Trust Technology Assessment Program

Evaluation Technical Report
For

Check Point Software Technologies Ltd
FireWall-1 Version 4.0

Prepared by:

Computer Sciences Corporation
7471 Candlewood Road
Hanover, MD 21076

Submitted to:
TTap Oversight board

Version 1.1
October 1999

FOREWORD

This publication, the Check Point FireWall-1 Version 4.0, 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 an Evaluation Assurance Level (EAL) 2 certification rating for the Check Point FireWall-1 Version 4.0 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 Target of Evaluation (TOE) security requirements referred to in this report are taken from the *Check Point Software Technologies Ltd. FireWall-1 Version 4.0 Security Target.* The activities performed by the evaluation team to conduct the evaluation were taken from the *Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 0.6* and the *Common Criteria for Information Technology Security Evaluation, Version 2.0.*

TABLE OF CONTENTS

LIST OF TABLES

CHECK POINT SOFTWARE TECHNOLOGIES LTD
FIREWALL-1 VERSION 4.0
EVALUATION TECHNICAL REPORT

1 INTRODUCTION

1.1 Identification

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 Scheme	United States Trust Technology Assessment Program
Evaluation Technical Report	Check Point Software Technologies Ltd FireWall-1 Version 4.0 Evaluation Technical Report, October 1999, Version 1.1
Security Target	Check Point Software Technologies Ltd FireWall-1 Version 4.0 Security Target, Version 2.4
Protection Profile(1)	U.S. Government Application-level Firewall Protection Profile for Low-Risk Environments, Version 1.d, Draft, September 1999
Protection Profile(2)	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999
Target of Evaluation	Check Point FireWall-1 Version 4.0 SP5 executing on Microsoft Windows NT 4.0 Service Pack 4
EAL	2
Developer	Check Point Software Technologies
Sponsor	Check Point Software Technologies
Evaluators	Computer Sciences Corporation Kimberly Caplan H. Patrick Dunn, CISSP Kim Jones, CISSP Carl Souba Vince Ritts Government Participants Traci Harrell William Noland Rob Preston
Certifers	Ken Elliott Kathy Dolan

1.2 Background

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.

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 be added to NSA's Evaluated Products List.

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). In anticipation of the final version of the CEM and its application, the TTAP Oversight Board has requested all TEFs to use the CEM when conducting CC evaluations, as appropriate.

1.3 References

The following documents are referenced throughout this report.

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, May 1998, version 2.0.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, May 1998, version 2.0.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, May 1998, version 2.0.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, May 1998, version 2.0.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, 1 November 1998, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, January 1999, version 0.6

[ALF_PP] U.S. Government Application-level Firewall Protection Profile for Low-Risk Environments, Version 1.d, Draft, September 1999

[TFF_PP] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999

[FW1_ST] Check Point Software Technologies Ltd FireWall-1 Version 4.0 Security Target, Version 2.4

1.4 Document Organization

This report was written using [CEM_PART2] as a guide and is divided into the following Chapters:

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

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

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;

Chapter 4 Results of the Evaluation, provides a verdict and supporting rationale for each evaluator action element completed for the evaluation;

Chapter 5, Conclusions and Recommendations;

Chapter 6, Acronyms and Glossary; and

Chapter 7, Problem Reports, lists the Evaluation Discovery Reports (EDRs) and Observation Reports (ORs) that were raised during the evaluation and their status.

2 ARCHITECTURAL DESCRIPTION

2.1 TOE Identification

The Check Point FireWall-1 Version 4.0 for Windows NT 4.0, referred to as the Target of Evaluation (TOE) consists of the hardware and software components described in Table 2.

Table 2: FireWall-1 Software/Hardware Components

Components	Items
Software	Check Point FireWall-1 Version 4.0 SP5 for Windows NT 4.0
	Check Point FireWall-1 GUI Version 4.0 SP5 for Windows NT 4.0
	Microsoft Windows NT Server 4.0 (service pack 4)
Hardware	Intel x86 - Pentium Processor (minimum)
	16 Mbytes (minimum)
	3COM EtherLink III 3C509TB 3COM Fast EtherLink XL NIC 3c905B-TX
	At least 20 Mbytes hard drive space
	Backup device

2.2 Evaluated Configuration

The evaluated configuration of the TOE consists of one (1) Check Point FireWall-1 Version 4.0 for Windows NT 4.0, which controls the flow of traffic between network elements and provides administrative interfaces for managing the FireWall-1 firewall.

The TOE provides two network interfaces. The console port on the TOE is used to provide system administration. Figure 1 illustrates this evaluated configuration. By default, all internal (protected) and external (unprotected) hosts are blocked from initiating connections or sessions.

