WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1

Security Target

Version 1.0

Final

August 3, 2000

Prepared for:

WatchGuard Technologies
316 Occidental Ave S, Suite 200
Seattle, WA 98104

Prepared by:

Computer Sciences Corporation
7471 Candlewood Road
Hanover, MD 21076

Revisions to Document		
Date	**Version**	**Changes Made**
24 April 2000	1.0	Original
13 June 2000	1.1	Addressed EDR 002
06 July 2000	1.1	Addressed EDR 004
18 July 2000	1.1	Addressed EDR 002
3 August 2000	1.3	Addressed EDR 015

Table of Contents

List of Tables

WatchGuard LiveSecurity System with Firebox II Version 4.1 Security Target

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Environment).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

2 The structure and contents of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the WatchGuard LiveSecurity System with Firebox II. This ST targets an Evaluation Assurance Level (EAL) 2 level of assurance.

- **ST Title:** WatchGuard LiveSecurity System with Firebox II Version 4.1 Security Target
- **ST Version:** 1.0
- **TOE Identification:** WatchGuard LiveSecurity System with Firebox II Version 4.1
- **CC Identification:** Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
- **ST Evaluation:** Computer Sciences Corporation

Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and acronyms used throughout the remainder of the document.

1.2.1 Conventions

5 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

6 The CC allows several operations to be performed on functional requirements; *assignment, iteration, refinement*, and *selection* are defined in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- Iteration of a component is used when a component is repeated more than once with varying operations. Iterated components are given unique identifiers by an iteration number or name in parenthesis appended to the component and element identifiers.
- 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 picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by <u>*underlined italicized text.*</u>

7 Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.2.2 Terminology

8 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

- ***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 be either the full or abbreviated name of that user or a pseudonym.

- ***Authentication data*** - Information used to verify the claimed identity of a user.

9 In addition to the above general definitions, this Security Target provides the following specialized definitions:

- ***Authorized Administrator*** - A role to which an authorized administrator is associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once identified to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

1.2.3 Acronyms

10 The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard Publication
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.3 Security Target Overview

11 The WatchGuard LiveSecurity System consists of a suite of management and security software tools coupled with a plug-and-play network appliance called the WatchGuard Firebox II. The WatchGuard LiveSecurity System with Firebox II, herein referred to as WatchGuard, is a reliable, flexible, and inexpensive firewall solution. WatchGuard uses dynamic packet filtering rules to allow the authorized administrator to add and remove rules depending on network activity. WatchGuard uses a hybrid technology of dynamic packet filtering and transparent proxies to control and monitor the flow of IP packets through the firewall. The transparent proxies used with WatchGuard provide added security and filtering options for connections. WatchGuard consists of four major components:

- LiveSecurity Broadcast Network – a subscription service that sends software updates from the external network directly to the Control Center platform. (This component is not part of the evaluated TOE configuration).
- Control Center – software executing on a Windows NT platform that configures and monitors the Firebox II. The Control Center also contains the tools to perform logging and notification of firewall events.
- Event Processor – software executing on a Windows NT platform responsible for logging firewall generated records and notifying the authorized administrator when a triggering event is detected.
- Firebox II – a hardware firewall device that runs the transparent proxies and the dynamic packet filter to control the flow of IP information. The Firebox II is designed to be a “network appliance” which is an easy to use, low maintenance component that plugs into an Ethernet network.

1.4 Common Criteria Conformance

12 The WatchGuard LiveSecurity System with Firebox II is Part 2 and Part 3 conformant. The TOE is conformant to Evaluation Assurance Level (EAL 2).

2 TOE DESCRIPTION

13 This Chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1.1 Product Type

14 The WatchGuard is comprised of four components:

- LiveSecurity Broadcast Network,
- Control Center,
- Event Processor, and
- Firebox II.

15 The Control Center is a toolkit of applications that configures, manages, and monitors the Firebox II, while the Firebox II performs as an Application-filter and Traffic-filter firewall. A definition of Application-level and Traffic-filter firewall is provided below:

- *Application-level Firewall* – mediates flows between clients and servers located on internal and external networks governed by the firewall. An application-level firewall may employ proxies to screen information flows to application level protocol standards. Only an authorized administrator has the authority to change the security policy rules. Only valid requests are relayed to the actual server by the proxy server on either an internal or an external network.

- *Traffic-filter Firewall* – selectively routes information flows between an internal and an external network according to a site's security policy rules, the default policy being *deny all*. Only an authorized administrator has the authority to change the security policy rules. Traffic filtering decisions are made on the source address, destination address, transport layer protocol, source port, destination port, and are based on the interface on which the packet arrives or goes out.

The LiveSecurity Broadcast Network provides subscription software to receive software updates and is not part of the evaluated TOE configuration.

2.1.2 Scope and Boundaries of the Evaluated Configuration

16 This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.1.2.1 Physical Scope and Boundary

17 The TOE configuration consists of two physical components:

- One Firebox II, a hardware device that runs the transparent proxies and dynamic packet filtering to control the flow of IP information. The WatchGuard Firebox II is designed to be a “Network Appliance” – an easy to use, low maintenance component that plugs into the network

- One NT Workstation with Service Pack 4.0 installed, referred to as the Management Station. The Management Station provides the execution environment for the Control Center software which configures and monitors the Firebox II. Also it contains the WatchGuard Event Processor – software that controls logging and notification of firewall events.

18 The evaluated TOE configuration includes the hardware and software elements identified in Table 1.

Table 1: Evaluated TOE Configuration Components

Components	Items
Software	WatchGuard LiveSecurity System, Version 4.1 HTML Level 2 Capable Web Browser. Microsoft Windows NT 4.0 with Service Pack 4
Hardware	Firebox II
	Intel x86-Pentium with 64 MB Memory for Windows NT 4.0 25 MB Hard Disk Space to install WatchGuard Modules 15 MB Hard Disk Space minimum for log file One CD-ROM drive to install WatchGuard from its CD-ROM distribution disk

Figure 1 illustrates the physical boundary of the TOE.

