Trust Technology Assessment Program

EVALUATION TECHNICAL REPORT

WATCHGUARD TECHNOLOGIES
WATCHGUARD LIVESECURITY SYSTEM
WITH FIREBOX II
4.1

PREPARED BY:
COMPUTER SCIENCES CORPORATION
7471 CANDLEWOOD ROAD
HANOVER, MD 21076

SUBMITTED TO:
TTAP OVERSIGHT BOARD

VERSION 1.0
AUGUST 2000

FOREWORD

This publication, the WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1, Evaluation Technical Report is being issued by Computer Sciences Corporation This report is the principle source of information used by the Trust Technology Assessment Program (TTAP) Oversight Board to render a certification rating for the WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 product. It is intended to support the TTAP certification process by providing all the information needed by the TTAP Oversight Board to verify the results of the evaluation. This report presents all evaluation results, their justifications and any findings derived from the work performed during the evaluation. The requirements stated in this report are taken from *the WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 Security Target, Version 1.3* and are conformant with the *Common Criteria for Information Technology Security Evaluation, Version 2.0*.

____*Hard copy signed*___

Director, TTAP Evaluation Facility

____*Hard copy signed*___

Evaluation Team Leader, TTAP Evaluation Facility

____*Hard copy signed*___

Quality Manager, TTAP Evaluation Facility

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

WATCHGUARD TECHNOLOGIES WATCHGUARD LIVESECURITY SYSTEM WITH FIREBOX II 4.1 EVALUATION TECHNICAL REPORT

1 INTRODUCTION

1.1 Background

1 The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called TTAP Evaluation Facilities (TEFs) using the current NSA evaluation methodology and proposed evaluation methodology for Evaluation Assurance Level (EAL) 1 and EAL 2 in accordance with cooperative research and development agreements. The program focuses on products with features and assurances characterized by the Common Criteria (CC) EAL 1 through EAL 4. In addition, TEFs are allowed to conduct PP evaluations.

2 The TTAP Oversight Board assigns a Certifier(s) to monitor the TEFs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a TEF and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NSA’s Evaluated Products List.

3 The TTAP is migrating to the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). Under the Mutual Recognition Arrangement (MRA), evaluation facilities conducting CC evaluations must apply the Common Evaluation Methodology (CEM). The Computer Sciences Corporation CCEL has applied for and has undergone an EAL4 accreditation process. This evaluation was performed under the TTAP/CCEVS practices and procedures using the CEM.

1.2 Evaluation Identifiers

4 Table 1 provides information needed to identify and control this Evaluation Technical Report (ETR), the Security Target (ST) and the Target of Evaluation (TOE). This table also identifies the key players involved with the evaluation.

Table 1: Evaluation identifiers

Item	Identifier
Evaluation Technical Report	The WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 Evaluation Technical Report, August 2000, Version 1.0.
Security Target	The WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 Security Target, August 2000, Version 1.3
Target of Evaluation	The WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1
Assurance Level	EAL 2

Item	Identifier
Developer	WatchGuard Technologies 316 Occidental Ave S, Suite 200 Seattle, WA 98104
Sponsor	WatchGuard Technologies
Evaluators	Computer Sciences Corporation James Fink Halvar Forsberg Joan Wallace Government Participants Rey Robles
Validators	Megan Roback John Wyszynski

1.3 Document organization

5 This ETR is organized according to the structure dictated by the Common Evaluation Methodology (CEM) Version 1.0 on page 14, Figure 2.2. All the sections of this ETR conform to the ETR requirements described in the CEM and is divided into the following Chapters:

6 Chapter 1 Introduction, describes the background of the Scheme, identifies the ETR, ST and TOE control identifiers, and identifies the developer, sponsor, evaluators, and validators of the evaluation;

7 Chapter 2 Architectural Description of the TOE, provides a high-level description of the TOE and its major components;

8 Chapter 3 Evaluation, describes the methods, techniques, tools, and standards used during the evaluation; constraints or assumptions regarding the conduct and results of the evaluation; and identifies the evaluation evidence examined;

9 Chapter 4 Results of the Evaluation, provides a verdict and supporting rationale for each assurance component completed for the evaluation;

10 Chapter 5, Conclusions and Recommendations, provides the CCEL’s conclusions and recommendations based on the results of the Evaluation;

11 Chapter 6, List of Evaluation Deliverables, identifies the evidence examined;

12 Chapter 7, Acronyms;

13 Chapter 8, Problem Reports, lists the Evaluation Discovery Reports (EDRs) and Observation Reports (ORs) that were raised during the evaluation and their status.

1.4 References

14 The following documents are referenced throughout this report.

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[LSS_ST] WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 Security Target, Version 1.3.

2 ARCHITECTURAL DESCRIPTION OF THE TOE

15 This section describes the high-level design of the WatchGuard LiveSecurity System and NT subsystems and identifies their interfaces. The information presented is not intended to describe the complete design of each subsystem, but rather to provide sufficient information to enable the reader to understand the WatchGuard LiveSecurity System design and provide evidence that the system satisfies its functional requirements as identified in the [LSS_ST].

16 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, 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 SMTP connections. WatchGuard consists of four major components:

- LiveSecurity Broadcast Service – 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 audit events 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 a network.

17 Figure 1 illustrates the physical boundary of the TOE. This configuration, or topology, was selected to allow the Firebox to protect the Management Station from attack by users on the Internal and External Network. The physical boundary of the TOE establishes a system topology(ies) as well as some constraints under which the TOE will operate.

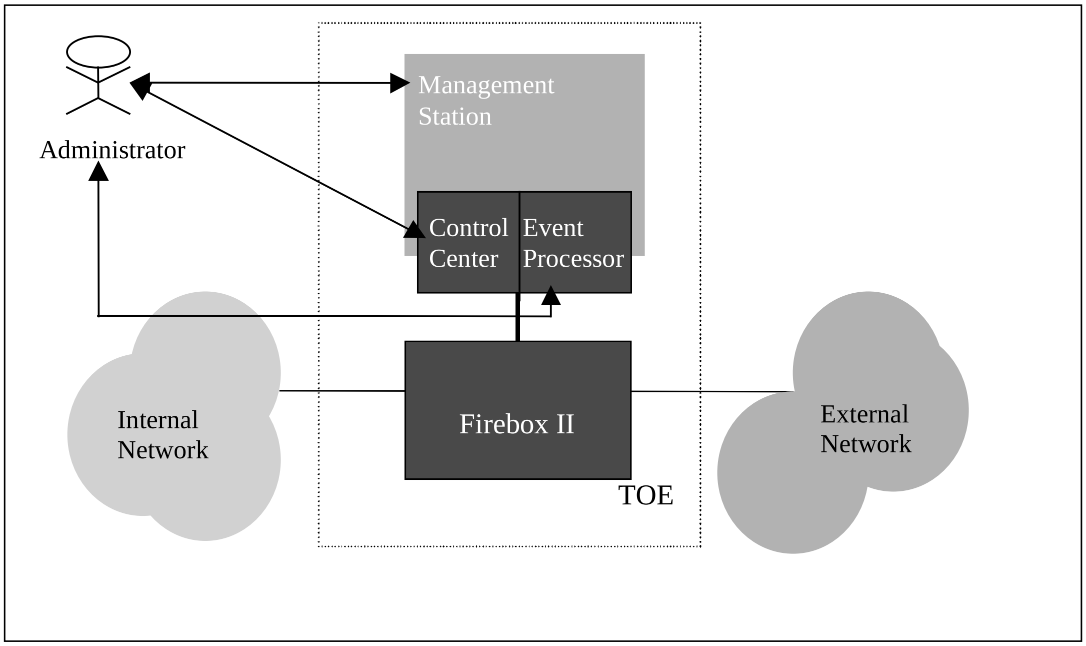

Figure 1: TOE Physical Boundary

18 The Control Center combines access to WatchGuard applications and tools in one intuitive interface. The Policy Manager is one of the tools accessed via the Control Center QuickGuide toolbar.

19 The Policy Manager configures the Firebox, and also displays a real-time monitor of traffic through the Firebox, connection status, and recent log activity. Firebox configuration results in the creation of the Firewall configuration file and component selection and generation into the Firebox operating system. The configuration file specifies the Firebox network environment parameters and information flow; i.e., security policy, firewall name, interface IP addresses, netmasks, stateful packet filtering, and proxies. The Firewall operating system is generated from several mandatory components and optional components to provide only the functionality to implement the Firebox information flow security policy. The Firebox operating system is built and then uploaded with the configuration file to the Firebox when the administrator saves the configuration file to the Firebox. The Firebox stores the operating system image and configuration file in flash memory.

