] and Telnet information through the TOE to one another; only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5;

b) information: FTP and Telnet sent through the TOE from one subject to another;

c) operation: initiate service and pass information].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 (1) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW CONTROL SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service].

[23] FTP – File Transfer Protocol

FDP_IFF.1.2

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

a) [Subject on an internal network 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, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network 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, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network].

FDP_IFF.1.3

The TSF shall enforce the [none].

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:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access of services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) For application protocols supported by the TOE (e.g., DNS[24], HTTP[25], SMTP[26], and POP3[27]), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC[28]). This shall be accomplished through protocol filtering proxies that are designed for that purpose].

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

[24] DNS – Domain Name Server

[25] HTTP – Hypertext Transfer Protocol

[26] SMTP – Simple Mail Transfer Protocol

[27] POP3 – Post Office Protocol version 3

[28] RFC – Request for Comment

FDP_IFF.1 (2)[29] Simple security attributes (Not applicable to this ST)

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [AUTHENTICATED INFORMATION FLOW CONTROL SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- no additional subject security attributes;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service (i.e., FTP and Telnet)].

FDP_IFF.1.2

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

a) [Subject on an internal network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.5;

[29] FDP_IFF.1(2) is not applicable to this ST. It is listed here for completeness of the Application-level Firewall PP.

- 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, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.5;
- 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, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network].

FDP_IFF.1.3

The TSF shall enforce the [none].

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:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access of services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall reject Telnet or FTP command requests that do not conforms to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose].

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

FDP_RIP.1 **Subset residual information protection**

Hierarchical to: **No other components.**

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [resources that are used by the subjects of the TOE to communicate through other subjects].

Dependencies: **No dependencies**

6.2.4 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [a Security Administrator-configurable integer] of unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;

b) association of a human user with the authorized administrator role;

c) a password to confirm the identity of the user].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

Refinement: The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the **authorized administrator authorized external IT entity accessing the TOE** ~~user~~ to be performed before the **authorized administrator or authorized external IT entity** ~~user~~ is authenticated.

FIA_UAU.1.2

Refinement: The TSF shall require each authorized **administrator or authorized external IT entity** ~~user~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **authorized administrator or authorized IT entity** ~~user~~.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.4.1

Refinement: The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

a) [authorized administrators;

b) ~~authorized external IT entities~~].

Dependencies: No dependencies

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide [password and single-use authentication mechanisms] to support user authentication.

FIA_UAU.5.2

Refinement: The TSF shall authenticate any user's claimed identity according to the [policy set by the TOE administrator to define which authentication mechanism rules:

a) [Single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

b) Single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;

~~c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;~~

d) Reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

Dependencies: **No dependencies**

FIA_UID.2 **User identification before any action**

Hierarchical to: **FIA_UID.1 Timing of identification**

FIA_UID.2.1

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

Dependencies: **No dependencies**

6.2.5 Class FMT: Security Management

FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to *modify the behavior of* the functions:

a) [start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify and view user attribute values defined in FIA_ATD.1;

d) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);

e) modify and set the time and date;

f) archive, create, delete, empty and review the audit trail;

g) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tool;

h) recover to the state following the last backup] to [an authorized administrator].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to: **No other components.**

FMT_MOF.1.1

The TSF shall restrict the ability to *enable, disable, determine and modify the behavior* of the functions:

a) [Audit trail management;

b) Backup and restore for TSF data, information flow rules, and audit trail data; and

c) Communication of authorized external IT entities with the TOE] to [an authorized administrator].

Dependencies: **FMT_SMF.1 Specification of management functions**

FMT_SMR.1 Security roles

FMT_MSA.1 (1) Management of security attributes

Hierarchical to: **No other components.**

FMT_MSA.1.1

The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW CONTROL SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes in a rule] the attributes [listed in section FDP_IFF.1(1)] to [the authorized administrator].

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 (2)[30] Management of security attributes (Not applicable to this ST)

Hierarchical to: **No other components.**

FMT_MSA.1.1

The TSF shall enforce the [AUTHENTICATED INFORMATION FLOW CONTROL SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes in a rule] the attributes [listed in section FDP_IFF.1(1)] to [the authorized administrator].