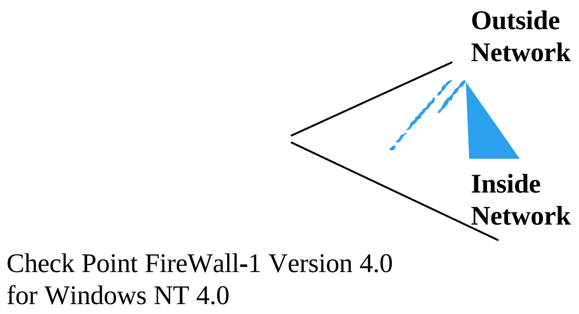

Figure 1: Evaluated Configuration

The evaluated configuration was limited to the software components that make up the TOE Security Function (TSF) interfaces and the TSF architecture in satisfaction of the functional requirements specified in [FW1_ST]. Software and hardware features outside the scope of the defined TSF and thus not evaluated are:

- Client Authentication;
- Session Authentication;

- Account Management (LDAP use);
- Interaction with OPSEC Products;
- Content filtering;
- Network Address Translation;
- Remote Administration;
- FireWall-1 Virtual Private Networking; and
- Windows NT 4.0 features not used by the TOE.

The software and hardware features outside the scope of the evaluation are not enabled or used by the TOE. If these features are enabled then no statement regarding the satisfaction of security requirements can be made or assumed.

2.3 System Overview

The TOE forms the boundary between an internal protected network and an external unprotected network. The TOE is physically protected such that the TOE is located within controlled access facilities that mitigate unauthorized, physical access. All traffic between the internal and external networks must flow through the TOE to maintain security. The external network may be accessible to the Internet and may contain systems that provide services such as HTTP, FTP, SMTP (electronic mail), and Telnet.

The TOE selectively routes information among internal and external networks according to rules established by an authorized administrator. The authorized administrator administers FireWall-1 from the system console. Remote administration (telnet from the external or internal networks) to the TOE is prohibited in the evaluated configuration. The default configuration of the TOE prohibits all connections between networks. After the authorized administrator has configured information flow rules, the TOE limits connections between networks to only those which are authorized.

2.3.1 Physical Scope and Boundary

The TOE configuration consists of one physical component executing:

- One FireWall Module, that implements the Security Policy, logs events, and communicates with the Management Module
- One Management Module which manages the FireWall-1 database: the Rule Base, network objects, services, users, etc.
- The Windows NT Server 4.0 operating system with service pack 4 installed
- Two network interfaces with one designated as internal and the other as external.

2.3.2 Logical Scope and Boundary

The TOE provides the following security features:

- **Security Audit:** Audit data generation, is implemented by the FireWall-1 and the NT operating system. The NT Auditing subsystem records events pertaining to accessing the Management Module. FireWall-1 provides logging for all activities pertaining to the actions to or through the product. Audit review of the NT log files is accomplished via the Event Viewer application. The Event Viewer is an application that forms a part of the NT Utilities subsystem and it permits the administrator to view, search and sort the audit files on all required parameters. Audit Review on FireWall-1 is accomplished via the graphic user interface (GUI) of the Management Server. The GUI interface permits the administrator to view, search and sort the audit files on all required parameters excluding range of addresses. Only authorized administrators are able to login to the firewall host and, subsequently, access the audit files. The audit trail is protected by the NT Access Control subsystem.

- **User Data Protection:** The FireWall-1 FTP and Telnet Security Servers (proxies) provide authentication and protection from malformed service requests. Additionally, the HTTP and SMTP Security Servers provide unauthenticated application level protection. The FireWall Module ensures that information contained in packets from previous sessions is no longer accessible once the session has been completed. The management of the storage and processing of data packets through the TOE ensures that no residual information is transferred to future sessions through the TOE. The Kernel Virtual Machine carries out the inspection process itself. Here the rules of the Security Policy in their compiled form are applied. INSPECT is a procedure that terminates in a decision on an action to take for the packet: *accept, reject, drop*. The INSPECT engine is a large switch that uses virtual machine language (INSPECT ML code) to carry out the operations of the Security Policy files. Its temporary data is maintained in a large stack.

- **Identification and Authentication**: The TOE provides user authentication and enables the authorized administrator to define a Security Policy on a per-user basis. Windows NT 4.0 Utilities and Authentication subsystems provide the ability to associate human users with specific identities (userid and password). The NT Authentication subsystem maintains an *administrator* users group with unique access and privileges to records, programs, and functions on the Management Module. FireWall-1 Security Server utilizes SKEY to initiate an authentication procedure. The FireWall-1 Security Servers start a secured interactive session on the target host. The interactive session's packets are inspected by the FireWall Module as they enter the gateway, passed up to the Security Server at the application layer, and then passed down again to the FireWall Module to be inspected once again before they continue on to the target host. The Security Servers also provide an authentication failure handling mechanism that locks individual accounts when a defined number of unsuccessful authentication attempts have been made. The NT User Management application allows the administrator to set an authentication policy, which is enforced, for all administration accounts on the TOE.

- **Security Management:** The Management Module maintains all security attributes for FireWall-1 authorized administrators. Additionally, Windows NT 4.0 Utilities and Authentication subsystems maintain security attributes for authorized administrators. Security procedures ensure that only authorized administrators can access the FireWall-1 Management Module.