2.1 Subsystem Description

20 WatchGuard is comprised of two physical components and fourteen (14) subsystems. Figure 2 identifies the physical location of each major subsystem grouping.

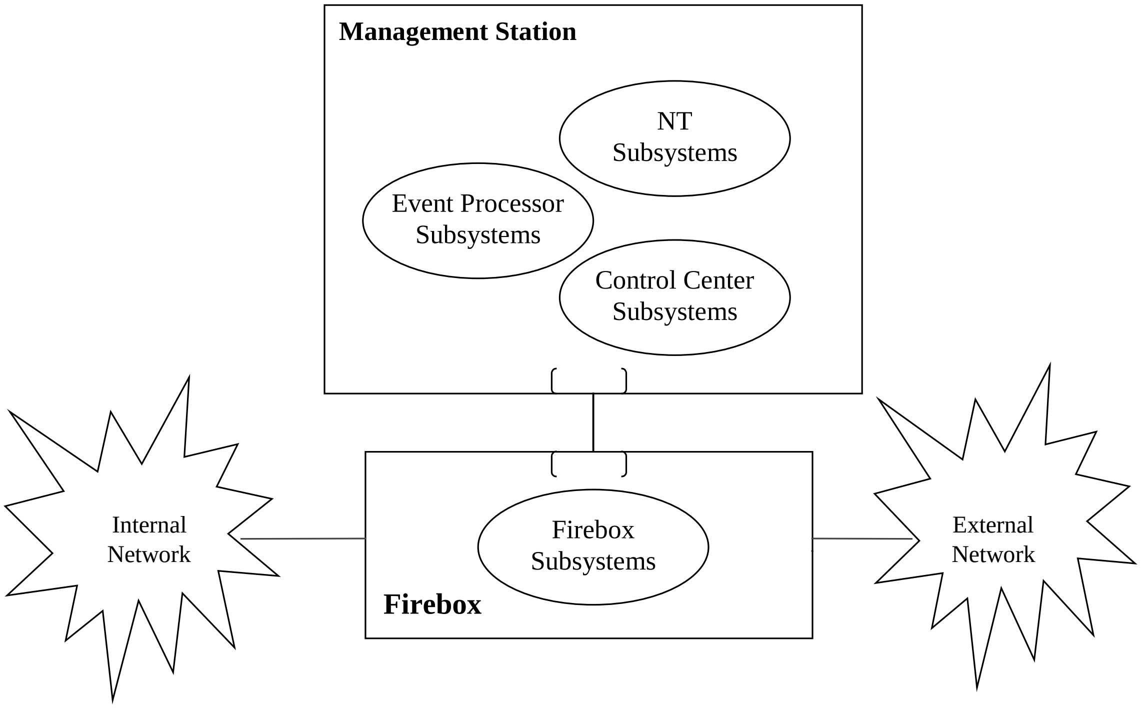

Figure 2: Management Station and Firebox Subsystem Groupings

21 Table 2 identifies the subsystems that comprise each Management Station subsystem grouping, and provides a brief description of each subsystem.

Table 2: Management Station Subsystems

Subsystems	Description
Control Center Subsystems	
Control Center	Combines access to WatchGuard LiveSecurity System applications and tools in one intuitive interface.
Policy Manager	Enables the system administrator to configure the Firebox.
Firebox Monitors	User interface providing real-time display of traffic through the firewall.
LogViewer	Displays log file data, syslog data, and bootup and kernel messages.
Historical Reports	Enables the system administrator to generate summaries and create reports from Firebox log files.
HostWatch	Displays active connections occurring on the Firebox.
Event Processor Subsystems	
LiveSecurity Event Processor	Controls logging, notification, and report scheduling services on the Firebox.
NT Subsystems	
NT Authentication	Provides NT trusted path and authentication services.
NT Access Control	Provides NT access control services.
NT Audit	Provides NT audit services for system, security, and application audit events.

Subsystems	Description
NT Utilities	Provides the system administrator with tools to configure the NT system.

22 Table 3 identifies and provides a brief description of the Firebox subsystems.

Table 3: Firebox Subsystems

Subsystems	Description
Boot	Enables Firebox to communicate with remote systems.
Root	Provides booting, integrity checking, log event detection, and provides stateful packet filtering security policy enforcement.
Proxy	Provides application layer security policy enforcement.

23 The next two subsections will describe the WatchGuard developed and the NT developed subsystems and their interfaces.

2.2 WatchGuard Subsystems

24 The TOE subsystems developed by WatchGuard consist of the Control Center, Event Processor, and Firebox II subsystem groupings as shown in Figure 3.

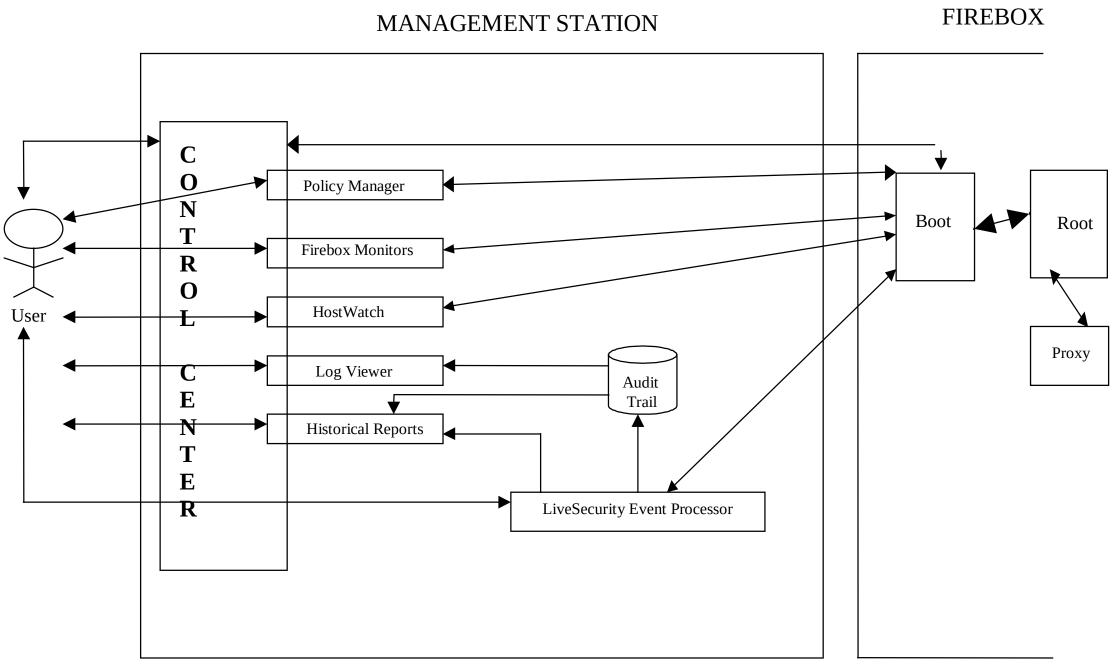

Figure 3: Subsystem Diagram

2.2.1 Management Station Subsystems

25 The WatchGuard Management Station subsystems are as follows:

1. Control Center
2. Policy Manager
3. Firebox Monitors
4. LogViewer
5. Historical Reports
6. HostWatch
7. LiveSecurity Event Processor (LSEP)

2.2.1.1 Control Center Subsystem

26 The WatchGuard Control Center provides a single interface to access the following WatchGuard applications and tools:

Table 4: Control Center Applications and Tools

Subsystems	Executable	Purpose	Interfaces with
Control Center	center.exe	Provides status information	Launches all the tools; Firebox II
Policy Manager	sms.exe	Used to configure management policy of Firebox II	Control Center, Firebox II
Firebox Monitors	wgmonitors.exe	Provides status information	Control Center, Firebox II
HostWatch	wghostmon.exe	Provides status information	Control Center, Firebox II
LogViewer	logviewer.exe	Log reader	Control Center, LSEP
Historical Reports	WGReports.exe	Log reader and report generator	Control Center, LSEP

27 The Control Center subsystem provides to the administrator a toolbar and menu system to enable the administrator to quickly connect to the Firebox II, view real-time status displays, and launch other tools.