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 (3) Management of security attributes

Hierarchical to: **No other components.**

FMT_MSA.1.1

The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW CONTROL SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

[30] FMT_MSA.1(2) is not applicable to this ST. It is listed here for completeness of the Application-level Firewall PP.

FMT_MSA.1 (4)[31] Management of security attributes (Not applicable to this ST)

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [AUTHENTICATED INFORMATION FLOW CONTROL SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

Refinement: The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW CONTROL SFP and AUTHENTICATED INFORMATION FLOW CONTROL 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 [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes (1-4)
FMT_SMR.1 Security roles

[31] FMT_MSA.1(4) is not applicable to this ST. It is listed here for completeness of the Application-level Firewall PP.

FMT_MTD.1 (1) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to *query*, *modify*, *delete*, [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1 (2) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

FMT_MTD.2.1

The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

FMT_MTD.2.2

The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [actions specified in FIA_AFL.1.2].

Dependencies: FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the role [authorized administrator].

FMT_SMR.1.2

The TSF shall be able to associate **human** users with the **authorized administrator role**.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP[32] (Not applicable in this ST)

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within TSC is allowed to proceed.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Dependencies: No dependencies

[32] FPT_RVM.1 is not applicable to this ST. It is listed here for completeness of the Traffic Filter Firewall PP.

6.3 Security Assurance Requirements

The TOE assurance requirements for the protection profiles listed below are EAL2 augmented by ALC_FLR.2.

- U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007
- U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007.

The TOE meets the above assurance requirements for the PPs and in addition, satisfies the EAL4 assurance requirements. This section defines the assurance requirements for the TOE. Table below summarizes the requirements.

Table 17 – Assurance Requirements

Assurance Requirements	
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 ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification

Assurance Requirements	
	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 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

7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 18 lists the security functionality and their associated security requirements.

Table 18 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	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
Security Management	FMT_MOF.1 (1)	Management of security functions behavior (1)
	FMT_MOF.1 (2)	Management of security functions behavior (2)
	FMT_MSA.1 (1)	Management of security attributes (1)
	FMT_MSA.1 (3)	Management of security attributes (3)

	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1 (1)	Management of TSF data (1)
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMR.1	Security roles
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
User Data Protection	FDP_IFC.1 (1)	Subset information flow control (1)
	FDP_IFF.1 (1)	Simple security attributes (1)
	FDP_RIP.1	Subset residual information protection
	FMT_MTD.1 (2)	Management of TSF data (2)
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction

	FCS_COP.1	Cryptographic generation

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 one activity that occurs on the TOE. For example, TOE's denying of a packet based on a policy set is an *event*. TOE also captures information about allowed events to give a more completed picture of the activities on the network.

The log message system has several components, which are described below.

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

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

- Alarm log messages – Alarm log message 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 Log 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 messages are:

- Device start up and shut down
- Device and VPN 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: identity of the subject that caused the event, the outcome of the event, and the date and time of the event.

7.1.1.2 Audit Review

Audits can be viewed using both the CLI and the Web User Interface. Reviewing the audit records is an activity limited to TOE's administrative accounts (*status* and *admin* accounts). Both accounts can perform searches and sorting of the audit data.

7.1.1.3 Audit Storage

The TOE contains a small amount of internal memory which it utilizes to temporarily save the audit records. In addition, the TOE is configured to send audit data to a WatchGuard Log Server. The TOE protects the unauthorized deletion of the audit data. The TOE also prevents the loss of audit data by setting rotation parameters to the TOE administrator-configurable number.

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

7.1.2 Cryptographic Support

The TOE protects the confidentiality and integrity of 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 SSH and TLS which perform the encryption and the decryption of data that is being passed.

All cryptographic functions used in SSH and TLS are performed by a FIPS 140-2 validated cryptographic module.