- **Protection of Security Functions:** The interface to the network interface is provided through the FireWall-1 Kernel subsystem It assures that the only means to enter the TCP/IP of the gateway is via the Kernel Attachment, thus securing the domain.

2.4 TOE Subsystems

Table 3 below summaries the functionality of the TOE subsystems. Subsequent subsections provide a more complete description of subsystem functionality, internal interfaces, and externally visible interfaces.

Table 3: TOE Subsystems

Subsystem Name	Functionality
FireWall-1 Graphical User Interface	Provides the authorized administrator with a GUI to manage the FireWall-1 product
FireWall-1 Management	Manages the information flows to and from FireWall-1 machines in a distributed configuration
FireWall-1 Kernel	Enforces of the Security Policy through stateful packet inspection and anti-spoofing capabilities; and provides protocol interface to users
FireWall-1 Daemon	Performs computationally difficult tasks on behalf of the Kernel subsystem
FireWall-1 Utilities	Processes and compiles the Security Policy and provides the authorized administrator with a command line interface to manage the FireWall-1 product
FireWall-1 Security Server	Enforces the Security Policy through enforcement of user authentication and protocol command mediation
NT Authentication	Provides a trusted path between the user and the FireWall-1 product
NT Access Control	Generates and enforces access control decisions on administrator login on NT system console
NT Audit	Records NT system, security, and application audit events to log files
NT Utilities	Provides GUI and command line interface to authorized administrator interface to manage NT services

Figure 2 below identifies the relationship between each subsystem and the function it plays within the TOE.