2.2.1.2 Policy Manager Subsystem

28 The Policy Manager subsystem provides the GUI interface that enables the administrator to design, configure, and manage the electronic portion of the Firebox II network security policy; Firebox II configuration file, installed operating system components, and read-only and read-write pass-phrases. These items when saved to the Firebox II flash memory enable the Firebox II to enforce the network security policy.

2.2.1.3 Firebox Monitors Subsystem

29 The Firebox Monitors subsystem provides the system administrator a real-time display of traffic going through the Firebox II. If the Firebox Monitors is functioning using the read-write pass-

phrase, the Firebox Monitors establishes a "read-write" encrypted socket session with the Firebox II. The Firebox II sends real-time traffic flow information to the Firebox Monitors which displays the traffic pattern information on the BandwidthMeter tab. The connection with the Firebox II remains until the Firebox Monitors is terminated.

2.2.1.4 LogViewer Subsystem

30 The LogViewer Subsystem provides the system administrator with the capability to read the audit trail that contains all log data received from the Firebox II. The administrator can browse the Windows NT file system and select a log file. By default, logs are stored in a subdirectory of the WatchGuard installation directory called \logs. LogViewer will open and display the selected log file in a readable format. The user is also able to filter the records that are displayed by key phrase (alphanumeric string) or field.

2.2.1.5 Historical Reports Subsystem

31 The Historical Reports subsystem provides the system administrator with the ability to generate summaries or reports of the Firebox II log activity. When Historical Reports is executed, the system administrator is prompted to build a template of the summary or report to be generated. When the administrator selects to run a report, Historical Reports generates the report by using the appropriate reportname.rep file and accessing the audit files. The report is placed in the specified output directory. If no output directory is specified, the report is written to the WatchGuard installation directory. The LiveSecurity Event Processor, for a scheduled report, will launch the Historical Reports executable at the scheduled time and pass it the reportname.rep file. Historical Reports will proceed to generate the report by using the named reportname.rep file and accessing the audit files. Once the report is generated, Historical Reports will terminate.

2.2.1.6 HostWatch Subsystem

32 The HostWatch subsystem provides the system administrator with real-time display of active connections on the Firebox II. The HostWatch establishes a read-only encrypted socket connection with the Firebox II to retrieve real-time active connection information. The connection with the Firebox II remains until HostWatch is terminated.

2.2.1.7 LSEP Subsystem

33 The LiveSecurity Event Processor (LSEP) subsystem controls logging, notification, and scheduling services for the Firebox II. It also provides timing services for the Firebox II. LSEP is installed on the NT platform as an NT service that is started automatically every time the Management Station is booted. The LSEP can be stopped or restarted from its GUI interface at any time.

34 When the LSEP is executed, it initiates a read-only encrypted socket connection with the Firebox II using the read-only pass phrase. The Firebox II uses this connection to send log events to the LSEP, which in turn writes all information to the audit files. If the administrator had specified for a notification to occur for certain situations, the Firebox II would send a notification message to LSEP. LSEP would then perform the notification as specified in the controld.wgc configuration file. The connection with the Firebox II remains until LSEP is terminated or the service is stopped.

35 The LSEP also provides a GUI interface, the Event Processor Interface. This interface allows the administrator to specify the maximum number of records to store in a log file, schedule reports of log activity, and control to whom and how notifications take place.

2.2.2 Firebox II Subsystems

36 The WatchGuard Firebox II subsystems are as follows:

1. Boot
2. Root
3. Proxy

37 A description of the security functionality provided by each subsystem and external interface identification is provided in the following subsections.

2.2.2.1 Boot Subsystem

38 The Boot subsystem provides the Firebox II with the capability to communicate with remote systems using its Ethernet Network Interface Card (NIC) and serial port.

39 The Boot subsystem consists of the Ethernet and WAN modules. The Ethernet Driver module provides the Linux kernel with the functionality to send and receive Ethernet packets. The Ethernet module complies with the IEEE 802.3 protocol standard. The WAN driver module provides the Linux kernel with the functionality to establish Point-to-Point (PPP) and Serial-Line-Interface-Protocol (SLIP) connections on the Firebox II serial interface. The WAN Driver module complies with the SLIP and PPP protocol standards.

2.2.2.2 Root Subsystem

40 The Root subsystem provides the Firebox II with the functionality to perform Firewall booting, integrity checking, logging event detection, generation, and transmission, and security policy enforcement. The Root subsystem consists of the Init, FW Check, Logging Client, Firewalld, and Firewall Engine modules.

2.2.2.3 Proxy Subsystem

41 The Proxy subsystem consists of the SMTP proxy module. The SMTP Proxy Module searches and rejects malformed SMTP service commands. The Firewall directs packets to the SMTP proxy when such packets are received by the Firebox II and successfully pass the stateful packets filter tests performed by the Firewall Engine Module. The SMTP Proxy will filter incoming and outgoing SMTP packets and only allow explicitly authorized content types and header patterns and disallows packets that contain specific address patterns or fail content and header pattern checks. The SMTP Proxy module generates log event messages that are passed through the Firewall process to the Logging Client when a filtering operation identifies that an SMTP packet fails a filtering test.

2.3 Windows NT Subsystems

42 The TOE Windows NT subsystems are as follows:

a) NT Access Control

b) NT Authentication

c) NT Utilities

d) NT Audit

43 The Windows NT subsystem descriptions provide only a high-level description of the security aspects of each subsystem.

2.3.1 NT Access Control Subsystem

44 The NT Access Control subsystem uses access tokens, which have been generated as a result of the authentication process, to identify the security context of a process or thread. A security context consists of information that describes the privileges, accounts, and groups associated with the process or thread. All programs that a user executes inherit a copy of the user’s initial access token.

45 The NT Access Control subsystem uses two token components to determine the privileges or access rights that a token's thread or process has. The first component comprises the token's user account SID and group account SID fields. The NT Access Control subsystem uses these SIDs to determine whether a process or thread can obtain requested access to a securable object. The second component is the token’s privilege array. A token's privilege array is a list of rights associated with the token.

46 The NT Access Control subsystem will produce audit records for all the attempts to archive, create, delete and empty the audit trail. Additionally, the NT Access Control subsystem will produce an audit record for changes to the system time. When changes have been made to a user’s privileges, this subsystem will also generate an audit record.

2.3.2 NT Authentication Subsystem

47 The NT Authentication subsystem provides a Trusted Path through the Secure Attention Sequence (SAS) preventing Trojan Horse programs from intercepting a user's name and password as the user logs on. This Trusted Path functionality exists in the form of its Ctrl+Alt+Del logon-attention sequence – the SAS.

48 The secure logon process follows the SAS. The logon interface package is known as a Graphical Identification and Authentication (GINA) library. When a user identifies themselves through the dialogue box with a username and password, MSGINA sends the gathered information to the Local Security Authority Sub System (LSASS) process, located in the *winnt\system32\lsass.exe* directory, with a local procedure call (LPC) message.

49 LSASS is the front end of the authentication mechanism for NT. The LSASS process uses a replaceable MSV1_0 library, located in the *winnt\system32\msv1_0.dll* directory, as its authentication package. LSASS calls the MSV1_0 library and passes the username and password attributes. MSV1_0 must then determine if the logon attempt is local or domain based.

50 This subsystem generates audit records for all uses of the NT identification and authentication mechanism.

2.3.3 NT Utilities Subsystem

51 The NT System Utilities subsystem provides the system administrator with a number of tools for configuring the NT system. Many of these tools provide supporting security functionality for the TOE.

2.3.3.1 Event Viewer

52 Event Viewer is NT's log file monitoring utility. Through Event Viewer, a user can examine the contents of the three main NT log files: System, Security, and Application. The System Log records events for internal processes, services, and drivers. The Security Log records security audit events, such as logons, access to user rights, object access, user/group management, and system shutdowns or restarts. The Application Log records application-related alerts and system messages.

2.3.3.2 User Manager for Domains

53 User Manager for Domains is a management tool for user and group-based NT security. With this utility, a user can create, modify, and manage users and groups. There are many configurable options such as group membership, profile settings, home directory assignment, logon script pointers, access scheduling, workstation privileges, and RAS restrictions. This utility also provides a facility for the management and control of system policies regarding accounts, user rights, and auditing. The account system policy sets parameters for user passwords and account lockouts for failed logon attempts. The user rights system policy sets rights for each group or user.