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

7.1.3 User Data Protection

The *security policy* of an organization in the context of computer networking is a set of rules to protect computer network of an organization and the information that goes through it. By default, The TOE denies all packets that are not specifically allowed. The TOE enables the administrator of the TOE to add a policy. Through the use of policy, the administrator configures a set of rules that tell the TOE to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

The TOE uses two categories of policies to filter network traffic: *packet filters* and *proxies*. A packet filter policy examines each packet's IP and TCP/UDP[33] 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 TOE administrator can configure an SMTP[34] proxy to deny email if the headers are

[33] UDP – User Datagram Protocol

[34] SMTP – Simple Mail Transfer Protocol

not properly set. The TOE supports proxy policies for many common protocols, including DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP[35], SMTP, and TCP/UDP.

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

- 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)

It should be noted that for a product such as TOE (i.e. Firewall device), it is critical that the memory used in assembling network packets is free of any residual information. TOE achieves this by zeroizing the memory bits before reuse of the memory for assembling additional packets. This ensures that any previous information content of the memory is not revealed.

TOE Security Functional Requirements Satisfied: FDP_IFC.1(1), FDP_IFF.1(1), FDP_RIP.1

7.1.4 Identification and Authentication

The TOE provides two built-in administrative accounts: *admin*, and *status*. These two accounts have default passphrases pre-supplied for them. They are *readwrite, and read-only* for the *admin* and *status* accounts, respectively. Theses passphrases can be changed after the TOE is configured for the first time.

[35] SIP – Session Initiation Protocol

Table 19 below summarizes the characteristics of these accounts.

Table 19 – Types of Administrative Accounts for the TOE

Account Name	Initial Passphrases	Note
admin	readwrite	"admin" account allows full access to the TOE. Administrator uses this account and the associated passphrase to save configuration changes to the TOE. It is also the account that can change the passphrases for both the "admin" and the "status" accounts.
status	read-only	"status" account allows 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.

Both the *admin* and *status accounts* are associated with human users. TOE requires that human users associated with these accounts to be identified and authenticated before they are given access to the TOE.

The TOE provides protection against unauthorized users gaining access to the TOE by allowing a settable number of unsuccessful login attempts for the *status* account before the *status* account is locked out. When the *status* account is locked out, it can be unlocked by the TOE administrator who holds the *admin* account.

The TOE allows the remote administration of the TOE from an external network over TLS connection. This demonstrably satisfies the single-use authentication requirement of the FIA_UAU.4.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.2.

7.1.5 Security Management

The TOE supports two roles of administrative users: *status* and *admin*. Since the *status* role is limited to read permission only, it is the *admin* role that is given the full authorization of the TOE administrator with ability to create, modify, delete, and save the TOE configuration data. In

addition, the TOE limits the ability to change the password of both the *status* account and the *admin* account to the TOE administrator.

Only the TOE administrator (*admin* role) is able to add, modify, delete and save the policies, thereby controlling the information flow through the TOE. Also, the TOE limits the ability to enable, disable, or modify the behavior of audit trail management to the TOE administrator.

The TOE provides restrictive default values for information flow control security attributes, and allows only the authorized administrator to set different values. Below lists some of the major default values that are pre-set out of the box, regarding information flow control security attributes:

- Trusted network default IP addresses – Depending on the TOE instances (in Table 4), this value is either 192.168.111.1 or 10.0.0.1
- The default port number for Fireware XTM Web UI is 8080.
- By default, the External network is configured to get an IP address with DHCP[36].
- By default, the optional network is disabled.
- By default, Ping requests received on the external network are denied.
- By default, all incoming policies are denied and the outgoing policy allows all outgoing traffic.
- By default, the TOE is set up only 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 ability to set the date and time (used to form timestamps) is limited to the TOE administrator. Also, the ability to reboot or shut down the TOE is limited to the TOE administrator.

[36] DHCP – Dynamic Host Configuration Protocol

TOE Security Functional Requirements Satisfied: FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(3), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.2, 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 by a user assuming an authorized administrator role. Setting the clock is done through the CLI by an authorized administrator. The time stamps are considered reliable because they are all from the same source and only the authorized administrator has access to change the time. Changing the time is also an auditable event, so if the clock has been changed, there will be a record of it.