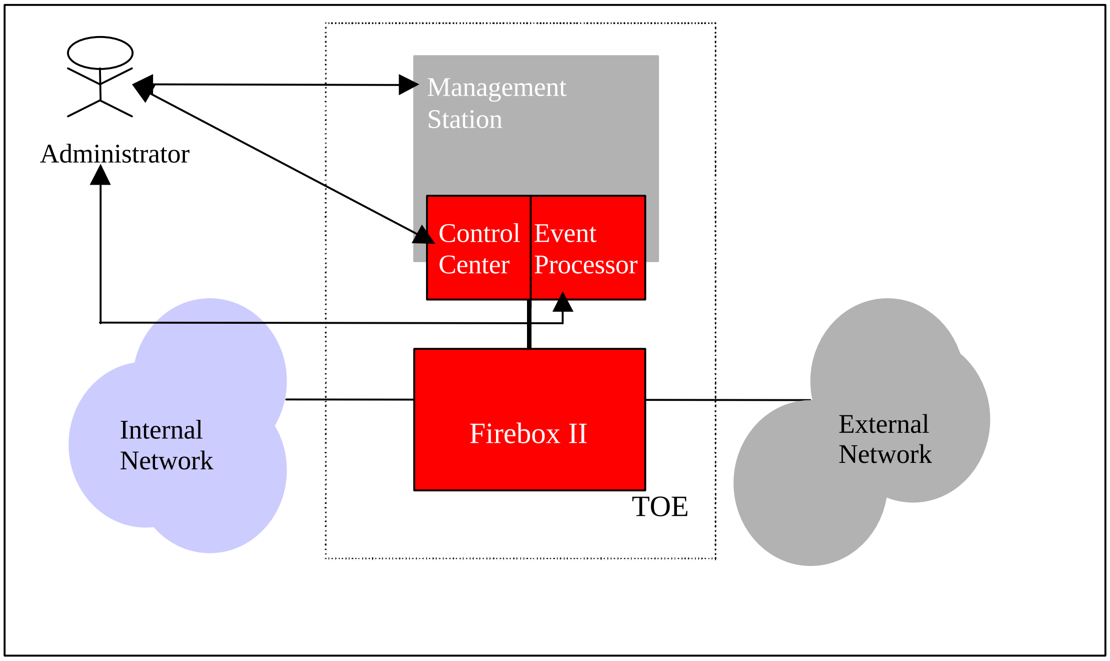

Figure 1 TOE Physical Boundary

2.1.2.2 Logical Scope and Boundary

19 The TOE provides the following security features:

- **Security Audit:** The Control Center provides the authorized administrator with the ability to specify which traffic-filter and application-filter log events to detect on the Firebox II. These events are time-stamped and sent to the Event Processor to be recorded within the audit log. The Control Center is used by the authorized administrator to review audit data generated by the Firebox II. The Control Center provides the authorized administrator with the ability to search the audit log by keywords and field types and sort the audit log in chronological order.
- **User Data Protection:** The Firebox II provides SMTP application level protection. The Firebox II ensures that information contained in packets is no longer accessible once the packet has been processed. The Firebox II enforces the information flow Security Policy for all flows through the TOE.
- **Privacy:** NAT hides the internal network addresses from hosts on an external network. WatchGuard supports two types of NAT: Dynamic NAT and Static NAT.
- **Authentication and Identification**: The Control Center provides role identification. This permits separation of *review* operations from *review/modify* operations. The Control Center and Firebox II establish an encrypted channel to securely exchange control and status information. The Windows NT login interface is used to provide authentication and identification for authorized administrators accessing the Management Station.

- **Security Management:** The Control Center provides the authorized administrator with the ability to manage the information flow Security Policy enforced by the Firebox II, and audit events generated by the Firebox II. It also permits the authorized administrator to examine information flow rules, configuration parameters, and the audit log.

- **Protection of Security Functions:** Interfaces between the external and internal networks are provided by the Firebox II. It assures that information flow from the external and internal networks cannot flow to or from the Management Station.

20 Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Remote Administration;

- User Authentication for Internet Services

- Firebox II Virtual Private Networking (Remote User, Branch Office);

- LiveSecurity Broadcast Network;

- WebBlocker; and

- Windows NT 4.0 features not used by the TOE.

The assessment of the strength of the encryption algorithm used to protect communications between the Firebox II and the Management Station is not part of the TOE evaluation.

3 TOE SECURITY ENVIRONMENT

21 The TOE is a dual-homed device mediating information flows between two networks such as an internal, protected network, and an external, hostile network. The TOE is intended for use in small to medium size organizations in which system administration is the responsibility of one, or at most, two people. The firewall’s purpose is to restrict access to services provided by and the information stored on the internal network and to protect applications on the internal network from typical attacks generated from the external network. To clarify and define the security environment, assumptions about the security environment and/or the manner in which the TOE will be used are provided.

22 The assumptions and threat identification combined with any organization security policy statement or rules requiring TOE compliance completes the definition of the security environment. It is necessary that a comprehensive security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- ***Physical security*** - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.
- ***Procedural security*** - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.
- ***Personnel security*** - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.1 Assumptions

23 The specific conditions listed in Table 2 are assumed to exist for the TOE.

Table 2: Assumptions for the TOE

Name	Description
A.LOWEXP	Potential threat agents attempting to attack the TOE are considered to be of lower than a low attack potential such that their level of expertise is of a layman with no specialized tools.
A.NOEVIL	Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.ONEWAY	Information cannot flow between the internal and external networks unless it passes through the Firebox II.
A.NOREM	Human users cannot access the TOE remotely from the internal or external networks.

Name	Description
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection.
A.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.

3.2 Threats

24 Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats Addressed by the TOE

25 Table 3 identifies threats to the assets against which specific protection within the TOE is required. In all cases the threat agent is considered to possess a minimum attack potential such that their level of expertise that of a layman, possesses no specialized tools, and only public knowledge of the TOE.

Table 3: Threats Addressed by the TOE

Name	Description
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions provided by the TOE.
T.ASPOOF	An unauthorized user may carry out spoofing in which information flows through the TOE into the connected network by using a spoofed source address.
T.MEDTF	An unauthorized user may send impermissible network information through the TOE which results in the exploitation of resources on the protected network.
T.MEDAPPL	An unauthorized user may send impermissible application information through the TOE which results in the exploitation of resources on the protected network.
T.OLDINF	An unauthorized user may gather residual information from a previous information flow by monitoring the padding of the information flows from the TOE.
T.AUDACC	Users may not be accountable for the actions that they conduct because security-relevant events are not logged.
T.NODETECT	An unauthorized user may continuously attempt to bypass the TSP without detection in order to successfully send information through the TOE.

Name	Description
T.SELPRO	An unauthorized user may read, modify, or destroy security critical TOE configuration data.
T.PRIVACY	With knowledge of the real IP addresses of external IT entities on the internal network, an attacker may have enough information about the internal network to affect the internal network in an undesirable manner.

3.2.2 Threats Addressed by the Operating Environment

26 Table 4 identifies threats to the assets against which specific protection within the TOE environment is required.

Table 4: Threats Addressed by Operating Environment

Name	Description
T.USAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by a human user.

3.3 Organizational Security Policies

27 The WatchGuard LiveSecurity System with Firebox II ST does not identify any organizational security policy statements or rules with which the TOE must comply.

4 SECURITY OBJECTIVES

28 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the Operating Environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

29 Table 5 identifies the security objectives to address security concerns that are directly addressed by the TOE.

Table 5: Security Objectives for the TOE

Name	Description	Threat
O.IDAUTH	The TOE will uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.	T.NOAUTH
O.IDENTIFY	The TOE will uniquely identify all users before using TOE functions to grant access to the external or internal network	T.NOAUTH
O.MEDTF	The TOE will mediate the flow of all information from users on a connected network to users on another connected network based on network layer information as configured by the authorized administrator	T.ASPOOF T.MEDTF
O.MEDAPPL	The TOE will mediate the flow of all information from users on a connected network to users on another connected network based on application layer information as configured by the authorized administrator.	T.MEDAPPL
O.INFPRO	The TOE will ensure that residual information from a previous information flow is not transmitted in any way.	T.OLDINF
O.SELPRO	The TOE will protect itself against attempts by unauthorized user to bypass, deactivate, or tamper with TOE security functions.	T.SELPRO

Name	Description	Threat
O.AUDIT	The TOE will provide the means of recording, detecting violations, alerting, and reviewing security relevant events so as to assist an authorized administrator in detecting or identifying potential attacks. The TOE will take appropriate action for detection of violations as configured by the authorized administrator.	T.AUDACC T.NODETECT
O.ADMIN	The TOE will provide functionality to allow an authorized administrator to manage access and use of security functions, and will ensure that only authorized administrators are able to access such functionality.	T.NOAUTH
O.PRIVACY	The TOE must ensure that users on the external network can not determine the addresses of the users on the internal network as specified by the authorized administrator.	T.PRIVACY

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

30 Table 6 identifies security objectives to address security concerns that are directly addressed by the TOE environment.