54 The User Manager for Domains system utility provides the user with the ability to configure account attributes that are used during the authentication process by the NT Authentication Module. The utility provides the ability to configure the user identification and password and to set the system account policy. This utility provides the facility for the administrator to provide unique accounts for all individual users of the system. When changes have been made to the account policy, the user rights policy or the audit policy an audit record will be generated and forwarded to the NT Audit subsystem.

2.3.3.3 Time & Date

55 The NT Operating System provides a system utility for changing the date and/or time for the host hardware platform that the operating system is residing on. The date and time system utility has a graphical user interface which allows for a privileged user to set and configure the date and/or time. This system utility controls the time and date on the host system through the Windows Hardware Abstraction Layer (HAL).

2.3.4 NT Audit Subsystem

56 The NT Audit subsystem provides three categories of event logs: *System*, *Security*, and *Application*. The event logs are located in the directory: *winnt\system32\config* The three log files are *sysevent.evt*, *secevent.evt*, and *appevent.evt*. These files cannot be accessed by a regular text editor as they are stored in a specific format. The Event Viewer component of the NT Utilities subsystem lets you see the contents of each log, including the most recent information.

57 The NT Auditing subsystem has the ability to capture many different types of records in response to a multitude of system events and user actions.

2.3.4.1 Audit Records Generated

58 An audit record is generated by this subsystem when the NT audit functions have started or shut-down. An audit record can be captured for any change to the set of user or group accounts managed by the system. The NT Audit subsystem can be configured to capture an audit record for all attempts to logon to the system. The NT audit record shows the information that is captured when a change is made to the system time or date. The NT Audit subsystem can produce an audit record for all access to any file or directory object created on an NTFS formatted drive. Additionally, when a user makes a change to the Control Center logs by archiving and purging the log files through the Log Viewer application, a message is sent to the NT Auditing subsystem and the following audit records is captured as an Application Event Log.

3 EVALUATION

3.1 Evaluation Methods, Techniques, and Standards

59 The *evaluator action elements* documented in [CC_PART3] for EAL 2 assurance components were the basis of the approach for evaluating the TOE. In addition, [CEM_PART2] Chapter 6 was used to define the specific evaluator actions for conducting the evaluation.

60 To manage the evaluation effort and to document progress and findings, the evaluation team developed evaluation work package reports for each assurance family as listed in Table 5. All CEM work units associated with these assurance components were completed and addressed as instructed by the Scheme.

Table 5: Evaluation Work Packages

Work Package	Assurance Component
Security Target	ASE
Configuration Management	ACM_CAP.2
Delivery and Operation	ADO_DEL.1
	ADO_IGS.1
Development	ADV_FSP.1
	ADV_HLD.1
	ADV_RCR.1
Guidance Documents	AGD_ADM.1
	AGD_USR.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessments	AVA_SOF.1
	AVA_VLA.1
Assurance Maintenance	AMA_AMP.1
	AMA_CAT.1

61 For the ATE_IND.2.2E evaluator action element, the evaluation team wrote a test plan and conducted functional testing in accordance with the plan. For the AVA_VLA.1.2E evaluator action element, the evaluation team identified the current list of obvious vulnerabilities. The team wrote a test plan for penetration testing and conducted tests in accordance with the plan.

62 No Observation Reports against the CC or CEM were generated during the course of the evaluation. Evaluation Discovery Reports (EDRs) were generated for the following reasons:

- To identify a potential vulnerability or deficiency found in the TOE;
- To identify deficiencies found in evaluation evidence; and
- To request additional information from the vendor.

63 EDRs were submitted to the vendor and not formally distributed to the TTAP Oversight Board, although the Certifier did receive a copy of all EDRs. Chapter 8, Problem Reports, contains a listing of all EDRs that were generated during the evaluation.

3.2 Evaluation Tools

64 To perform independent and penetration testing activities, the evaluation team used network tools:

- to observe the success or failure of information flows through the TOE based on flow rules;
- to examine packet information at all protocol layers for residual information; and
- to manipulate network and application layer flows to simulate various attack scenarios.

65 The evaluation team used network tools found in the public domain and proprietary tools developed by Computer Sciences Corporation.

3.3 Evaluation assumptions and constraints

66 The evaluation results and evidence will be maintained and retired as specified in CSC's Common Criteria Evaluation Laboratory Quality Manual.

67 While the TOE does not make a protection profile (PP) conformance claim, CERT Advisories from firewall PPs were used in the completion the AVA work package. CERT Advisories prior to December 1997 were not assessed since it was deemed that the firewall PP writers had already discounted these.

4 RESULTS OF THE EVALUATION

68 This Chapter presents the findings and results of the evaluation by identifying the verdict with supporting rationale for each assurance component that constitutes an activity for the ST Evaluation and EAL 2 Evaluation. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. Three mutually exclusive verdict states can be rendered:

- Pass, if the evaluator successfully completes a [CC_PART3] evaluator action element. The conditions for successfully completing an evaluator action element are defined by the constituent work units of the related [CEM_PART2] action.

- Inconclusive, if the evaluator has not completed one or more work units of the [CEM_PART2] action related to the [CC_PART3] evaluator action element.

- Fail, if the evaluator unsuccessfully completes a [CC_PART3] evaluator action element.

69 Section 5 provides the overall verdict of the evaluation team's findings as defined in [CC_PART1] Chapter 5, and determined by the verdict assignments presented in this Chapter.

70 Table 6 provides a listing of the activities, associated assurance components, and evaluator action elements for a ST Evaluation and an EAL 2 Evaluation.

Table 6: Evaluation Activities, Assurance Components, and Action Elements

Activity	**Assurance Component**	**Evaluator Action Elements**
ST Evaluation	ASE_DES.1	ASE_DES.1.1E, ASE_DSE1.2E, ASE_DES1.3E
	ASE_ENV.1	ASE_ENV.1.1.E, ASE_ENV.1.2E
	ASE_INT.1	ASE_INT.1.1E, ASE_INT.1.2E, ASE_INT.1.3E
	ASE_OBJ.1	ASE_OBJ.1.1E, ASE_OBJ.1.2E
	ASE_PPC.1	ASE_PPC.1.1E, ASE_PPC.1.2E
	ASE_REQ.1	ASE_REQ.1.1E, ASE_REQ.1.2E
	ASE_SRE.1	ASE_SRE.1.1E, ASE_SRE.1.2E
	ASE_TSS.1	ASE_TSS.1.1E, ASE_TSS.1.2E
Configuration management	ACM_CAP.2	ACM_CAP.2.1E
Delivery and operation	ADO_DEL.1	ADO_DEL.1.1E
	ADO_IGS.1	ADO_IGS.1.1E, ADO_IGS.1.2E
Development	ADV_FSP.1	ADV_FSP.1.1.E, ADV_FSP.1.2E
	ADV_HLD.1	ADV_HLD.1.1E, ADV_HLD.1.2E
	ADV_RCR.1	ADV_RCR.1.1E
Guidance documents	AGD_ADM.1	AGD_ADM.1.1E
	AGD_USR.1	AGD_USR.1.1E
Tests	ATE_COV.1	ATE_COV.1.1E
	ATE_FUN.1	ATE_FUN.1.1E
	ATE_IND.2	ATE_IND.2.1E, ATE_IND.2.2E, ATE_IND.2.3E

Activity	Assurance Component	Evaluator Action Elements
Vulnerability assessment	AVA_SOF.1	AVA_SOF.1.1E, AVA_SOF.1.2E
	AVA_VLA.1	AVA_VLA.1.1E, AVA_VLA.1.2E

4.1 Security Target

4.1.1 ASE_DES.1 – TOE Description

71 The evaluator reviewed the TOE description section of the WatchGuard Technologies WatchGuard LiveSecurity System with Firebox II 4.1 Security Target, to make a determination that the section describes the WatchGuard LiveSecurity System with Firebox II 4.1, the TOE. The TOE description defines the boundaries of the TOE in both a physical and logical way. It was clear to the evaluator after reading the TOE description that the product is a hybrid firewall product that performs both dynamic packet filtering and transparent proxies to control and monitor the flow of IP packets through the firewall.

72 The TOE description was checked for consistency by looking for any contradictory statements that might appear within this section of the ST. No statements were found while examining the TOE description that contradicted each other.

73 The TOE description was checked for consistency with other sections of the ST. This consistency check was performed in conjunction with the other ASE work units. The description given of the functionality and assurance measures of the TOE are consistent throughout the whole ST.