TOE Security Functional Requirements Satisfied: FPT_STM.1

8 Rationale

8.1 Protection Profile Conformance Claims

This chapter provides detailed information in reference to the Protection Profile conformance.

8.1.1 Protection Profile References

U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007

U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007.

8.1.2 Protection Profile Rationale

The following tailoring was applied to the Application-level Firewall PP and Traffic Filter PP to produce this ST.

8.1.2.1 Assumptions

In both the ALF and TTF, A.REMACC is stated as:

- *Authorized administrators may access the TOE remotely from the internal and external networks.*

In this ST, A.REMACC has been modified to:

- *Authorized administrators may access the TOE remotely from the external networks.*

The TOE configuration has three modes of TOE administration as explained in Section 1.5.1. As the scope of Local Administration covers the access to the TOE from the internal networks, Remote Administration happens only from the external networks.

8.1.2.2 Security Objectives for the IT Environment

To be consistent with the change applied to the A. REMACC, OE.REMACC has been modified to:

Authorized administrators may access the TOE remotely from the external networks.

Also, it should be noted that the ST author has changed the naming style of Security Objectives for the IT environment. In the Application-level Firewall PP and Traffic Filter Firewall PP, the

prefix of "O." is used. In this ST, the prefix of "OE." is used, to distinguish the Security Objectives for the IT Environment from the Security Objectives for the TOE.

8.1.2.3 Organizational Security Policy

As the TOE implements multiple FIPS-approved cryptographic algorithms including AES and TDES[37], the P.CRYPTO statement has been modified from:

- *AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).*

to:

- *Where the TOE requires FIPS-approved security functions, only National Institute of Standards and Technology (NIST) FIPS compliant cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).*

8.1.2.4 Security Functional Requirements

In this ST, as the FTP and Telnet service were not included in the TOE boundary, the following SFRs from Application-level Firewall PP are not included: FDP_IFC.1(2), FDP_IFF.1(2), FMT_MSA.1(2), and FMT_MSA.1(4). Also, as the ST conforms to the part 3 of the CC, FPT_RVM .1 from Traffic Filter Firewall PP is not included.

Refinements to FIA_UAU.4 and FIA_UAU.5 have been applied as the CC-evaluated deployment of the TOE does not include the authorized external IT entity.

Refinement to the FCS_COP has been applied to reflect the modifications of the statement made in P.CRYPTO. Below shows the FCS_COP.1 statement from the Application-level Firewall PP[38].

[37] TDES – Triple Data Encryption Standard

- *FCS_COP.1.1 -The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67)] and cryptographic key sizes [that are at least 128 binary digits in length] that meet the following: [FIPS PUB 140-2 (Level 2)].*

In the ST, the above statement has been refined by the ST author to:

- ***FCS_COP.1.1***

  Refinement: The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with specified cryptographic algorithms [the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 16] and cryptographic key sizes [the cryptographic key sizes listed in the Key Sizes (bits) column of Table 16] that meets the following: [the list of standards in the Standards (Certificate #) column of Table 16].

It should be noted that the TOE implements AES and TDES algorithms as indicated in Table 16.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus	O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and

[38] Traffic Filter Firewall PP has the same FCS_COP.1statement, except it uses FIPS PUB 140-2 (Level 1)

allowing an attacker to escape detection.	of security functions related to audit.	that authorized administrators are accountable for the use of security functions related to audit.
T.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.	OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.	This security objective is necessary to counter the treat: T.TUSAGE because it ensures that authorized administrators receive the proper training.
T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.
T.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.	This security objective is necessary to counter the threat: T.LOWEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential.
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.	O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.	This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