Table 6: Security Objectives for the Environment

Name	Description	Assumption(s) /Threats
OE.LOWEXP	Those responsible for the TOE must use the TOE in an environment in which the threat of malicious attacks at discovering exploitable vulnerabilities is considered low.	A.LOWEXP
OE.NOEVIL	Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	A.NOEVIL
OE.ONEWAY	Those responsible for the TOE must ensure that no connections are provided such that information flow among the internal and external networks physically bypasses the Firebox II.	A.ONEWAY
OE.NOREM	Those responsible for the TOE must ensure that no user can remotely access the TOE from the internal or external networks.	A.NOREM

Name	Description	Assumption(s) /Threats
OE.GENPUR	Those responsible for the TOE must ensure that the Firebox II and Management Station only stores and executes security-relevant applications and only stores data required for its secure operation.	A.GENPUR
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection.	A.DIRECT
OE.PHYSEC	Those responsible for the TOE must ensure that the processing resources of the TOE that depend on hardware security features are located within controlled access facilities that mitigate unauthorized, physical access.	A.PHYSEC
OE.GUIDANCE	Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, and operated in a manner that maintains security.	T.USAGE
OE.ADMTRA	Administrators are trained as to establishment and maintenance of security policies and practices.	T.USAGE

5 TOE SECURITY REQUIREMENTS

31 IT security requirements include:

- TOE security requirements, and (optionally)
- Security requirements for the TOE's IT environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

32 These requirements are discussed separately below.

5.1 TOE Security Requirements

33 The CC divides security requirements into two categories:

- *Security functional requirements (SFRs)*: that is, requirements for security functions such as information flow control, audit, and identification.
- *Security assurance requirements (SARs)*: provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

5.1.1 TOE Security Functional Requirements

34 Table 7 identifies the SFRs for the TOE. These requirements were derived from the CC Part 2 Security Functional Requirements. The overall minimum Strength of function claim for the TOE SFRs is SOF-basic.

Table 7: TOE Security Functional Requirements

Functional Component ID	Functional Component Name	Security Objectives	Dependencies
Security Audit			
FAU_GEN.1	Audit data generation	O.AUDIT	FMT_STM.1
FAU_SAR.1	Audit review	O.AUDIT O.ADMIN;	FAU_GEN.1
FAU_SAR.3 (1)	Selectable audit review	O.AUDIT	FAU_SAR.1
FAU_SAR.3 (2)	Selectable audit review	O.AUDIT	FAU_SAR.1
FAU_SAA.1	Audit analysis	O.AUDIT	FAU_GEN.1
FAU_ARP.1	Audit automatic response	O.AUDIT	FAU_SAA.1
User Data Protection			
FDP_IFC.1 (1)	Subset information	O.MEDTF	FDP_IFF.1

Functional Component ID	**Functional Component Name**	**Security Objectives**	**Dependencies**
	flow control		
FDP_IFC.1 (2)	Subset information flow control	O.MEDAPPL	FDP_IFF.1
FDP_IFF.1 (1)	Simple security attributes	O.MEDTF	FDP_IFC.1, FMT_MSA.3
FDP_IFF.1 (2)	Simple security attributes	O.MEDAPPL	FDP_IFC.1, FMT_MSA.3
FDP_RIP.1	Residual Information Protection	O.INFPRO	None
Identification and Authentication			
FIA_UAU.1	Timing Authentication	O.IDAUTH	FIA_UID.1
FIA_UID.2	User Identification before any action	O.IDENTIFY	None
Security Management			
FMT_MOF.1	Management of security functions behavior	O.ADMIN	FMT_SMR.1
FMT_MSA.1 (1)	Management of security attributes	O.MEDTF	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1 (2)	Management of security attributes	O.MEDAPPL	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1 (3)	Management of security attributes	O.MEDTF	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1 (4)	Management of security attributes	O.MEDAPPL	FDP_IFC.1, FMT_SMR.1
FMT_MSA.3 (1)	Static attribute initialization	O.MEDTF	FMT_MSA.1, FMT_SMR.1
FMT_MSA.3 (2)	Static attribute initialization	O.MEDAPPL	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1 (1)	Management of TSF data	O.ADMIN	FMT_SMR.1
FMT_MTD.1 (2)	Management of TSF data	O.ADMIN	FMT_SMR.1
FMT_MTD.1 (3)	Management of TSF data	O.ADMIN	FMT_SMR.1
FMT_MTD.1 (4)	Management of TSF data	O.PRIVACY	FMT_SMR.1
FMT_SMR.1	Security roles	O.ADMIN	FIA_UID.1
Privacy			
FPR_PSE.1	Pseudonymity	O.PRIVACY	None

Functional Component ID	Functional Component Name	Security Objectives	Dependencies
(Dynamic)			
FPR_PSE.1 (Static)	Pseudonymity	O.PRIVACY	None
Protection of the TOE Security Functions			
FPT_ITT.1	Basis internal TSF data transfer protection	O.SELPRO	None
FPT_RVM.1	Reference Mediation	O.SELPRO	None
FPT_SEP.1	TSF domain separation	O.SELPRO	None
FPT_STM.1	Reliable time stamps	O.AUDIT	None

5.1.1.1 Class FAU: Security Audit

35 **FAU_GEN.1 Audit data generation**

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 in Table 8].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 8]

Table 8: Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FIA_UAU.1	All use of the authentication mechanism	
FIA_UID.2	All use of the user identification mechanism	The user identity provided to the TOE.
FDP_IFF.1 (1) FDP_IFF.1 (2)	All decisions on request for information flow	The presumed addresses of the source and destination subject.
FDP_IFF.1 (1) FDP_IFF.1 (2)	Spoofing attacks	The presumed addresses of the source and destination subject.
FDP_IFF.1 (1) FDP_IFF.1 (2)	Port Probes	The presumed addresses of the source and destination subject.
FDP_IFF.1 (1) FDP_IFF.1 (2)	Address space probes	The presumed addresses of the source and destination subject.

FDP_IFF.1 (1) FDP_IFF.1 (2)	IP option	The presumed addresses of the source and destination subject.
FDP_IFF.1 (1) FDP_IFF.1 (2)	Incoming packets not handled	The presumed addresses of the source and destination subject.
FDP_IFF.1 (1) FDP_IFF.1 (2)	Outgoing packets not handled	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time	

36 **FAU_SAR.1 Audit review**

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.

37 **FAU_SAR.3 (1) Selectable audit review**

FAU_SAR.3.1 (1) The TSF shall provide the ability to perform *searches* of audit data based on

[a) alphanumeric string keyphrase;
b) specified audit trail field and value].

38 **FAU_SAR.3 (2) Selectable audit review**

FAU_SAR.3.1 (2) The TSF shall provide the ability to perform *sorting* of audit data based on

[a) the chronological order of audit event occurrence.]

39 **FAU_SAA.1 Potential violation analysis**

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

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

a) Accumulation or combination of [spoofing attack audit events] known to indicate a potential security violation;
b) [Accumulation or combination of IP option audit events known to indicate a potential security violation;
c) Accumulation or combination of port probe audit events known to indicate a potential security violation;
d) Accumulation or combination of address space probes audit events known to indicate a potential security violation;
e) Accumulation or combination of incoming packets not handled audit events known to indicate a potential security violation; and
f) Accumulation or combination of outgoing packets not handled audit events known to indicate a potential security violation].

40 **FAU_ARP.1 Security alarms**

FAU_ARP.1.1 The TSF shall take [one or more of the following activities as specified by an authorized administrator:

a. reject potentially threatening packets ,
b. automatically block all communication from a source site,
c. add an event to the log, or
d. send a notification of potential security threats to an authorized administrator]

upon detection of a potential security violation.

5.1.1.2 Class FDP: User Data Protection

41 **FDP_IFC.1 (1) Subset information flow control**

FDP_IFC.1.1 (1) - The TSF shall enforce the [TRAFFICFLOW SFP] on:

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

b) information: packets;

c) operation: pass information].

42 **FDP_IFC.1 (2) Subset information flow control**

FDP_IFC.1.1 (2) - The TSF shall enforce the [APPLICATIONFLOW SFP] on:

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

b) information: SMTP packets;

c) operation: pass information].