74 ASE_DES.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_DES.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.2 ASE_ENV.1 – Security environment

75 The security environment section of the [LSS_ST] was used to satisfy this assurance component. The evaluator reviewed this section to determine that it identifies the assumptions and threats for the TOE and its environment. The [LSS_ST] does not contain any organizational security policies.

76 While reviewing the individual assumptions and threats the evaluator was also determining if the assumptions and threats were coherent, understandable to the evaluator and the audience for the [LSS_ST]. An overall consistency verdict was reached after all the assumptions and threats had been reviewed. Part of the consistency check was to make sure that no assumptions are in conflict with the threats and that the threats, as specified, are plausible based on the threat agents described, the attack and the asset that could be under attack.

77 ASE_ENV.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_ENV.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.3 ASE_INT.1– ST introduction

78 The evaluator reviewed the security target introduction section of the [LSS_ST] to satisfy the evaluator elements of this assurance component. The ST introduction of the [LSS_ST] clearly identifies the [LSS_ST] with a name and version for the [LSS_ST]. Along with the [LSS_ST] identification it also gives a unique label with a version number for the TOE under evaluation. The CC version used to develop the ST is clearly identified in the [LSS_ST].

79 Part of the evaluation of the [LSS_ST] introduction was to determine if it contained a narrative description of the [LSS_ST]. The [LSS_ST] clearly states what is in the [LSS_ST]. It is stated in such a manner and to a level that is clear that a hybrid firewall product that performs both traffic-filtering and application filtering on IP packets is being described and thereby indicating the functionality that is being provided by the TOE.

80 The [LSS_ST] introduction clearly states the conformance claims of the [LSS_ST]. It mentions the relevant Part 2 and 3 conformance claims to the CC.

81 The evaluator determined that the [LSS_ST] introduction is coherent by reading the section and being able to understand what was being described in the section. Further it was determined that the section was consistent because the statements of functionality and use of terms in this section did not conflict with each other.

82 It was determined that the [LSS_ST] introduction is consistent with the other sections of the [LSS_ST]. The determination of consistency with the other sections of the [LSS_ST] was undertaken while working on the other evaluator actions in other ASE components. The evaluator checked for consistency in the [LSS_ST] by reviewing all the other sections of the [LSS_ST]. The evaluator looked for any conflict between the description of functionality through out the different sections of the [LSS_ST]. This included looking at the functional requirements and the security functions described in the TOE summary specification. The words of the assumptions, threats, and objectives were compared with each other and the functional requirements to determine that they did not conflict with each other. The conventions and terminology were used consistently throughout the [LSS_ST].

83 ASE_INT.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_INT.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.4 ASE_OBJ.1 – Security objectives

84 The evaluator reviewed the ‘security objectives’ section of the [LSS_ST] to satisfy the evaluator elements of this assurance component. The [LSS_ST] security objective section breaks the objectives out into security objectives for the TOE and security objectives for the environment.

85 The evaluator reviewed the mappings supplied by the developer in the [LSS_ST] to see that all security objectives for the TOE are traced back to the identified threats to be countered by the TOE. The evaluator developed a table that contained the threats and objectives for the TOE. This table was used to determine that all threats for the TOE are being mapped to the objectives of the TOE and that all the objectives of the TOE are being used and mapped to the threats of the TOE. The evaluator’s table was a check on the developer’s generated table to determine that it was accurate with respect to the objectives and threats being listed and articulated elsewhere in the [LSS_ST].

86 The same approach described in the above paragraph was used to determine that the objectives for the environment are traced backed to threats and assumptions not completely countered by the TOE. This approach again was used to verify a mapping that the developer provided in the [LSS_ST].

87 The evaluator read each security objective in the [LSS_ST] to make a determination that each objective is clearly stated and understandable.

88 As part of determining the tracings discussed above the evaluator was also reviewing the rationale that was being given by the developer as to why a particular mapping was suitable to cover an identified threat and/or assumption. The rationale given by the developer explained how the objectives are suitable to cover the threats and/or assumptions stated in the [LSS_ST].

89 ASE_OBJ.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_OBJ.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.5 ASE_PPC.1 – PP claims

90 There are no Protection Profile conformance claims.

91 ASE_PPC.1 Verdict: The evaluation team concluded that the TOE has trivially met the assurance requirements of ASE_PPC.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.6 ASE_REQ.1 – IT security requirements

92 The evaluator examined the [LSS_ST] to accomplish the evaluator activities for ASE_REQ.

93 Part of the examination of the requirements of the [LSS_ST] was to see if the functional requirements are transcribed from the CC correctly. The functional requirements in the [LSS_ST] were compared to Part 2 of the CC during examination of the requirement sections. If the functional requirement was not exactly transcribed from the CC then the operations performed on the functional requirements in the [LSS_ST] were examined. The examination of the operation was used to determine if the operation fit within the bounds for that specific functional requirement as stated in the CC. Also part of the comparison of the functional requirements involved making sure that those operations that are performed in the [LSS_ST] are properly identified. The same procedure was used for the assurance requirement section of the [LSS_ST].

94 The dependency analysis and rationale was confirmed through independent analysis by the evaluator.

95 The examination of the functional requirement section of the [LSS_ST] involved checking for a statement of Strength of Function (SOF) and checking that the appropriate requirements contained a SOF statement. The SOF rationale was examined to determine if it was appropriate for the TOE and the environment of the TOE.

96 The rationale for the assurance and functional requirements was examined. The examination of this rationale was undertaken to determine if the security requirements are able to meet the objectives specified in the [LSS_ST]. The evaluator was also examining the IT security requirements rationale to see if there is a demonstration of how the security requirements are a

mutually supportive and consistent whole. After reviewing the requirements rationale it could be seen that the requirements where mutually supportive in satisfying the security objectives of the [LSS_ST]. The evaluator examined the security requirements, objectives, the mappings in the [LSS_ST], and the requirement dependencies in achieving the satisfaction of mutually supportive and consistent whole. The requirements supported each other by setting up a security perimeter for the TOE that is non-bypassable and that maintains a separate domain that only the TOE executes in. This allows the security functions that enforce the traffic -filter and application-filter and auditing rules of the TOE to execute without interference. Further, the non-bypassable separate domain of the TOE only allows for those authorized to administer the TOE to do so. The requirements in the [LSS_ST] are a mutually supportive and consistent whole because the requirements are structured and support each other, in a non-contradictory way, to enforce the security objectives expressed in the [LSS_ST].

97 ASE_REQ.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_REQ.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.7 ASE_SRE.1 – Explicitly stated IT security requirements

98 There are no explicitly stated IT security requirements.

99 ASE_SRE.1 Verdict: The evaluation team concluded that the TOE has trivially met the assurance requirements of ASE_SRE.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.8 ASE_TSS.1 – TOE summary specification

100 The evaluator examined the TOE summary specification section of the [LSS_ST]. The evaluator examined the summary specification for the functional and assurance requirements.

101 The evaluator examined each security function to determine that it was to a level of detail that summarized what the security functionality is and if the security function could satisfy the security functional requirement that it was mapped back to. The evaluator also checked that each security functional requirement had at least one security function being mapped to it.

102 The mapping of assurance measures to assurance components were examined. The evaluator checked to make sure that each assurance component had a measure mapped to it and the measure is appropriate to satisfy a particular assurance component.

103 To accomplish the examination of the TOE summary specification the evaluator came up with their own tables to supplement and check the consistency of the tables supplied in the [LSS_ST].

104 ASE_TSS.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ASE_TSS.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.2 Configuration management

4.2.1 ACM_CAP.2 – CM capabilities

105 The evaluator checked and examined [LSS_CM] and [LSS_ST], as well as [LSS_UG_4.1], [LSS_SW_CD], [LSS_RELNOTES], [LSS_IG]. The evaluator examined [LSS_ST] to understand the definition of the TOE and then checked [LSS_CM] to determine if the Configuration Items (CI) identified made sense given the TOE definition. The Configuration Management documentation allowed the evaluator to validate the uniqueness of the identifiers of the items that comprise the TOE. Consequently, the use of these items in the evaluation of the product for this assurance class assures the consumers they have purchased and installed the evaluated version of the TOE using the correct version of the guidance to operate the TOE in accordance with its ST.