T.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.	OE.GUIDAN The TOE must be delivered, installed, and operated in a manner that maintains security.	This security objective is necessary to counter the treat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, intalled, administered, and operated in a secure manner.
T.MEDIAT An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.	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, and must ensure that residual information from a previous information flow is not transmitted in any way.	This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
T.OLDINF Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.	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, and must ensure that residual information from a previous information flow is not transmitted in any way.	This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functionality, and must ensure that only authorized	This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the

attackers actions.	administrators are able to access such functionality.	TOE security functionality.
	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functionality.
T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functionality.
	O.SECSTA The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.
T.NOAUTH An unauthorized person may attemp to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided bu the TOE.	O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.	This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.
	O.IDAUTH The TOE must uniquely	This security objective is necessary to counter the threat: T.NOAUTH because it

	identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.	requires that users be uniquely identified before accessing the TOE.
	O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functionality by an authorized external IT entity.	This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functionality.
	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functionality, and must ensure that only authorized administrators are able to access such functionality.	This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functionailty.
	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functionality.
	O.SECSTA The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and	This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

	data.	
T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.	O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functionality, and must ensure that only authorized administrators are able to access such functionality.	This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functionality.
	O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
T.ASPOOF An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.	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, and must ensure that residual information from a previous information flow is not	This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that

	transmitted in any way.	no residual information is transmitted.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 21 – Policies: Objectives Mapping

Policies	Objectives	Rationale
P.CRYPTO Where the TOE requires FIPS-approved security functions, only National Institute of Standards and Technology (NIST) FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).	O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.	This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 22 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale

A.PHYSEC TOE is physically secure.	OE.PHYSEC The TOE is physically secure.	OE.PHYSICAL is a restatement of the assumption, and therefore traces to the assumption trivially and is suitable for covering the assumptions.
A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.	OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC The TOE does not host public data.	OE.PUBLIC The TOE does not host public data.	The TOE does not host public data.
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the	OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

connection is part of the TOE.	the connection is part of the TOE.	
A.NOREMO Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.	OE.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networs.
A.REMACC Authorized administrators may access the TOE remotely from the external networks.	OE.REMACC Authorized administrators may access the TOE remotely from the external networks.	Authorized administrators may access the TOE remotely from the external networks.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended Security Functional Requirements in this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE Security Assurance Requirements.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 23 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.	FAU_GEN.1 Audit Data Generation	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
	FIA_UID.2 User identification before any action	This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.
O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	FAU_GEN.1 Audit Data Generation	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
	FAU_SAR.1 Audit review	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
	FAU_SAR.3	This component ensures that a variety of searches and sorts

	Selectable audit review	can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
	FPT_STM.1 Reliable time stamps	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.	FCS_COP.1 Cryptographic generation	This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.
O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.	FCS_CKM.1 Cryptographic key generation	This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.
	FCS_CKM.4 Cryptographic key destruction	This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or

		external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.
	FCS_COP.1 Cryptographic generation	This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.
O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.	FIA_ATD.1 User attribute definition	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.
	FIA_UAU.1 Timing of authentication	This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which

		to audit any of their actions. This component traces back to aand aids in meeting the following objectives: O.IDAUTH and O.SINUSE
	FIA_UAU.5 Multiple authentication mechanisms	This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. A SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.
	FIA_UID.2 User identification before any action	This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.
O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functionality by an authorized external IT entity.	FMT_MOF.1 (1) Management of security functions behavior	This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN,

		O.LIMEXT, and O.SECSTA.
	FMT_MOF.1 (2) Management of security functions behavior	This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.
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, and must ensure that residual information from a previous information flow is not transmitted in any way.	FDP_IFC.1 (1) Subset information flow control	This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.
	FDP_IFF.1 (1) Simple security attributes	This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
	FDP_RIP.1	This component ensures that neither information that had

	Subset residual information protection	flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.
	FMT_MSA.1 (1) Management of security attributes	This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MSA.1 (3) Management of security attributes	This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MSA.3 Static attribute initialization	This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functionality, and must ensure that only authorized administrators are able to access such functionality.	FAU_STG.1 Protected audit trail storage	This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FAU_STG.4 Prevention of audit data loss	This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FIA_ATD.1 User attribute definition	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and

		O.SECFUN.
	FMT_MOF.1 (2) Management of security functions behavior (2)	This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.
	FMT_MSA.1 (1) Management of security attributes	This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MSA.1 (3) Management of security attributes	This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MTD.1 (1)	This component ensures that the TSF restrict abilities to