43 **FDP_IFF.1 (1) Simple security attributes**

FDP_IFF.1.1 (1) The TSF shall enforce the [TRAFFICFLOW SFP] based on 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.]

FDP_IFF.1.2 (1) 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) Subjects 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 (1) The TSF shall enforce the [rules of the APPLICATIONFLOW SFP for SMTP packets as specified by the authorized administrator].

FDP_IFF.1.4 (1) The TSF shall provide the following [none].

FDP_IFF.1.5 (1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (1) 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 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 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.]

44 **FDP_IFF.1 (2) Simple security attributes**

FDP_IFF.1.1 (2) The TSF shall enforce the [APPLICATIONFLOW SFP] based on 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.]

FDP_IFF.1.2 (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) Subjects 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 (2) The TSF shall enforce the [none].

FDP_IFF.1.4 (2) The TSF shall provide the following [none].

FDP_IFF.1.5 (2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (2) 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 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 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 malformed service requests.]

45 **FDP_RIP.1 Subset residual information protection**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>*allocation of the resource to*</u>, the following objects: [all objects].

5.1.1.3 Class FIA: Identification and Authentication

46 **FIA_UAU.1 Timing of authentication**

FIA_UAU.1.1 The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the **authorized administrator accessing the TOE** to be performed before the **authorized administrator** is authenticated.

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

47 **FIA_UID.2 User Identification before any action**

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.4 Class FMT: Security Management

48 **FMT_MOF.1 Management of security functions behavior**

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable, and/or modify the behavior of* the functions:
[a) management of audit record generation;
b) maintenance of security audit analysis rules;
c) management of security audit automatic response actions]
to [authorized administrator].

49 **FMT_MSA.1 (1) Management of security attributes**

FMT_MSA.1.1 (1) The TSF shall enforce the [TRAFFICFLOW SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule] the security attributes [listed in section FDP_IFF.1.1 (1)] to [the authorized administrator].

50 **FMT_MSA.1 (2) Management of security attributes**

FMT_MSA.1.1 (2) The TSF shall enforce the [APPLICATIONFLOW SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule] the security attributes [listed in section FDP_IFF.1.1 (2)] to [the authorized administrator].

51 **FMT_MSA.1 (3) Management of security attributes**

FMT_MSA.1.1 (3) The TSF shall enforce the [TRAFFICFLOW SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in section FDP_IFF.1.1 (1)] to [the authorized administrator].

52 **FMT_MSA.1 (4) Management of security attributes**

FMT_MSA.1.1 (4) The TSF shall enforce the [APPLICATIONFLOW SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in section FDP_IFF.1.1 (2)] to [the authorized administrator].

53 **FMT_MSA.3 (1) Static attribute initialization**

FMT_MSA.3.1 (1) The TSF shall enforce the [TRAFFICFLOW SFP] to provide *restrictive* default values for security attributes that are used to enforce the **TRAFFICFLOW** SFP.

FMT_MSA.3.2 (1) The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

54 **FMT_MSA.3 (2) Static attribute initialization**

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

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

55 **FMT_MTD.1 (1) Management of TSF data**

FMT_MTD.1.1 (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].

56 **FMT_MTD.1 (2) Management of TSF data**

FMT_MTD.1.1 (2) The TSF shall restrict the ability to *query* the [audit trail] to [the authorized administrator].

57 **FMT_MTD.1 (3) Management of TSF data**

FMT_MTD.1.1 (3) The TSF shall restrict the ability to *create, modify, and delete* the [user identity used in FIA_UID.2] to [the authorized administrator].

58 **FMT_MTD.1 (4) Management of TSF data**

FMT_MTD.1.1 (4) The TSF shall restrict the ability to *create, modify, and delete* the [aliases used in FPR_PSE.1 (static) and FPR_PSE.1 (dynamic)] to [the authorized administrator].

59 **FMT_SMR.1 Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator].

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

5.1.1.5 Class FPR: Privacy

60 **FPR_PSE.1 Pseudonymity (Dynamic)**

FPR_PSE.1.1 (Dynamic) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real **IP address** bound to [external IT entities on the internal network that generate connections to external IT entities on the external network].

FPR_PSE.1.2 (Dynamic) The TSF shall be able to provide [4000] aliases of the real **IP address** to [external IT entities on the internal network].

FPR_PSE.1.3 (Dynamic) The TSF shall *determine an alias for an external IT entity on the internal network* and verify that it conforms to the [dynamic NAT port randomness algorithm].

61 **FPR_PSE.1 Pseudonymity (Static)**

FPR_PSE.1.1 (Static) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real **IP address** bound to [external IT entities on the internal network].

FPR_PSE.1.2 (Static) The TSF shall be able to provide [255] aliases of the real **IP address** to [external IT entities on the internal network].

FPR_PSE.1.3 (Static) The TSF shall *determine an alias for an external IT entity on the internal network* and verify that it conforms to the [static NAT rules as specified by the authorized administrator].

5.1.1.6 Class FPT: Protection of the TOE Security Functions

62 **FPT_ITT.1 Basic internal TSF data transfer protection**

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

63 **FPT_RVM.1 Non-bypassability of the TSP**

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

64 **FPT_SEP.1 TSF domain separation**

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

65 **FPT_STM.1 Reliable time stamps**

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.1.7 SFRs With SOF Declarations

66 The overall Strength of function claim for the TOE is SOF-basic. Specific strength of function metrics are defined for the FIA_UAU.1.

FIA_UAU.1 Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million (.000001).

5.1.2 TOE Security Assurance Requirements

67 Table 9 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL 2.

Table 9: EAL 2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1,

Assurance Component ID	Assurance Component Name	Dependencies
		AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1

68 **ACM_CAP.2 Configuration items**

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

69 **ADO_DEL.1 Delivery procedures**

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

70 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

71 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

72 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

73 **ADV_RCR.1 Informal correspondence demonstration**

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

74 **AGD_ADM.1 Administrator guidance**

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

75 **AGD_USR.1 User guidance**

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

76 **ATE_COV.1 Evidence of coverage**

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

77 **ATE_FUN.1 Functional testing**

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

78 **ATE_IND.2 Independent testing – sample**

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

79 **AVA_SOF.1 Strength of TOE security function evaluation**

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

80 **AVA_VLA.1 Developer vulnerability analysis**

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, including those identified in Appendix A of ALFPP v1.c., that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2 Security Requirements for the IT Environment

81 The TOE has no security requirements allocated to its IT environment.

6 TOE SUMMARY SPECIFICATION

82 This Chapter presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

83 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1.

6.1.1 Security Administration [WG_ADMIN]

84 The WatchGuard Control Center component is a toolkit of applications executing from the Management Station that enables the users who are administrating the TOE to configure, manage, and monitor the network security policy enforced by Firebox II. Triple DES using port 4105 protects the communication between the Management Station and the Firebox II. The administrator uses the Windows NT Networking services and Policy Manager to define the communication interface between the Management Station and Firebox II. The Control Center includes the Policy Manager, Firebox Monitors, LogViewer, Historical Reports and HostWatch. The Control Center interface uses a quick guide tool bar and menu system to connect to the Firebox II, view real-time status, and open security suite tools. The Control Center supports two types of password access to administer the Firebox II: read/write access and read only access. The authorized administrator is allowed to view and modify the configuration file, manage the audit log, and view the static and real-time audit log information by entering the read/write pass phrase to start the Control Center and to access the Firebox. The authorized administrator is only allowed to read the configuration file and view the static and real-time audit log information when entering the read-only pass phrase to start the Control Center and to access the Firebox.

85 The LiveSecurity Event Processor is used by the administrator to manage the audit trail and provides an interface to specify the maximum number of records stored in a log file (i.e., Log Roll over). The Windows NT User Manager for Domains is used by the authorized administrator to configure NT accounts to include configuring user account identity and user audited events.