106 The evaluator validated the uniqueness of the reference by checking the CI list to ensure that the CIs were uniquely identified. The evaluator further identified a referencing system that was capable of supporting unique references (e.g., numbers, letters, or dates). The evaluator checked the Firebox II subsystem of the TOE to determine if it was labeled with its reference and found a plate affixed to the rear of the Firebox II chassis that contained the serial number of the device. The evaluator found that the labeling is used consistently in the guidance documentation, the [LSS_SW_CD], and both the hardware and software components of the Firebox II hardware.

107 The CI list in the [LSS_CM_1.1, Appendix A] identified the configuration items that comprise the TOE based on CM system "list" commands. The CI list demonstrated the parallel CM systems, CVS and VSS, maintain the configuration items based on version numbers incremented as changes are applied to files, and branching and builds/TOE versions based on specified tags (branches and tags are supported by both CM systems).

108 ACM_CAP.2 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ACM_CAP.2. Therefore, a **pass** verdict has been issued for this assurance component.

4.3 Delivery and operation

4.3.1 ADO_DEL.1 – Delivery Procedures

The evaluator checked and examined the following evidence [LSS_DEL] and [LSS_IGSG]. After examining [LSS_DEL], the evaluator determined that the use of a LiveSecurity license keys and a protective packaging is adequate to provide secure delivery of the TOE, given the low-risk environment specified in the [LSS_ST]. The evaluator did verify the procedures for delivery through conversations with the LiveSecurity Team at WatchGuard Technologies. The LiveSecurity Team is responsible for for maintaining the WatchGuard Web Site (www.watchguard.com). The evaluator has determined that all requirements for this component have been satisfied.

109 ADO_DEL.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ADO_DEL.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.3.2 ADO_IGS.1 – Installation, generation, and start-up procedures

110 The evaluation team checked and examined the following evidence: [LSS_IGSG] and [LSS_ST]. The evaluator found that the procedures for secure installation, generation and startup were provided. The evaluator determined that the evidence did describe the necessary steps for secure installation, generation, and startup of the TOE. [LSS_IGSG] methodically describes the installation and configuration of the Management Station, physical connection of the Firebox II appliance, and start-up procedures. In addition, the procedures were verified through testing activities in the ATE_IND work units.

111 ADO_IGS.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ADO_IGS.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4 Development

4.4.1 ADV_FSP.1 – Informal functional specification

112 The evaluator used the TOE administrator guidance and the NT administrator guidance referenced in the [LSS_FSP] to help in the assessment of this assurance component. The other documents that were used were the [LSS_ST], [LSS_HLD], [LSS_UG_4.1] and [LSS_RCR]. Through the evaluation of the evidence, it was determined that the functional specification was composed of the [LSS_FSP], the [LSS_HLD], the [LSS_RCR], the TOE administrator guidance that comes with the TOE and the NT administrator guidance referenced in the [LSS_FSP].

113 To satisfy this assurance component, the evaluator relied on the supporting information provided in the [LSS_HLD], [LSS_UG_4.1] and [LSS_RCR] to corroborate and supplement the [LSS_FSP]. The evaluator used the [LSS_ST] and the supporting descriptions of the TOE provided in the high-level design, functional specification, and user manuals that are part of the TOE to determine the TOE boundary. Through examination of these documents the evaluator determined that the external interfaces to the TOE are the Management Station GUI, the external and internal networking interfaces and the GUIs supplied by the NT workstation.

114 The [LSS_FSP] helps satisfy this assurance component by identifying the security functional components of the TOE. The [LSS_FSP] references several reference manuals provided with the TOE, as well as NT administrator manuals. These manuals help satisfy the functional specification assurance requirement by further defining and describing the security functionality of the components and the external interfaces of the TOE. The [LSS_HLD] supplements the [LSS_FSP] by defining the interface input parameters and behavior of the interfaces in the management of the functional components of the TOE, as well as the network and NT interfaces. The reference manuals describe the Management Station GUI interfaces and the LiveSecurity Event Processor interface. The developer is using RFCs for the description of the network interfaces of the TOE, and these are described in the [LSS_HLD]. The RFCs describe the protocol interface that is used to control the networking interfaces.

115 The evaluation of the functional specification was linked to the evaluation activities of the correspondence evidence. The information provided in the correspondence mappings was used by the evaluator to map the security functional requirements in the [LSS_ST] to the security functions and the TSF interfaces as presented in the [LSS_FSP] and [LSS_HLD]. This permitted the evaluator to confirm the TOE security functions satisfy the security functional requirements.

116 Using the correspondence mapping, the evaluator examined the security functions described in the TOE Summary Specification [LSS_ST] to confirm the security functional requirements were completely satisfied, and that the security functionality actually existed in the TOE to support the functional requirement. The evaluator also used the correspondence mapping and the interface descriptions in the [LSS_HLD] to external interfaces with the potential to impact the security functionality of the TOE. This provided the evaluation team information on which external interfaces to test security functionality of the TOE.

117 Through examination of the correspondence mappings and the description of the security functions it can be seen that the TOE has all the necessary security functionality to satisfy the security functional requirements in the [LSS_ST].

118 ADV_FSP.1 Verdict**:** The evaluation team concluded that the TOE has met the assurance requirements of ADV_FSP.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4.2 ADV_HLD.1 – Descriptive high level design

119 The evaluator while examining the high-level design looked to see if it was in terms of major structural units. The evaluator also examined the high-level design to determine if it contained the major structural units to satisfy the security functional requirements in the [LSS_ST]. The high-level design for this evaluation is in terms of subsystems.

120 The [LSS_HLD], the high-level design document, was the primary document reviewed to satisfy this assurance component. The document has individual sections that describe each subsystem. The description given in each section describes the security functionality that the subsystem supports. The high-level design of the TOE described an architecture that allows for the satisfaction of the security functional requirements that are present in the [LSS_ST]. Further the high-level design shows the information flow and relationships between the different subsystems of the TOE.

121 The correspondence document, [LSS_RCR], was an important document in the satisfaction of this assurance component. The correspondence mappings provide a mapping of the security functions onto subsystems. This allowed the evaluator to determine if the subsystem contained the proper functionality to satisfy the security function(s) being mapped to the subsystem. This also allowed the evaluator to determine if there were enough subsystems to cover all the security functionality (security functions and security functional requirements) being described in the [LSS_ST].

122 The evaluator followed the requirements and guidance for the configuration management activity for EAL 2 as specified in the [CEM_PART2] to determine if the high-level design assurance class requirements were met. If the work unit specified that a condition/item be *check*ed, the evaluator generated a verdict through comparing the evidence, TOE action, or both, against the requirement specified in the work unit. If the work unit specified that the evaluator's action was to *examine*, the verdict was based on direct analysis of the object, specified in the work unit, for the properties also specified in the work unit.

123 The evaluation team does not believe it is the intent of EAL 2 high-level design to describe all interfaces to the subsystems. The evaluation team believes that for EAL 2 it is more appropriate that the relationship of the subsystems should be shown in a high-level design. The evaluation

team believes that the [LSS_HLD] meets the intent of the ADV_HLD.1 component by showing the relationships and flow of information between the subsystems.

124 ADV_HLD.1 Verdict**:** The evaluation team concluded that the TOE has met the assurance requirements of ADV_HLD.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4.3 ADV_RCR.1 – Informal correspondence demonstration

125 The main evidence examined for this assurance component was [LSS_RCR], [LSS_HLD], [LSS_ST], TOE documents (administrator, installation, etc.) and [LSS_FSP]. The [LSS_RCR] document supplied all the relevant mappings that are required for this assurance component. The correspondence document mapped security functions to security functional requirements. It mapped security functions to TSFIs. It further mapped security functions onto subsystems. With all these mappings the evaluator had enough information to determine which TSFI was being used to satisfy which security functional requirements and which subsystem is responsible for the security functionality. These mappings allow for a correspondence between the functional requirements, security functions, TSFI, and the high-level design.