	Management of TSF data	query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
	FMT_MTD.1 (2) Management of TSF data	This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
	FMT_MTD.2 Management of limits on TSF data	This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.
	FMT_SMR.1 Security roles	Each of the CC class FMT components in this Protection Profile depends on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.
O.SELPRO The TOE must protect itself	FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering, the

against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	Protected audit trail storage	security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FAU_STG.4 Prevention of audit data loss	This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FIA_AFL.1 Authentication failure handling	This component ensures that human users who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible

		again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.
O.SECSTA The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1 Protected audit trail storage	This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FAU_STG.4 Prevention of audit data loss	This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.
	FMT_MOF.1 (1) Management of security functions behavior	This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the

		authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.
	FMT_MSA.1 (1) Management of security attributes	This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MSA.1 (3) Management of security attributes	This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
	FMT_MSA.3 Static attribute initialization	This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.
O.SINUSE The TOE must prevent the reuse of authentication data for	FIA_UAU.1 Timing of authentication	This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users

users attempting to authenticate to the TOE from a connected network.		are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE
	FIA_UAU.4 Single-use authentication	This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: O.SINUSE
	FIA_UAU.5 Multiple authentication mechanisms	This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. A SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.SINUSE and

		O.IDAUTH.

8.5.2 Security Assurance Requirements Rationale

EAL4, augmented with ALC_FLR.2 was chosen to provide a moderate- to high-level of assurance that is consistent with the requirements of both the Application-level Firewall PP and Traffic Filter Firewall PP. The chosen assurance level is appropriate with the threats defined for the environment. At EAL4+, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of enhanced-basic.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 24 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 24 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FMT_SMR.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_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	

FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_IFC.1 (1)	FDP_IFF.1 (1)	✓	
FDP_IFF.1 (1)	FMT_MSA.1 (1)	✓	
	FDP_IFC.1 (1)	✓	
FDP_RIP.1	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UAU.4	No dependencies	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UID.2	No dependencies	✓	
FMT_MOF.1 (1)	FMT_SMF.1	No	Refer to the note below
	FMT_SMR.1	✓	
FMT_MOF.1 (2)	FMT_SMF.1	No	Refer to the note below
FMT_MSA.1 (1)	FDP_IFC.1 (1)	✓	
	FMT_SMF.1	No	Refer to the note below
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_IFC.1 (1)	✓	

(3)	FMT_SMF.1	No	Refer to the note below
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1(3)	✓	
	FMT_SMR.1	✓	
	FMT_MSA.1 (1)	✓	
FMT_MTD.1 (1)	FMT_SMR.1	✓	
	FMT_SMF.1	No	Refer to the note below
FMT_MTD.1 (2)	FMR_SMF.1	No	Refer to the note below
	FMT_SMR.1	✓	
FMT_MTD.2	FMT_MTD.1 (1)	✓	
	FMT_MTD.1 (2)	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1
FPT_STM.1	No dependencies	✓	

Note: Although the FMT_SMF.1 requirement is a dependency of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1, it has not been included in this ST, as it was not included in the protection profiles. The following rationale is given.

The requirements FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 express the functionality required by the TSF to provide the specified functions to manage TSF data, security attributes and management functions. These requirements make it clear that the TSF has to provide the functions to manage the identified data,

attributes and functions. Therefore FMT_SMF.1 is not necessary.

9 Acronyms

This section describes the acronyms used in this document.

Table 25 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ALF	Application-level Firewall
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light-emitting diode
MGMT	Management
OS	Operating System
OSP	Organizational Security Policy
POP3	Post Office Protocol version 3
PP	Protection Profile

Acronym	Definition
PRNG	Pseudo-Random Number Generator
PUB	Publication
RFC	Request for Comment
RJ	Registered Jack
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hashing Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
ST	Security Target
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Triple Data Encryption Standard
TFF	Traffic Filter Firewall
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UDP	User Datagram Protocol
UI	User Interface
USB	Universal Serial Bus
VPN	Virtual Private Network
VT	Virtual Terminal
WSM	WatchGuard System Manager
XMT	eXtensible Threat Management

Prepared by:

Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220

Fairfax, VA 22033

United States of America

Phone: +1 703 267 6050

Email: info@corsec.com

http://www.corsec.com