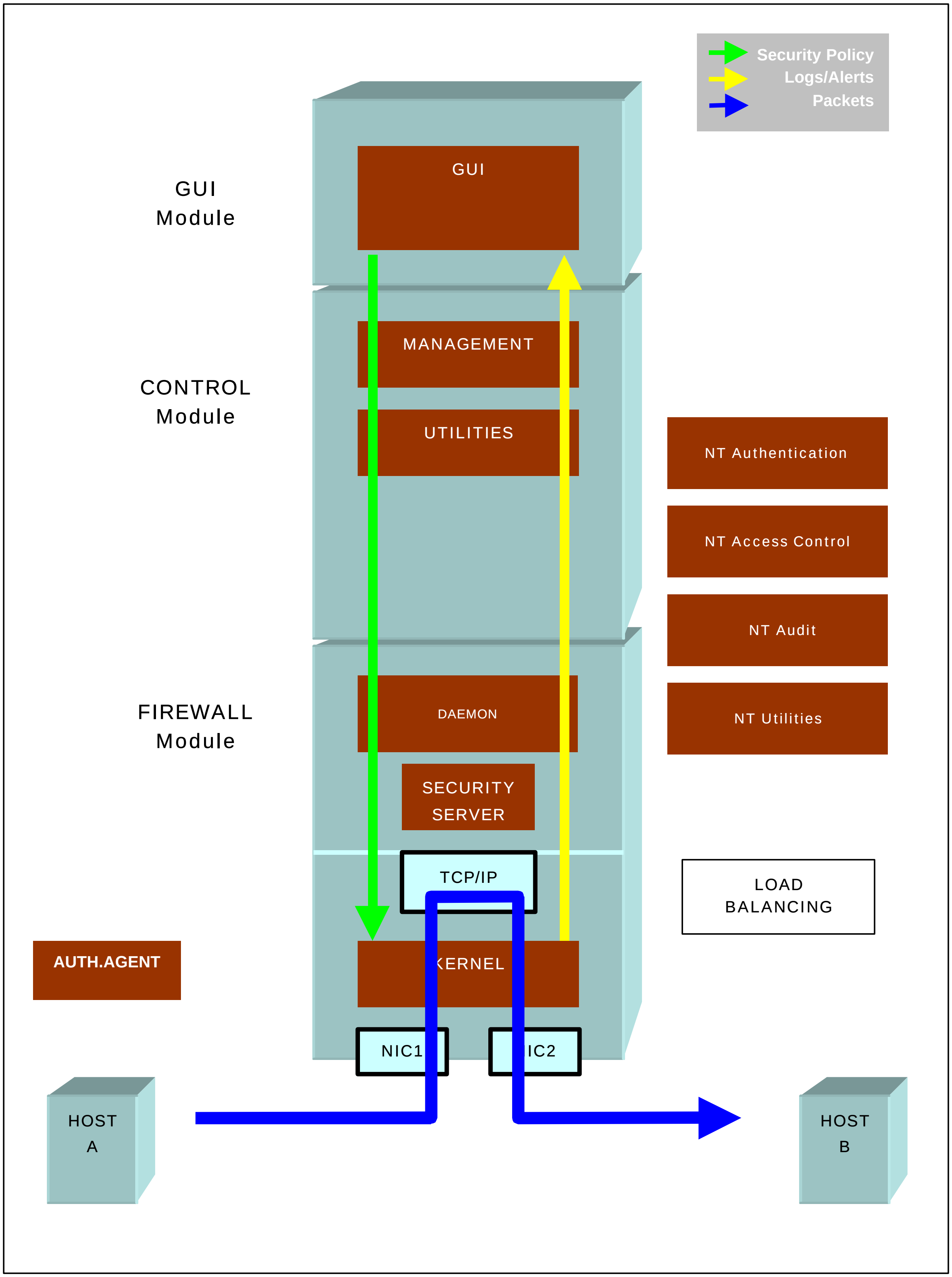

Figure 2: FireWall-1 Subsystems and Modules

2.4.1 FireWall-1 Graphical User Interface

The Firewall-1 Graphical User Interface (GUI) subsystem provides and externally visible user interface that is engaged by the user for Security Policy entry, and for viewing log files and receiving graphical alerts. Table 4 below identifies the FireWall-1 GUI interface windows and provides a description of the management functions provided by each window.

Table 4: FireWall-1 GUI Interface Window Descriptions

FireWall-1 GUI Windows	Description
Network Objects Manager	The Network Objects Manager window allows you to manages properties of network objects, including hosts, gateways, routers, networks, switches. Logical Servers and domains.
Users Manager	The Users Manager window allows you to manage user and group properties.
Services Manager	The Services Manager window allows you to manage services that control access to a host, not only based on source and destination of each communication, but also according to the service request. Services include those based on TCP, UDP, RPC and other protocols.
Resources Manager	The Resources Manager window allows you to manage server objects. Server objects include URL filtering (UFP), Content Vectoring Protocol (CVP), RADIUS, TACACS, AXENT Defender, and LDAP Account Units
Servers Manager	The Servers Manager window allows you to enable Content Security on FireWall-1 Resource objects. FireWall-1 provides content security for HTTP, FTP, and SMTP connection using FireWall-1 Security Servers.
System Status	The System Status window presents a high-level view of the operation and flow statistics for all FireWall-1 objects.
Log Viewer	The Log Viewer allows you to view entries in the Log File.
Properties Setup	The Properties Setup window allows you to manage properties. A security policy is defined not only by the Rule Base, but also by the properties specified.

The FireWall-1 GUI subsystem also interfaces with the Management and Utilities subsystems.

2.4.2 FireWall-1 Management

The Firewall-1 Management subsystem receives instructions from the FireWall-1 GUI subsystem, stores them on the local hard drive and distributes these to other FireWall-1 subsystems. The Firewall-1 Management subsystem also receives files and processes logs/alerts from the Kernel(s). The FireWall-1 Management subsystem interfaces with the GUI, Daemon, and Security Server subsystems.

2.4.3 FireWall-1 Kernel

TheFirewall-1 Kernel subsystem is the main packet filtering/transforming subsystem, located within the OS kernel that, intercepts packet flows between Network Interface Cards (NIC)s and the NT Internet Protocol (IP) module. The Kernel subsystem is installed during booting of FireWall-1 and cannot be bypassed. The FireWall-1 Kernel subsystem enforces the security policy by denying all information flows between internal and external networks until a less restrictive security policy is installed by an authorized administrator. The Kernel subsystem can enforce any security policy installed by the authorized administrator that is based on the presumed address of source, presumed address of destination, transport layer protocol, TOE interface packet arrivals and departs, and all services except FTP, TELNET, HTTP, and SMTP. The FireWall-1 subsystem and security policy rule sets provide FireWall-1 with an ALFPP compliant anti-spoofing capability. The FireWall-1 Kernel subsystem also interfaces with the Daemon, and Management subsystems.

2.4.4 FireWall-1 Daemon

The Firewall-1 Daemon subsystem, receives and installs the Security Policy on the Kernel, and processes logs, alerts, and traps generated by the Kernel; receives transmitted logs/alerts, writes the log file and issues alerts. The FireWall-1 Daemon subsystem does not have any externally visible subsystem interface. The FireWall-1 Daemon subsystem interfaces with the Kernel and Management subsystems.

2.4.5 FireWall-1 Utilities

The Firewall-1 Utilities subsystem resides on the Control module, and is involved in compiling and loading the Security Policy. It provides a command-line interface means of engaging Control module functionality. Table 5 below identifies the FireWall-1 Utilities command line interface commands and provides a description of the management functions provided by each command.

Table 5: Command Line Interface Commands

Command Area	Command	Description
Setup	fwconfig	Reconfigures an existing FireWall-1 installation
	fwinstall	Installs the FireWall-1 software from the files extracted from the distribution media
	fwstart	Loads the FireWall-1 FireWall Module, starts the FireWall-1 daemon (fwd), the FireWall-1 SNMP daemon (snmpd) and the authentication deamons, and starts fwm, the Management Server
	fwstop	Kills the FireWall-1 FireWall daemon (fwd) and the Management Server (fwm), the FireWall-1 SNMP daemon (snmpd) and the authentication daemons and unloads the FireWall Module
	fw	Program used to manage the system
Control	fw load	Compiles and install the Security Policy to the target's Firewall Modules
	fw unload	Uninstalls the currently loaded Inspection Code from the selected targets
	fw fetch	Fetches the Inspection Code that was lasted installed on the local host
	fw logswitch	Creates a new Log File
	fw putkey	Installs a FireWall-1 authentication password on a host, thus enabling control connections between the hosts on which the fw putkey command is run and a second host.
	fw putlic	Installs the FireWall-1 license on a host.
Monitor	fw stat	Displays the status of target hosts in various formats.
	fw lichosts	Prints a list of hosts protected by the FireWall-1/n products.
	fw log	Displays the current log files.
	fw logexport	Exports the log file to an ASCII file.
	fw ver	Displays the FireWall-1 version number.
	fw printlic	Prints details of the FireWall-1 license.
	fw sam	Inhibits (blocks) connections to and from specific IP addresses without the need to change the Security Policy.