126 ADV_RCR.1 Verdict**:** The evaluation team concluded that the TOE has met the assurance requirements of ADV_RCR.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.5 Guidance documents

4.5.1 AGD_ADM.1 – Administrator guidance

127 The evaluator used as the set of administrator guidance documents the following: [LSS_FSP], [LSS_UG_4.1], [LSS_ST], [LSS_IG_4.1], [LSS_IGSG], [LSS_DEL] and [LSS_HLD]. The TOE summary specification in the [LSS_ST] described that authorized users must authenticate and identify at the NT Login (interface 1) and identified two types of authorized administrator password access (interface 2): read/write, and read only for accessing the Firebox II. The administrator guidance did contain a description of the security functionality that is visible at the administrator interface. The entire interface is a GUI interface where the administrator is required to login and provide either a read/write password, or a read only password. The guidance identified and described the interfaces to configure the information flow policies, manage the audit trail to include selecting logged events, reviewing the log files, management of user accounts on Windows NT, and setting the system clock. The administrator guidance did describe how to operate the TOE in a secure environment as described in the ST and provided warnings and tips about functions and parameter settings that should be controlled. The administrator guidance described security parameters under the control of the administrator indicating appropriate secure values. The administrator guidance adequately describes the following security-relevant events relative to the administrative functions that need to be performed: audit trail overflow, system crashes and recovery, time changes, security policy flow changes, and user account changes. The administrator guidance was compared to the development evidence, installation, generation and startup procedures, and ST and was found to be consistent with these documents. Since the ST does not include requirements on the IT environment, the evaluator determined that descriptions concerning the IT security requirements was not applicable. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

128 AGD_ADM.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of AGD_ADM.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.5.2 AGD_USR.1 – User guidance

The WatchGuard does not allow users to interact directly with the security functionality of the TOE. Therefore, there is no requirement to provide any user documentation. The evaluation team determined that this assurance component as not applicable.

129 AGD_USR.1 Verdict***:*** The evaluation team concluded that the assurance requirements of AGD_USR.1 was not applicable and that the assurance component satisfied. Therefore, a **pass** verdict has been issued for this assurance component.

4.6 Testing

4.6.1 ATE_COV.1 – Evidence of coverage

130 The objective of ATE_COV.1 is to examine the vendor's test coverage of the security functions of the TOE. The evaluator mapped the vendor's tests to actual security requirements as stated in the [LSS_TCA_1.0] and the [LSS_ST]. In determining what the vendor covered, the evaluator is given the means to properly judge the efficiency of the vendor's analysis and insight into developing the independence testing.

131 The evaluator examined the nine tests the vendor provided and examined the [LSS_ST] and [LSS_TCA_1.0]. With these key items the evaluator determined that specific tests mapped to specific Security Functions as described in [LSS_ST]. The evaluator developed tables to establish the mappings and satisfaction of the SFRs.

132 ATE_COV.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ATE_COV.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.6.2 ATE_FUN.1 – Functional testing

133 The objective ofATE_FUN.1 is to evaluate the content of the tests provided by the vendor. The tests were examined for consistency between test plans, test procedures, expected test results, actual test results, security functions, initial TOE configuration(s) used. The evaluator determined if the test procedures provided sufficient detail to enable the evaluator to reproduce the test results achieved by the vendor.

134 The evidence used in this work unit was the test packages provided by the vendor. The evaluator used supporting evidence in the form of [LSS_ST] and [LSS_IGS_1.0]. The test plans are consistent throughout and test the security function as stated in the [LSS_ST].

135 ATE_FUN.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ATE_FUN.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.7 Independent testing results

4.7.1 ATE_IND.2 – Independent testing – sample

136 The objective of ATE_IND.1 is for the evaluator to review the tests provided by the vendor and to introduce some independent tests that will cover security functions that the vendor's tests did not address, thereby extending the TOE test coverage.

137 The evaluator examined the vendor supplied tests, and used the independent testing document [LSS_IND_0.1]. The vendor supplied test plans provided good coverage of the security functionality of the TOE. The introduction of the independent testing document [LSS_IND_0.1] introduced additional coverage of security functions tested through the vendor supplied tests. This [LSS_IND_0.1] provides a complete record of all independent tests including verification of vendors test data, admin ID, Flow and Audit. The evaluator tests consisted of a sampling of the vendor-supplied test plus the tests described in the independent testing document [LSS_IND_0.1]. The results of the tests were consistent with the expected test results and verified the requirements as stated by the [LSS_ST].

138 ATE_IND.2 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of ATE_IND.2. Therefore, a **pass** verdict has been issued for this assurance component.

4.8 Vulnerability assessment

4.8.1 AVA_SOF.1 – Strength of TOE security functions

139 The evaluation team examined the following evidence [LSS_ST], [LSS_HLD], [LSS_FSP], [LSS_IGSG], and [LSS_AG]. The [LSS_ST] states that the minimum SOF level of SOF-basic shall apply to the FIA_UAU.1.SFR. [LSS_FSP] provides the SOF analysis that the probability of guessing a password with the correct security policy set for the administrator account is 8.7919 x 10-9. This figure satisfies the metric for the probability that authentication data can be guessed is no greater than one in a million, which is the stated requirement in the [LSS_ST]. The evaluator analyzed the [LSS_ST], [LSS_HLD], and [LSS_FSP] documents to search for security mechanisms that are either probabilistic or permutational. It was determined that the identification and authentication mechanism used by the administrator to authenticated to the SMS is the only security mechanism within testing scope that has these properties.

AVA_SOF.1 Verdict: The evaluation team concluded that the TOE has met the assurance requirements of AVA_SOF.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.9 Penetration testing results

4.9.1 AVA_VLA.1 – Vulnerability analysis

140 The evaluation team examined the following evidence [LSS_ST], [LSS_VLA], [LSS_HLD], and [LSS_FSP], and the test results in [LSS_IND] of the evaluator tests conducted as part of completing ATE_IND independent testing. The evaluators determined that vulnerability analysis performed by the vendor did consider relevant information (e.g., CERT advisories) to search for obvious vulnerabilities. The vendor's analysis identified vulnerabilities and provided rationale

for each vulnerability that described why the vulnerability was not exploitable in the intended environment for the TOE. The arguments provided are consistent with TOE description in the ST and guidance for administering the system.

141 ***Penetration Testing Details***

142 The evaluation team produced [LSS_VLA_TR], which describes the penetration tests conducted by the evaluation team. The test configuration used was the exact same configuration used for independent testing (ATE_IND.2). The penetration testing of the WatchGuard was broken down into the following areas:

- Testing for the existence of vulnerabilities identified in the vendor's vulnerability analysis, the [LSS_VLA] document.
- Testing for additional vulnerabilities that may be relevant to the TOE. These vulnerabilities were identified by searching vulnerability advisories and databases at various web sites.

143 The evaluation team used protocol analyzers and CSC's proprietary Hydra Security Toolset to perform the penetration tests. These tests covered the following: IP spoofing, UDP attacks, ICMP Malformed Service Request vulnerability, IP Loose Source Routing Option vulnerability, fragmentation attacks, and OS race conditions. The evaluation team successfully completed the vulnerability tests and found the TOE to operate as expected. The TOE was not exploitable in the evaluated configuration.

144 ***Evaluation Observation:*** In the initial LSS_VLA_IPS_003 Spoofing test, it appeared that the TOE ended up in an endless loop denying the packet from the 30.2.2.10 interface (optional) to the 20.2.2.10 interface on port 1030 without logging the event. The developer could not reproduce the problem when provided the Firebox II configuration file, test script, and test executable (hping) by the evaluator. The developer concluded that the deficiency was in the Control Center GUI software and that it had no security impact. Because the developer could not reproduce the test results, the CCEL lab continued to test the deficiency. During the last testing period with only the SMTP proxy configured, the error did not manifest itself and the error was not repeatable. Viewing the symptom of the problem on the Firebox II monitor during the period that this test failed, the scrolling of the last packet received indicated that that packet was in an internal loop within the Firebox II. The looping stopped when another log event was introduced into the system (e.g., a denied ping (ICMP) packet). Because the TOE continued to function during the looping event, this indicated that the error had no collateral effect on the security functional processing of the TOE. The evaluator assigned the verdict for this test as PASS since the TOE exhibited good behavior with respect to the security functional processing during and subsequent to the looping event, and because it was not reproduceable-on-demand by the developer and subsequently the CCEL Lab.

145 ***AVA_VLA.1 Verdict:***

146 The evaluation team concluded that the TOE has met the assurance requirements of AVA_VLA.1. Therefore, a **pass** verdict has been issued for this assurance component.

5 CONCLUSIONS AND RECOMMENDATIONS

147 The TOE was evaluated against the [LSS_ST]. The assurance component verdicts presented in Chapter 4 of this report received final evaluation verdicts of **Pass**. Therefore, the evaluation team assigns an overall Pass verdict for satisfying the evaluator action elements defined for EAL 2. As defined by [CC_PART1] Chapter 5, the TOE was found to be Part 2 conformant, and Part 3 conformant. The evaluation team recommends that an EAL 2 certificate rating be issued for the TOE.