86 The Policy Manager is used to design, configure and manage the electronic portion of a network security policy. Upon initial installation of WatchGuard, the Firebox II does not allow any packet flows through the TOE. Within the Policy Manager, the authorized administrator can configure networks and services, regulate incoming and outgoing access, define aliases for dynamic and static network address translation, and control the logging of audit events and actions to be taken for security violations. The Policy Manager is the software tool for creating, modifying, and saving the configuration file that contains all the settings, options, addresses, and information that together constitute the Firebox II information flow rules. The default packet handling configuration feature of the Policy Manager determines whether and how the Firebox II handles incoming communications that appear to be attacks to the internal network. The authorized administrator can configure the security analysis rules to block spoofing attacks, IP options, port space probes, and address space probes. The authorized administrator can set up the packet handling to take the following automatic response actions:

- Reject potentially threatening packets
- Automatically block all communication from a source site
- Add an event to the log
- Send a notification of potential security threats. The notification can be configured to be sent as an email, a page, pop-up window, or triggering a custom program.

87 The Firebox Monitors provides the authorized administrator real-time displays of traffic through the Firebox II. The LogViewer is used by the authorized administrator to view the static audit log files generated by the Firebox II. LogViewer has a search tool to find specific events by keyphrase and field/value. The LogViewer sorts audit records in chronological order. The time stamp on the audit records is generated by Firebox II by receiving the time from the Management Station. Historical Reports is a reporting tool used by the authorized administrator to generate reports from the audit log files. The authorized administrator can modify the Windows NT clock by using the Date and Time utility and commands provided by Windows NT. HostWatch allows the authorized administrator to view real-time active connections on the Firebox II. It can also graphically represent the connections listed in a log file, either playing back a previous file for review or displaying connections as they are logged into the current audit log file. The Windows NT Event Viewer is used to view and query the NT audit log.

88 **Functional Requirements Satisfied**: FAU_ARP.1, FAU_SAR.1, FMT_MOF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FMT_MSA.1 (4), FMT_MSA.3 (1), FMT_MSA.2 (2), FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FPT_ITT.1, and FMT_SMR.1.

6.1.2 Identification [WG_ADMINID]

89 To gain access to the TOE for viewing or changing Firebox II information flows, authorized users must authenticate and identify themselves via the NT Login window, AND identify themselves at the Firebox II login prompt. There are two pass phrases that are setup by the authorized administrator on the Firebox II; one for “read-only” access, and one for “read/write” privileges. The read-only pass phrase is used to restrict the authorized administrator to read-only access.

90 The pass phrase must be at least one character, and there are no limitations on possible characters (including spaces). In addition to a required pass phrase, the TOE can be configured to only allow management changes for a specific IP address.

91 Users are identified by a presumed IP address when gaining access through the TOE (i.e., sending and receiving information through the TOE.).

92 **Functional Requirements Satisfied**: FIA_UID.2, FIA_UAU.1

6.1.3 Information Flow Control [WG_FLOW]

93 WatchGuard provides security through the following mechanisms: dynamic packet filtering, transparent application proxies, and dynamic/static network address translation (NAT). The

TOE ensures that previous packet data is unavailable for the next packet being processed. For each packet received by the Firebox II, the information flow policy rules are always applied and enforced. The authorized administrator uses the default packet handling configuration feature of the Policy Manager to specify whether and how the Firebox II handles incoming communications that appear to be attacks to the internal network. The authorized administrator can configure the default packet handling options to block spoofing attacks, IP options, port space probes, and address space probes. The TOE maintains a security domain for its own execution that is protected from interference and tampering by the fact that the Firebox II is a dedicated appliance containing no untrusted entities. The operating system shell is removed from the Firebox II to protect the integrity of the information flow enforcement functions. The TOE is assumed to be physically protected from unauthorized users.

6.1.3.1 Dynamic Packet Filtering

94 Dynamic packet filtering examines the headers of packets being sent or received. Headers provide information on the source of the packet, the destination, the protocol used, the port number, and other similar information. A packet filter examines the headers to determine whether they follow legitimate syntax rules and comply with the configured security policy.

95 A firewall packet filter is analogous to the mail sorter at a publishing company, who examines the authors' envelopes to make sure that they are both coming from a legitimate address, and bound for a legitimate editor within the company. He checks the postal guidelines to make sure that he is allowed to send this type of mail to this particular editor. He does not open the envelopes and examine the story being sent; he simply sorts and routes the mail. This is essentially what packet filters do.

96 For example, if a packet filter encountered a packet assigned to port 403, and the filter "knows" that this port has not been opened for any service, the filter would reject the packet because its port number is invalid according to packet filter rules.

97 Packet filters typically operate according to rules that determine packet disposition. These rules are written in a filter language and collected into groups called Rule Sets. Rule Sets can be difficult to configure and work best when interpreted by properly-written firewall software rather than by harried network system administrators. In addition, many packet filters do not provide the means to filter on some of the more useful properties of IP packets.

98 The TOE uses dynamic packet filtering rules which go beyond basic packet filtering described above. Firebox II bases its filtering not only on service types, but also on conditions surrounding the initiation of a connection. Firebox II uses dynamic rule-sets, allowing the authorized administrator to add and remove rules depending on network activity. For example, if a particular site attempts to connect to a port it has no business connecting to, Firebox II can be configured to automatically add that particular host to a blocked sites list, making things such as port space probes increasingly difficult to carry out. WatchGuard supports many well-known service types as specified in the *WatchGuard LiveSecurity Reference Guide, LiveSecurity System 4.1.*

6.1.3.2 Proxies

99 The WatchGuard proxy includes SMTP (e-mail). This proxy automatically search and reject malformed service requests. Even with packet filters, an administrator can determine what hosts within a LAN and on the Internet can communicate with one another through that protocol, which events to log (such as rejected incoming packets), and which series of events should initiate a notification of the network administrator.

6.1.3.3 Dynamic NAT

100 Dynamic NAT hides local network addresses from hosts on the external network. Hosts elsewhere on the external network only see outgoing packets from the Firebox II itself. Dynamic NAT can translate the addresses of almost all TCP and UDP-based transmissions.

101 In Dynamic NAT, outgoing packets are mapped to a random port on the Firebox II. The source address on these packets is then re-written with the IP address of the Firebox II, and the random port number. The remote end sees the IP address of the Firebox II and the random port number. Data is sent back to this location; the Firebox II then examines the headers, and maps the port number back to the masqueraded host.

102 This address translation is dynamic in that a new port-to-internal-host mapping is made for each connection. On any given connection, an internal host may be mapped to any given port. The implications of this are important: Dynamic NAT works only one way--for Outgoing traffic. To perform the same sort of operation from the outside to the inside, you must employ Static NAT to designate specific internal hosts to receive the packets of only one port. Static NAT is described in more detail in the next section.

6.1.3.4 Static NAT

103 Static NAT provides host-to-host re-mapping of incoming IP packets destined for a public address to a single internal address. It maintains the security of anonymity of Dynamic NAT and adds the functionality of forwarding externally originated traffic to specific internal hosts. Static NAT redirects IP packets destined to a Firebox II to the specific masqueraded host behind it. It rewrites the headers of the packets and forwards them based on the original destination port number. Static NAT is typically used for public services such as Web sites and e-mail.

104 For example, to set up a mail server that has anonymity, or that has an IP address that would not be legitimate on the external network, designate a specific internal server to receive all e-mail. Then, whenever someone sends e-mail addressed to the Firebox II, the Firebox II knows to translate the address to the designated e-mail (SMTP) server.