Command Area	Command	Description
Utilities	fwiscolod	Downloads a security policy to a cisco router
	fw ctl	Sends control information to the Firewall-1 Kernel Module
	fw gen	Generates an Inspection Script file from a Rule Base.
	fw kill	Sends a signal to a Firewall-1 daemon
	fwc	Is the Firewall-1 INSPECT language compiler.
	fwm	Is the Firewall-1 Management Server in the Client/Server implementation of the Management Module, and is used for communicating with the GUI and adding, updating and removing administrators.
	fwell	Manages Access Lists for Wellfleet (Bay Network) routers.
	fw tab	Displays the content of the INSPECT tables on the target hosts in various formats.
	fwxlcomf	Is the Firewall-1 address translation configuration utility.
	snmp_trap	Sends an SNMP trap to the specified host.
	status_alert	Generates an alert.
	fw converthosts	Converts a file in the /etc/hosts format to a file in the dnsinfo.C format.
User Database – Importing and Exporting	fw ddimport	To import users into the FireWall-1 User database from an external source.
	fw dbexport	To export the FireWall-1 user database file to an external source.

The FireWall-1 Utilities subsystem also interfaces with Management, Kernel, and GUI subsystems.

2.4.6 FireWall-1 Security Server

The FireWall-1 Security Server subsystem enforces the security policy on user authentication attempts, protocol commands, and malformed service requests. The FireWall-1 Security Server subsystem provides an externally visible user interface through TELNET, SMTP, FTP, and HTTP protocols. The FireWall-1 Security Server subsystem also interfaces with the Kernel and Management subsystems.

2.4.7 NT Authentication

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. When a user enters the SAS a logon dialogue box appears and a process is started to capture untrusted processes. The secure logon process follows the SAS. The NT Authentication subsystem has an external user interface to the NT GUI Subsystem; NT Logon. The user is required to enter a SAS via the keyboard to initiate the authentication process. In addition, the user is prompted via a dialogue box to enter both a username and password for validation. The NT Authentication subsystem also interfaces with the NT Access Control, NT Utilities, and NT Audit subsystems.

2.4.8 NT Access Control

The Access Control subsystem determines user privileges or access rights (based upon user account SID and group account SID) and enforces those access rights to determine whether a process or thread can obtain requested access to a securable object. The NT Access Control subsystem interfaces with the NT Authentication and NT Audit subsystems.

2.4.9 NT Audit

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.* The NT Audit subsystem contains a users visible interface through the NT GUI Interface: NT Event View for viewing and managing NT log data. The NT Audit subsystem also contains interfaces with the NT Authentication, NT Utilities, and NT Access Control subsystems.

2.4.10 NT Utilities

The NT System Utilities subsystem provides the system administrator with a number of tools for configuring the NT system and providing supporting security functionality for the TOE. Table 6 identifies the externally visible NT Utilities interfaces.

Table 6: NT Utilities Externally Visible Interfaces

Interface	Module
NT GUI	NT User Manager for Domains
NT Command Line	Date/Time
NT GUI	NT Date and Time
NT GUI	NT Backup
NT GUI	NT Event Viewer

The NT Utilities subsystem also has interfaces to NT Authentication and NT Audit.

3 EVALUATION

3.1 Evaluation Methods, Techniques, and Standards

The *evaluator action elements* documented in [CC_PART3] for EAL2 assurance components was 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.

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 7.

Table 7: 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

For the ATE_IND.1.2E 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 coordinated with the PP author to identify the current list of obvious vulnerabilities. The team wrote a test plan for penetration testing and conducted tests in accordance with the plan.

Throughout the evaluation, the evaluation team generated Observation Reports (ORs) to request clarification on the [ALF_PP] or Common Criteria requirements. ORs were submitted to the Certifier for posting and resolution. 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.

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 ORs and EDRs that were generated during the evaluation.

3.2 Evaluation Tools

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 layers for residual information; and
- to manipulate network and application layer flows to simulate various attack scenarios.

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

The ST is based on the Security Functional Requirements (SFRs) of the [ALF_PP] and the [TFF_PP]. The [ALF_PP] is a draft PP and during the evaluation several flaws in the PP were identified and documented in ORs. The problems with the [ALF_PP] directly impacted the evaluation of the ST because the ST was claiming conformance to [ALF_PP]. Not all the ORs resulted in immediate changes to [ALF_PP]. To assign a Pass verdict for the ST evaluation, the Developer had to make adjustments to the SFRs in the ST and provide supporting rationale in order to claim conformance to [ALF_PP].