6 LIST OF EVALUATION DELIVERABLES

148 Table 7 provides a listing of evidence supplied as evaluation deliverables.

Table 7: Evaluation Deliverables

Identifier	Date of Receipt	Issuing Body	Title
[Firebox II]	8/16/99	WatchGuard Technologies	Firebox II
[LSS_1.0_REVA]	8/16/99	WatchGuard Technologies	WatchGuard LiveSecurity Version 1.0 REVA
[LSS_SW_CD]	3/14/00	WatchGuard Technologies	WatchGuard LiveSecurity System Install Guide, LiveSecurity System 4.1
[LSS_IGSG]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Installation, Generation, and Startup Guide, Version 1.3, July31, 2000
[LSS_DEL]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Delivery Procedures for Evaluated Version of WatchGuard LiveSecurity System with Firebox II, version 0.6, WPG-001, March 15, 2000
[LSS_ST]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Security Target, Version 1.3, August 3, 2000
[LSS_FSP]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Functional Specification, Version 1.5, August 7, 2000
[LSS_HLD]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, High-level Design, Version 1.9, August 2, 2000
[LSS_RCR]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Correspondence Spreadsheet, Version 1.3, August 2, 2000
[LSS_CM]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1. Convifguration Management, Version 1.0, August 3, 2000
[LSS_UG_4.1]	3/13/00	WatchGuard Technologies	WatchGuard LiveSecurity 4.1 System User Guide
[LSS_BSSPA0]	5/24/00	WatchGuard Technologies	Test Plan: Basic Service Setup Procedure A0
LSS_CCFBMA1	5/24/00	WatchGuard Technologies	Test Plan: Control Center – Firebox Monitor A1

Identifier	Date of Receipt	Issuing Body	Title
[LSS_CCHRA2]	5/24/00	WatchGuard Technologies	Test Plan: Control Center – Historical Reports A2
[LSS_CCHWA3]	5/24/00	WatchGuard Technologies	Test Plan: Control Center – Host Watch A3
[LSS_CCLVA4]	5/24/00	WatchGuard Technologies	Test Plan: Control Center – Log Vierwer A4
[LSS_CCPMA5	5/24/00	WatchGuard Technologies	Test Plan: Control Center – Policy Manager A5
[LSS_TCPHA6]	5/24/00	WatchGuard Technologies	Test Plan: Transmission Control Protocol (TCP) Handling A6
[LSS_ICMPHA7]	5/24/00	WatchGuard Technologies	Test Plan Internet Control Message Protocol (ICMP) Handling A7
[LSS_FTPHA8]	5/24/00	WatchGuard Technologies	Test Plan: Filte Transfer Protocol (FTP) Handling A8
[LSS_TCA_1.0]	5/24/00	WatchGuard Technologies	WatchGuard Technologies WatchGuard LiveSecurity system with Firebox II 4.1 Test coverage Analysis, Version 1.0, May 18, 2000
[LSS_VLA]		WatchGuard Technologies	WatchGuard Technologies, WatchGuard Live Security System with Firebox II, 4.1, Vulnerability Assessment, Version 1.4, August 2, 2000
[LSS_RELNOTES]		WatchGuard Technologies	WatchGuard LiveSecurity System, Version 4.1 Release Notes
[LSS_BSP]	12/16/99	WatchGuard Technologies	Build System Proposal ("build system proposal.doc")
[LSS_BLD]	12/16/99	WatchGuard Technologies	Build Instructions ("build_instructions.doc")
[LSS_QTP]	12/16/99	WatchGuard Technologies	QA Test Plan ("Humtulips Test Plan.doc")
[LSS_CM_LCL]	12/16/99	WatchGuard Technologies	CM Specs for Windows Build Machine/CM Support for Localization ("localization.doc)
[LSS_RELFRM]	12/16/99	WatchGuard Technologies	WatchGuard Release Form ("release form.xls")
[LSS_VSS]	12/16/99	WatchGuard Technologies	Running Analyze in VSS ("vss.doc")
[LSS_LOCAL]	12/16/99	WatchGuard Technologies	Localization ("localization.vsd")
[LSS_BUGFLW]	12/16/99	WatchGuard Technologies	Bug Flow ("bug flow.vsd")
[LSS_PRCS]	12/16/99	WatchGuard Technologies	"process_a.vsd"
[LSS_RLS]	12/16/99	WatchGuard Technologies	"release.vsd"
[LSS_AUTH_TP]	10/12/99	WatchGuard	Authentication Test Plan

Identifier	Date of Receipt	Issuing Body	Title
		Technologies	("authentication.doc")
[LSS_CTP]	12/16/99	WatchGuard Technologies	Controld Test Plan ("controld.doc")
[LSS_FLTP]	12/16/99	WatchGuard Technologies	FB LINT Test Plan ("fb lint.doc")
[LSS_HWTP]	12/16/99	WatchGuard Technologies	Host Watch Test Plan ("host_watch.doc")
[LSS_ITP]	12/16/99	WatchGuard Technologies	Installation Test Plan ("installation.doc")
[LSS_NTP]	12/16/99	WatchGuard Technologies	Notification Test Plan ("notification.doc")
[LSS_PMTP]	12/16/99	WatchGuard Technologies	Policy Manager Test Plan ("policy_manager.doc")
[LSS_REP_CMD]	12/16/99	WatchGuard Technologies	REP_CMD Test Plan ("rep_cmd.doc").
[LSS_SWTP]	12/16/99	WatchGuard Technologies	Service Watch Test Plan ("Service_Watch.doc")
[LSS_WMTP]	12/16/99	WatchGuard Technologies	WatchGuard Monitors Test Plan ("wg_monitor.doc")
[LSS_41QA]	3/14/00	WatchGuard Technologies	LSS_41 QA Docs
[LSS_WCC_GUI_TP]	4/27/00	WatchGuard Technologies	WatchGuard Control Center GUI Interface Firebox Monitors Test Plan

7 LIST OF ACRONYMS

149 The following acronyms are used throughout this document.

ARP	Address Resolution Protocol
CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CEM	Common Evaluation Methodology
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
FER	Final Evaluation Report
IP	Internet Protocol
LAN	Local Area Network
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions

8 PROBLEM REPORTS

8.1 Evaluation Discovery Reports

This section of contains all EDRs raised as a result of work performed during the evaluation. Table 8 provides the EDRs unique identifier, the work package in which the problem was discovered, a brief summary of the problem, and their status.

Table 8: WatchGuard EDRs

File Name (EDR Number)	Date Created	Severity	EDR Title	Status of EDRs
LSS_EDR_001	05/12/00	Urgent	Configuration Management Discoveries - Configuration List Not Provided	Resolved
LSS_EDR_002	05/18/00 & 07/11/00	Urgent	Security Target Evaluation Discoveries	Resolved
LSS_EDR_003	06/15/00	Urgent	HLD Initial Review Issues	Resolved
LSS_EDR_004	07/22/00	Urgent	AGD Clarification	Resolved
LSS_EDR_005	7/26/00	Urgent	ADV_FSP Discoveries	Resolved
LSS_EDR_006	07/20/00	Moderate	Vulnerability Analysis (AVA) Discoveries	Resolved
LSS_EDR_007	7/25/00	Urgent	ADV_FSP - SOF	Resolved
LSS_EDR_008	07/25/00	Moderate	Strength of Function Analysis (AVA_SOF.1) Discoveries	Resolved
LSS_EDR_009	07/25/00	Urgent	Vulnerability Analysis Discoveries	Resolved
LSS_EDR_010	7/26/00	Urgent	IGSG Clarification	Resolved
LSS_EDR_011	7/26/00	Urgent	ST – RCR Conflicts	Resolved
LSS_EDR_012	7/26/00	Urgent	RCR Deficiency	Resolved
LSS_EDR_013	7/26/00	Urgent	FSP RCR Discoveries	Resolved
LSS-EDR_014	7/28/00	Urgent	ATE_FUN Deficiency	Resolved
LSS_EDR_015	7/28/00	Urgent	ATE IND.2: Test Configuration	Resolved
LSS-EDR_016	8/4/00	Urgent	ST – TSS SOF Claims	Resolved
LSS-EDR_017	8/7/00	Urgent	AVA_VLA – Failure to Log Spoofing	Resolved

8.2 Observation Reports

151 No Observation Reports were generated during the EAL 2 evaluation of the WatchGuard LiveSecurity System with FireBox II 4.1.