105 **Functional Requirements Satisfied**: FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2), FAU_SAA.1, FAU_ARP.1, FDP_RIP.1, FPR_PSE.1 (Dynamic), FPR_PSE.1 (Static), FPT_RVM.1, and FPT_SEP.1

6.1.4 Audit [WG_AUDIT]

106 WatchGuard supports audit event logging, detection of potential security violations, and notification. Audit event logging occurs when the firewall records the occurrence of an event to a log file. An event is any single activity that occurs at the Firebox II, such as allowing a packet-

-or more importantly--denying a packet passage through the Firebox II. The Firebox II can create audit events for all requests for information flow, spoofing attacks, IP options, port probes, address space probes, incoming packets not handled (i.e., denied), outgoing packets not handled (i.e., denied), and authorized administrator actions to configure the Firebox II. The Windows NT operating system generates audit events for use of user identity and authentication and changes to the time. The audit information captured by the Firebox II includes the date and time of the event, firewall name or IP address, the process sending the information. The rest of the information depends on the type of event. For information flow related events the disposition (allow, deny, or log), direction, interface, protocol, source IP address, and destination IP address, type and code is captured. The time stamp is received from the Windows NT platform when the Firebox II boots up. The Firebox II sets its clock to the same time as the Window NT platform. If the authorized administrator changed the time on the management station, Firebox II would re-synchronize its time, the next time the Firebox is rebooted.

107 Audit event logging involves the interaction of the Firebox II, the LiveSecurity Event Processor (LSEP), and the log host (Windows NT platform). When an event (for example, a denied incoming packet) occurs at the Firebox II, it informs the LSEP which in turn formats and standardizes the event and adds the event to the log file. LSEP is the program on the Management Station that controls logging and notification. It also provides timing services for the Firebox II. The LSEP is a separate program from the Control Center. It must be installed separately with the log encryption key entered. The audit event logging connection between the Firebox II and the Management Station is encrypted to ensure security. Both the Management Station and the Event Processor must possess the encryption key. WatchGuard allows the authorized administrator to create custom logging and notification properties for each service and blocking option.

108 In any firewall installation, it is necessary to make some basic assumptions regarding the layout of the various components. The WatchGuard has a distributed architecture: it intentionally separates the logging, management, and traffic discrimination functions into three separate logical and physical components: the log host, the management station and the Firebox II. In the evaluated TOE configuration the log host and Management Station are co-located on the same physical Windows NT platform.

109 The LogViewer provides a static display of audit log file data generated by the Firebox II. The data can be viewed as a whole or broken up into pages which can be accessed individually or in a chronological sequence. LogViewer also searches and displays by key phrase and field/value. Historical Reports allows the administrator to generate HTML reports using log files generated from the LSEP. These reports are viewed using a web browser. Firebox Monitors is an interface providing real-time displays of traffic through the Firebox II. HostWatch displays in real-time active connections occurring on the Firebox II. The LiveSecurity Event Processor is used by the administrator to manage the audit trail and provides an interface to specify the maximum number of records stored in a log file (i.e., Log Roll over). The Windows NT User Manager for Domains is used by the authorized administrator to configure NT accounts to include configuring user account identity and user audited events.

110 **Functional Requirements Satisfied**: FPT_STM.1, FAU_GEN.1, FAU_SAR.1, FAU_SAR.3 (1), and FAU_SAR.3 (2).

6.2 Assurance Measures

111 The TOE claims to satisfy the CC EAL 2 assurance requirements. WatchGuard has assurance measures for the TOE to satisfy the stated SARs. Table 10 shows which assurance measures are traced to the assurance requirements identified in Section 5.1.2:

Table 10: Traced Assurance Measures

Assurance Component ID	Assurance Component Name	Assurance Measure
ACM_CAP.2	Configuration items	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Configuration Management;
ADO_DEL.1	Delivery procedures	Delivery Procedures For Evaluated Version of WatchGuard LiveSecurity System with Firebox II;

ADO_IGS.1	Installation, generation, and start-up procedures	WatchGuard LiveSecurity System Install Guide, LiveSecurity System 4.1;
		WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Installation, Generation, and Startup Guide;
		WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1;

ADV_FSP.1	Informal functional specification	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Functional Specification;
		WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1;

ADV_HLD.1	Descriptive high-level design	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, High-Level Design Document
ADV_RCR.1	Informal correspondence demonstration	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Correspondence Demonstration

AGD_ADM.1	Administrator guidance	WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1;
		WatchGuard LiveSecurity Reference Guide, LiveSecurity System 4.1;
		WatchGuard LiveSecurity System Install Guide, LiveSecurity System 4.1;
		WatchGuard LiveSecurity System Internet Security Handbook, LiveSecurity System 4.1
		WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Installation, Generation and Startup Guide;

AGD_USR.1	User guidance	WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1;

Assurance Component ID	**Assurance Component Name**	**Assurance Measure**
ATE_COV.1	Evidence of coverage	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Test Coverage Analysis
ATE_FUN.1	Functional testing	WatchGuard LiveSecurity System Test Plans, Procedures, and Results
ATE_IND.2	Independent testing-sample	NA
AVA_SOF.1	Strength of TOE security function evaluation	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Functional Specification
AVA_VLA.1	Developer vulnerability analysis	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Vulnerability Assessment

7 PP CLAIMS

112 The WatchGuard LiveSecurity System with Firebox II was not written to comply with any PP.

8 RATIONALE

8.1 Security Objectives Rationale

113 The Table 5 and Table 6 in Section 4 demonstrate that all security objectives are addressed by at least one assumption or threat and thus suitable to address the TOE security environment.

114 The following tables demonstrate that the stated security objectives are traceable to all aspects identified in the TOE security environment presented in Chapter 3. A justification why the security objective is suitable to counter that threat or cover the assumption is also provided in the tables.

Table 11: Security Objectives Suitable for Threats

Threat Identifier	Security Objective	Justification
T.NOAUTH	O.IDENTIFY O.ADMIN O.IDAUTH	O.IDENTIFY is necessary to counter the threat because it requires that users be uniquely identified before accessing the TOE security functions thus restricting access to users who successfully identify themselves. O.ADMIN and O.REVIEW counter the threat by defining the type of users who can access the TOE by role and what actions they can perform in the role. By establishing what type of access is allowed. The combination of these objectives will help to diminish the threat because the TOE would require the user to successfully identify themselves and then the user is restricted to a set of functions. O.IDAUTH counters the threat by requiring users to be identified and authenticated before accessing the TOE.
T.ASPOOF	O.MEDTF	O.MEDTF is necessary to counter the threat of a spoofed source address and thus allowing impermissible information to flow through the TOE. This threat is an attack that occurs at the network layer. This security objective removes the threat by requiring that all information that passes through the networks be mediated by the TOE at the network layer.
T.MEDTF	O.MEDTF	O.MEDTF is necessary to counter the threat of attacks targeted at the network layer and thus allowing impermissible information to flow through the TOE. This security objective removes the threat by requiring that all information that passes through the networks is mediated by the TOE at the network layer as configured by the authorized administrator.