3.4 Evaluation Deliverables

Table 8 provides a listing of evidence supplied as evaluation deliverables.

Table 8: Evaluation Deliverables

Identifier	Date of Receipt	Issuing Body	Title
[FW1_AGD_001]	1-5-1999	Developer	Managing FireWall-1 Using the Windows GUI User Guide ,Version 4.0.
[FW1_AGD_002]	1-5-1999	Developer	Getting Started with FireWall-1 User Guide, Version 4.0.
[FW1_AGD_003]	1-5-1999	Developer	Architecture and Administration User Guide, Version 4.0.
[FW1_AGD_004]	1-5-1999	Developer	FW-1 User Guidance, Version 1.1.
[FW1_AGD_005]	1-5-1999	Developer	Managing FireWall-1 Using the OpenLook GUI User Guide ,Version 4.0.
[FW1_CM]	10-11-1999	Developer	FW-1 Configuration Management, Version 1.2.
[FW1_DEL]	8-17-1999	Developer	FW-1 Secure Delivery, Version 1.3.
[FW1_FSP]	9-14-1999	Developer	Check Point Technologies FireWall-1 Version 4.0 Functional Specification, Version 4.9.

[FW1_HLD]	9-20-1999	Developer	Check Point Firewall-1, High-level Design, Version 3.7, Draft.
[FW1_IGS]	9-16-1999	Developer	FW-1 Installation, Generation, and Start-up Guide, Version 1.12.
[FW1_RCR]	9-21-1999	Developer	FW-1 Informal Correspondence Demonstration, Version 1.6.
[FW1_SOF]	9-24-1999	Developer	FireWall-1 Version 4.0 Strength of Function Analysis, Check Point Technologies, Draft Version 1.1.
[FW1_ST]	10-12-1999	Developer	Check Point Software Technologies Ltd FireWall-1 Version 4.0 Security Target (V2.4).
[FW1_TST]	9-07-1999	Developer	Check Point FireWall-1 Functional Testing, Version 1.5.
[FW1_QSG]	1-5-99	Developer	FW-1 Quick Start Guide, Version 4.0
[FW1_VUL]	9-18-1999	Developer	FireWall-1 Version 4.0 Vulnerability Analysis, Check Point Technologies, Version 1.4.
[FW1_SOFT]	9-2-1999	Developer	Check Point FireWall-1, version 4.0, build 1458, Patch 3.

4 RESULTS OF THE EVALUATION

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.

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.

Table 9 provides a listing of the activities, associated assurance components, and evaluator action elements for a ST Evaluation and an EAL 2 Evaluation.

Table 9: 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, Implied Action
	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 Evaluation

The objective of the ST evaluation is to determine whether [FW1_ST] is complete, consistent, technically sound, and to determine that the [FW1_ST] provides a suitable baseline for evaluation of the TOE.

4.1.1 ASE_DES.1 – TOE Description

ASE_DES.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_DES.1 because the evaluator action elements ASE_DES.1.1E, ASE_DES.1.2E, and ASE_DES.1.3E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_DES.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_DES.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_DES.1.1E Rationale:

The evaluation team checked and examined the [FW1_ST]. The evaluator examined the evidence and determined that the TOE Description in Section 2 of [FW1_ST] describes the product and the scope and boundaries of the TOE, both in a physical and logical way. As a result, the evaluator determined that all requirements for this activity were satisfied.

ASE_DES.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_DES.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_DES.1.2E Rationale:

The TOE Description in [FW1_ST] was examined and found to provide a consistent description of the functionality provided by the TOE. Section 2.1 describes the FireWall-1 Architecture, which is comprised of the Management Module and the FireWall Module. Section 2.2.2 provides the security features of the TOE. For each security feature a brief overview is provided as to how the TOE addresses that feature. Section 2.3 provides further information. The information found in this section is consistent with the information found through out the TOE Description. As a result, the evaluator determined that all requirements for this activity were satisfied.

ASE_DES.1.3E Verdict:

The evaluation team successfully completed the evaluator action element ASE_DES.1.3E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_DES.1.3E Rationale:

In [FW1_ST], the chapters that contain descriptive material regarding the TOE are Chapter 1, “Security Target Introduction”, Chapter 2, “TOE Description” and Chapter 5, “TOE Summary

Specification”. The TOE Description gives a brief overview of the TOE’s features, while the TOE Summary Specification provides a high-level definition of these features. The evaluator determined that the TOE Description was consistent with other parts of the ST. As a result, the evaluator determined that all requirements for this activity were satisfied.