Threat Identifier	Security Objective	Justification
T.MEDAPPL	O.MEDAPPL	O.MEDTF is necessary to counter the threat of attacks targeted at the application layer and thus allowing impermissible information to flow through the TOE. This security objective removes the threat by requiring that information that passes through the networks be mediated by the TOE at the application layer as configured by the authorized administrator.
T.OLDINF	O.INFPRO	O.INFPRO is necessary to remove the opportunity for threat agents to gather residual data from previous information flows. This security objective requires that that no residual information be transmitted.
T.AUDACC	O.AUDIT	O.AUDIT is necessary to diminish the threat of users not being accountable for their actions by requiring an audit trail and a means to search and sort the information contained in the audit trail
T.NODETECT	O.AUDIT	O.AUDIT is necessary to diminish the threat of users continuously trying to bypass the TOE by requiring detection of security violations and alerting the authorized administrator. O.AUDIT also mitigates the threat by requiring an action to be taken when violations are detected.
T.SELPRO	O.SELPRO	This security objective is necessary to remove the threat because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
T.PRIVACY	O.PRIVACY	This security objective is necessary to diminish the threat of a host on the internal network from being explicitly targeted for an attack. The objective requires privacy protection for internal hosts such that users on the external network can not determine the IP address of the users on the internal network.
T.USAGE	OE.GUIDANCE OE.ADMTRA	These security objectives are necessary to diminish the threat of the TOE being insecurely configured. OE.GUIDANCE requires that the owners of the TOE have ensure that the TOE is operated in a secure manner. OE.ADMTRA ensure that administrators receive proper training.

Table 12: Security Objectives Suitable for Assumptions

Assumption Identifier	Security Objective	Justification
A.LOWEXP	OE.LOWEXP	This security objective is necessary to ensure that the TOE is used in an environment for which it is intended

Assumption Identifier	Security Objective	Justification
A.NOEVIL	OE.NOEVIL	This security objective is necessary to ensure that authorized administrators are trustworthy to perform their duties.
A.ONEWAY	OE.ONEWAY	This security objective is necessary to ensure that the TOE can not be bypassed.
A.NOREM	OE.NOREM	This security objective is necessary to prevent remote access from being allowed
A.GENPUR	OE.GENPUR	This security objective is necessary to prevent additional applications from being loaded on TOE and thus ensuring that no untrusted entities are part of the TOE configuration.
A.DIRECT	OE.DIRECT	This security objective is necessary to ensure that only personnel within the physical boundary of the TOE may have direct access to the TOE.
A.PHYSEC	OE.PHYSEC	This security objective is necessary to ensure the physical protection of the TOE.

8.2 Security Requirements Rationale

115 The security requirements rationale section is provided to demonstrate that the set of security requirements is suitable to meet and traceable to the security objectives.

8.2.1 Traceability and Suitability

116 Table 7 in section 5.1.1 traces each TOE SFR to at least one security objective for the TOE. The table below contains a justification for the chosen SFRs and their suitability to satisfy each security objective for the TOE.

Table 13: SFRs Suitable for Security Objectives

Security Objective	Security Functional Requirement	Justification
O.IDAUTH	FIA_UAU.1	This SFR address the authenticated aspect of the objective.
O.IDENTIFY	FIA_UID.2	This SFR requires the user to identify itself before the TOE is allowed to perform any security relevant actions on behalf of that user. The requirement would apply to both human users and external IT entities.

Security Objective	**Security Functional Requirement**	**Justification**

O.MEDTF	FDP_IFC.1 (1);
	FDP_IFF.1 (1);
	FMT_MSA.1 (1);
	FMT_MSA.1 (3);
	FMT_MSA.3 (1)
		This objective requires that information flows at the network layer be mediated as configured by the authorized administrator. FDP_IFC.1 (1) and FDP_IFC.1 (1) define the security policy for which mediation decisions are based. FMT_MSA.1 (1), FMT_MSA.1 (3), and FMT_MSA.3 (1) define the functionality to allow the authorized administrator to configure the information flow rules.

O.MEDAPPL	FDP_IFC.1 (2);
	FDP_IFF.1 (2);
	FMT_MSA.1 (2);
	FMT_MSA.1 (4);
	FMT_MSA.3 (2)
		This objective requires that information flows at the application layer be mediated as configured by the authorized administrator. FDP_IFC.1 (2) and FDP_IFC.1 (2) define the security policy for which mediation decisions are based. FMT_MSA.1 (2), FMT_MSA.1 (4), and FMT_MSA.3 (2) define the functionality to allow the authorized administrator to configure the information flow rules.

O.INFPRO	FDP_RIP.1	The requirement directly addresses the security objective because it ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows.

O.SELPRO	FPT_ITT.1;
	FPT_SEP.1;
	FPT_RVM.1
		FPT_ITT.1 ensures that the TOE parts, the Firebox II and Management Station platform have a connection that is cannot be tampered with. FPT_SEP.1 ensures that the TSF have a domain of execution that is separate and that cannot be tampered or deactivated by unauthorized users. FPT_RVM ensures that the TSF are always invoked and not bypassed.

O.AUDIT	FAU_GEN.1;
	FAU_SAR.1;
	FAU_SAR.3 (1);
	FAU_SAR.3 (2);
	FAU_SAA.1;
	FAU_ARP.1;
	FPT_STM.1
		FAU_GEN.1 and FPT_STM.1 provide the functionality to generate and record audit records. FAU_SAR.1; FAU_SAR.3 (1); FAU_SAR.3 (2) provide the functionality to review the audit and restricts this functionality to authorized administrator. FAU_SAA.1 and FAU_ARP.1 provide the functionality to detect potential violations and to take action as specified by the authorized administrator.

Security Objective	Security Functional Requirement	Justification

O.ADMIN	FMT_MOF.1;
	FMT_MTD.1 (1);
	FMT_MTD.1 (2);
	FMT_MTD.1 (3);
	FMT_SMR.1;
	FAU_SAR.1
		All these requirements address the security objective because they define the functions that are restricted to the authorized administrator. FMT_SMR.1 is included because of its dependency from the other requirements.

O.PRIVACY	FPR_PSE.1 (Dynamic);
	FPR_PSE.1 (Static);
	FMT_MTD.1 (4)
		These requirements provide the functionality to provide network address translation such that the identity of internal IP addresses cannot be determined. FMT_MTD.1 (4) restricts setting up the alias used to the authorized administrator.

8.2.2 Rationale For Assurance Requirements

117 The chosen assurance level EAL 2 is consistent with the minimum required level of assurance for firewalls as specified by the US Government through their publication of the *US Government Traffic Filter Protection Profile for Low Risk Environments* and the *US Government Application Level Protection Profile for Low Risk Environments.* It is WatchGuard's intention to satisfy the US Government's minimum assurance requirements.

8.2.3 Rationale for Strength of Function

118 The rationale for the chosen level of SOF-basic is based on the minimum attack potential of the threat agents identified in this security target. The CC associates a SOF-Basic as being resistant to threats possessing low attack potential. The minimum attack potential that is assumed by this ST is considered lower than a low attack potential. Since SOF-Basic is the lowest SOF that can be identified, SOF-Basic was chosen.

8.2.4 Mutually Supportive

119 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole as evidenced by the following:

a) The choice of security requirements is justified as shown in Sections 8.2.1 and 8.2.2. The choice of SFR and SARs were made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. This ST provides evidence the security objectives counter threats to the TOE (Table 11), and also, the assumptions and objectives counter threats to the TOE environment (Table 12).

b) All SFR dependencies have been satisfied as shown in Table 7.

c) The SOF claim is valid with the threat environment described in Section 3. The rationale for the chosen level of SOF-basic is based on the minimum attack potential of the threat agents identified in this security target. The SOF claim is commensurate with the EAL 2 level of assurance.

d) The SARs are appropriate for the assurance level of EAL 2 and are satisfied as shown in Section 6.2.

e) The statement of requirements is written using consistent language and does not contradict each other to present security functionality of the TOE.

8.3 Rationale for TOE Summary Specification

120 This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

8.3.1 TOE Security Functions

121 The specified TOE security functions work together so as to satisfy the TOE security functional requirements. Section 6.1 includes in the descriptions of security functions a mapping of SFRs to the security functional requirements to show that each security function is traced to at least one SFR. Table 14 * MERGEFORMAT demonstrates that each SFR is covered by at least one security function.

Table 14: Mapping of SFRs to Security Functions

Functional Component ID	Functional Component Name	Security Function
FAU_GEN.1	Audit data generation	WG_AUDIT
FAU_SAR.1	Audit review	WG_ADMIN; WG_AUDIT
FAU_SAR.3 (1)	Selectable audit review	WG_AUDIT
FAU_SAR.3 (2)	Selectable audit review	WG_AUDIT
FAU_SAA.1	Audit analysis	WG_FLOW
FAU_ARP.1	Audit automatic response	WG_ADMIN WG_FLOW
FDP_IFC.1 (1)	Subset information flow control	WG_FLOW
FDP_IFC.1 (2)	Subset information flow control	WG_FLOW
FDP_IFF.1 (1)	Simple security attributes	WG_FLOW
FDP_IFF.1 (2)	Simple security attributes	WG_FLOW
FDP_RIP.1	Residual Information Protection	WG_FLOW
FIA_UAU.1	Timing of authentication	WG_ADMINID
FIA_UID.2	User Identification before any action	WG_ADMINID
FMT_MOF.1	Management of	WG_ADMIN

Functional Component ID	Functional Component Name	Security Function
	security functions behavior	
FMT_MSA.1 (1)	Management of security attributes	WG_ADMIN
FMT_MSA.1 (2)	Management of security attributes	WG_ADMIN
FMT_MSA.1 (3)	Management of security attributes	WG_ADMIN
FMT_MSA.1 (4)	Management of security attributes	WG_ADMIN
FMT_MSA.3 (1)	Static attribute initialization	WG_ADMIN
FMT_MSA.3 (2)	Static attribute initialization	WG_ADMIN
FMT_MTD.1 (1)	Management of TSF data	WG_ADMIN
FMT_MTD.1 (2)	Management of TSF data	WG_ADMIN
FMT_MTD.1 (3)	Management of TSF data	WG_ADMIN
FMT_MTD.1 (4)	Management of TSF data	WG_ADMIN
FMT_SMR.1	Security roles	WG_ADMIN
FPR_PSE.1 (Dynamic)	Pseudonymity	WG_FLOW
FPR_PSE.1 (Static)	Pseudonymity	WG_FLOW
FPT_ITT.1	Basis internal TSF data transfer protection	WG_ADMIN
FPT_RVM.1	Reference Mediation	WG_FLOW
FPT_SEP.1	TSF domain separation	WG_FLOW
FPT_STM.1	Reliable time stamps	WG_AUDIT

Table 16 provides rationale that the security functions are suitable to meet the SFRs.

Table 16: Suitability of Security Functions

Security Function	Security Functional Requirement	Justification

WG_ADMIN	FAU_ARP.1, FAU_SAR.1, FMT_MOF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FMT_MSA.1 (4), FMT_MSA.3 (1), FMT_MSA.2 (2), FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FPT_ITT.1, and FMT_SMR.1.	The WG_ADMIN security function implements the functionality to provide the authorized administrator as appropriate, the interfaces necessary to perform audit management, manage information flow, set the clock, manage NAT alias, and set up violation detection and notification rules as appropriate. Because the authorized administrator is managing the Firebox II from a separate platform, the communication is protected.
WG_ADMINID	FIA_UID.2 FIA_UAU.1	The WG_ADMINID security functions directly address both requirements such that a user directly accessing the TOE must be identified and authenticated before any TSF mediated action. Users are identified by a presumed IP address when sending and receiving information through the TOE.
WG_FLOW	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2), FAU_SAA.1; FAU_ARP.1 FDP_RIP.1, FPR_PSE.1 (Dynamic), FPR_PSE.1 (Static), FPT_RVM.1, and FPT_SEP.1	This security function implements the information flow functionality used to mediate all flows through Firebox II. This includes defining aliases for NAT defining a set of rules to monitor potential security violations and taking the proper action as specified by the administrator. Because the TSF enforcement is implemented by this security function, the requirements for reference mediation and separation are part of this security function.
WG_AUDIT	FPT_STM.1, FAU_GEN.1, FAU_SAR.1, FAU_SAR.3 (1), and FAU_SAR.3 (2).	This security function implements the audit functionality of WatchGuard and includes recording and reviewing the audit logs using tools for searching and sorting.

122 Because the security functions trace to SFRs which were shown to be mutually supportive in Section 8.2.4, and Table 16 justifies that the security functions implement all the SFRs, it is concluded that the security functions have to work together to satisfy the SFRs.

8.3.2 TOE Assurance Requirements

123 Table 17 is provided to demonstrate that each TOE SAR is adequately addressed by at least one assurance measure.

Table 17: Assurance Measure Suitability

Assurance Component ID	Assurance Measure	Justification
ACM_CAP.2	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Configuration	This assurance measure was written to addresses the configuration management documentation for EAL

Assurance Component ID	Assurance Measure	Justification
	Management.	2. This includes identifying the evaluated TOE and providing a configuration list with configuration items that have been uniquely identified and the method used to identify them.
ADO_DEL.1	Delivery Procedures For Evaluated Version of WatchGuard LiveSecurity System with Firebox II.	This assurance measure addresses delivery procedures for the TOE and documents how WatchGuard is securely provided to a customer.

ADO_IGS.1	WatchGuard LiveSecurity System Install Guide, LiveSecurity System 4.1;
	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Installation, Generation and Startup Guide;
	WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1.
		These assurance measures address Installation, Generation and Startup procedures for the evaluated TOE. This includes that the TOE is installed, generated, and started as the developers intended with the assurance that each time it is done the same way and securely.

ADV_FSP.1	Watchguard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Functional Specification; WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1.	These assurance measures address the security functions of the TOE. This includes identifying and describing the external TOE security function interfaces.
ADV_HLD.1	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, High-Level Design Document.	This assurance measure addresses the TOE in terms of subsystems. It describes the security functionality of each subsystem and the supporting protection mechanisms implemented.
ADV_RCR.1	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Correspondence Documentation.	This assurance measure was specifically written to address the EAL 2 requirements for correspondence evidence. This includes showing a correspondence analysis between the security target and the functional specification; and between the functional specification and the high-level design.

AGD_ADM.1	WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1;
	WatchGuard LiveSecurity System Reference Guide, LiveSecurity System 4.1;
	WatchGuard LiveSecurity System Install Guide, LiveSecurity System 4.1;
	WatchGuard LiveSecurity System Internet Security Handbook, LiveSecurity System 4.1;
	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Installation, Generation and Startup Guide.
		This assurance measure addresses administrator guidance. It describes how to securely administer the TOE.

Assurance Component ID	Assurance Measure	Justification
AGD_USR.1	WatchGuard LiveSecurity System User Guide, LiveSecurity System 4.1.	This assurance measure addresses user guidance. It describes the instructions and guidelines for secure use of the TOE.
ATE_COV.1	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Test Coverage Analysis	This assurance measure was specifically written to address the EAL 2 requirements for test coverage analysis evidence. This includes showing which security functions were tested.
ATE_FUN.1	WatchGuard LiveSecurity System Test Plans, Procedures, and Results	This assurance measure provides the test documentation used by the vendor to test TOE functionality.
ATE_IND.2	NA	NA
AVA_SOF.1	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Functional Specification	This assurance measure includes a chapter that discusses strength of function of the authentication mechanism.
AVA_VLA.1	WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Vulnerability Assessment.	This assurance measure addresses the intended environment for the TOE. This includes that there are no exploitable obvious vulnerabilities.

8.3.3 Strength of Function Claim

124 The strength of TOE Security Function of SOF-basic is valid for the TOE Security Functions and Assurance Measures because they support the SFRs and SARs as demonstrated in 8.3.1 and 8.3.2. The explicit SOF claim for authentication on the management station is consistent with the Strength of TOE Function. The claim of SOF-basic ensures that the mechanism is resistant to a low attack potential.