4.1.2 ASE_ENV.1 – Security Environment

ASE_ENV.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_ENV.1 because the evaluator action elements ASE_ENV.1.1E and ASE_ENV.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_ENV.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_ENV.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_ENV.1.1E Rationale:

The evaluation team checked and examined the [FW1_ST], [ALF_PP], and [TFF_PP]. . The evaluator examined the evidence and determined that the security environment explains all assumptions and threats. Because the ST was claiming conformance to the [ALF_PP] and [TFF_PP], the evaluator checked that the assumptions, threats, and organizational security policies were used from the protection profiles. The evaluator examined the evidence and found that all identified threats are clearly explained in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. The evaluator examined the evidence and found that because of the TOE definition, there were no organizational security policies. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

ASE_ENV.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_ENV.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_ENV.1.2E Rationale:

The evaluator examined the [FW1_ST] and determined that the TOE security environment was coherent and internally consistent. The evaluator examined the evidence and determined that the TOE security environment was consistent with the ST introduction and the description of the TOE. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

4.1.3 ASE_INT.1 – ST Introduction

ASE_INT.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_INT.1 because the evaluator action elements ASE_INT.1.1E, ASE_INT.1.2E, and ASE_INT.1.3E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_INT.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_INT.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_INT.1.1E Rationale:

The evaluation team checked the [FW1_ST]. The evaluator checked the evidence and found that the ST introduction contains a ST identification information, a ST overview and a CC conformance claim.

ASE_INT.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_INT.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_INT.1.2E Rationale:

The evaluation team examined the ST introduction and determined that it is coherent and internally consistent. The ST introduction did not contain any ambiguous or potentially misleading statements.

ASE_INT.1.3E Verdict:

The evaluation team successfully completed the evaluator action element ASE_INT.1.3E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_INT.1.3E Rationale:

The evaluation team checked and examined the [FW1_ST]. The ST Introduction was examined and found to be consistent the rest of the [FW1_ST]. The Common Criteria Conformance Claims are consistent with those found in the PP Claims. The Security Target Overview is consistent with the TOE Description and TOE Summary Specification. The Conventions described are consistent with those used in the TOE Security Requirements. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.1.4 ASE_OBJ.1 – Security Objectives

ASE_OBJ.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_OBJ.1 because the evaluator action elements ASE_OBJ.1.1E and ASE_OBJ.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_OBJ.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_OBJ.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_OBJ.1.1E Rationale:

The evaluation team checked and examined the [FW1_ST], [ALF_PP], and [TFF_PP]. The evaluator examined the evidence and found that it defines the security objectives for the TOE and the security objectives for the environment. The evaluator examined the evidence and found that the security objectives are clearly stated. The evaluator examined the evidence and found that each security objective for the TOE traces back to an identified threat and that each security objective for the environment traces back to an assumption. Because the ST was claiming conformance to the [ALF_PP] and [TFF_PP], the evaluator checked that the security objectives from the protection profiles were referenced or transcribed into the ST. The evaluator examined the evidence and determined that the security objectives rationale identified threats to security and that the security objectives were suitable to counter those threats. The evaluator examined the evidence and determined that the security objectives rationale identifies assumptions and that the security objectives for the environment were suitable to cover those assumptions. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ASE_OBJ.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_OBJ.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_OBJ.1.2E Rationale:

The evaluation team examined [FW1_ST] and found the security objectives to be complete, coherent, and internally consistent. Each security objective, for both the TOE and the environment, is stated so that a mapping between assumptions and threats is possible. At least one security objective maps to at least one threat or assumption. All identified assumptions and threats are satisfied without contradiction. In the security objective rationale section, security objectives for both IT and non-IT are explained, so that a clear mapping is shown, along with a statement of how the objective counters the associated threat. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.1.5 ASE_PPC.1 – PP Claims

ASE_PPC.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_PPC.1 because the evaluator action elements ASE_PPC.1.1E and ASE_PPC.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_PPC.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_PPC.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_PPC.1.1E Rationale:

The evaluation team checked the [FW1_ST], [ALF_PP], and [TFF_PP]. The evaluator checked the evidence and determined that it describes each PP claim, it identifies the TOE security requirements that satisfy the permitted operations of the PP and it identifies those security objectives and IT security requirements that are additional. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ASE_PPC.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_PPC.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_PPC.1.2E Rationale:

The evaluation team examined the [FW1_ST], [ALF_PP], and [TFF_PP]. The evaluator examined the evidence and determined that all operations on security requirements transcribed from the PP are within the bounds set by the PP and that the information provided is consistent with the information in the PP. Because the PPs were slightly different, the evaluator checked that the ST requirements did intend capture the functionality described in both PPs. The evaluator checked that each requirement from the PPs was captured in the ST by either restatement or legitimate refinement. The evaluator was able to map all PP requirements to a corresponding ST requirement. Additional requirements in the ST were necessary for completeness and did not conflict with the PP requirements. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.1.6 ASE_REQ.1 – IT Security Requirements

ASE_REQ.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_REQ.1 because the evaluator action elements ASE_REQ.1.1E and ASE_REQ.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_REQ.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_REQ.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_REQ.1.1E Rationale:

The evaluation team checked and examined the [FW1_ST]. The evaluator checked the evidence and found that the TOE security functional requirement are clearly identified as TOE security functional requirements and were drawn from CC Part 2 functional requirements components. The evaluator checked the evidence and found that each security functional component and each assurance component were correctly transcribed into the ST. The evaluator checked the evidence and found that the TOE security assurance requirements are clearly identified as TOE security assurance requirements and were drawn from CC Part 3 assurance requirements components. The evaluator checked the evidence and found that the statement of TOE security assurance requirement includes EAL 2 and that there are no assurance requirements not included in EAL 2. The evaluator checked the evidence and found that all operations on IT security requirements were identified and performed correctly. The evaluator examined the security requirements rationale and determined that all dependencies required by the IT security requirements are accounted for and satisfied by the [FW1_ST]. The evaluator checked and found that the ST includes a minimum strength of SOF-basic and that it identifies the functional requirements that require an explicit strength of function, together with the specific metric. The evaluator examined the evidence and determined that the security requirement rationale demonstrates SOF-basic, together with the explicit strength of function claim, is consistent with the security objectives for the TOE. The evaluator examined the security requirements rationale and determined that the IT security requirements for the TOE and for the environment are suitable to meet all of the stated security objectives and the set of IT security requirements together are mutually supportive. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ASE_REQ.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_REQ.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_REQ.1.2E Rationale:

The evaluation team examined the IT security requirements and the security requirements rationale, and determined that these sections were complete, coherent, and internally consistent. An independent analysis was performed in work unit ASE_REQ.1-3 that shows all operations on IT security requirements were performed correctly. An independent analysis was performed in work unit ASE_REQ.1-19, which shows the security requirements are mutually supportive to ensure that all security objectives for the TOE are satisfied. The evaluator determined that no security requirement conflicts with any other security requirement. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.1.7 ASE_SRE.1 – Explicitly Stated IT Security Requirements

ASE_SRE.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_SRE.1 because the evaluator action elements ASE_SRE.1.1E and ASE_SRE.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_SRE.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_SRE.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_SRE.1.1E Rationale:

The [FW_ST] did not contain explicitly stated security requirements. The work units for this evaluation action element are trivially satisfied.

ASE_SRE.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_SRE.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_SRE.1.2E Rationale:

The [FW_ST] did not contain explicitly stated security requirements. The work units for this evaluation action element are trivially satisfied.

4.1.8 ASE_TSS.1 – TOE Summary Specification

ASE_TSS.1 Verdict:

The evaluation team concluded that the ST has met the security target evaluation criteria of ASE_TSS.1 because the evaluator action elements ASE_TSS.1.1E and ASE_TSS.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ASE_TSS.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ASE_TSS.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_TSS.1.1E Rationale:

The evaluation team checked and examined the [FW1_ST]. The evaluator checked the evidence and found that the TOE summary specification describes the IT security functions and assurance measures of the TOE. The evaluator checked the evidence and found that a mapping from IT security functions to TOE security functional requirements is provided and that each IT security function maps to at least one TOE security functional requirement. The evaluator examined the evidence and determined that each IT security function is presented so that a clear understanding of its intent can be made and all references to security mechanisms are traced to the relevant IT security functions. The evaluator examined the evidence and determined that the TOE summary specification rationale demonstrates that the IT security functions are suitable to meet the TOE security functional requirements and that the combination of the specified IT security functions work together to satisfy the TOE security functional requirements. The evaluator examined the evidence and determined that the assurance measures meet the TOE security assurance requirements. The evaluator checked the evidence and determined that the TOE summary specification identifies all IT security functions that are realized by a probabilistic or permutational mechanisms and states a strength of function claim. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ASE_TSS.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ASE_TSS.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ASE_TSS.1.2E Rationale:

The evaluation team examined the TOE summary specification and the TOE summary specification rationale of [FW1_ST], and determined that these two sections are complete, coherent, and internally consistent. The IT security functions and assurance measures are mutually supportive in achieving the TOE security requirements. Each IT security function maps to a security functional requirement and each assurance measure maps to a TOE security assurance requirement. Also, an independent analysis was performed in work units ASE_TSS.1-6 and ASE_TSS.1-9 showing these mappings. The strength of function claim is consistent between both IT security functions and IT security requirements. The IT security functions and assurance measures are sufficient to ensure that all specified TOE security requirements is satisfied. Both the TOE summary specification and its rationale were found to be internally consistent. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.2 Configuration Management

The objectives this activity are to determine whether Check Point has clearly identified the TOE and its associated configuration items.

4.2.1 ACM_CAP.2 – CM capabilities

ACM_CAP.2 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ACM_CAP.2 because the evaluator action element ACM_CAP2.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ACM_CAP.2.1E Verdict:

The evaluation team successfully completed the evaluator action element ACM_CAP.2.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ACM_CAP.2 Rationale:

The evaluation team checked and examined [FW1_CM] and [FW1_DEL]. The evaluator examined the evidence and determined that it describes the Configuration Management (CM) procedures. The evaluator examined the TOE software and the [FW1_DEL] documentation to determine that the TOE provides a unique reference and label by using a version number and service pack number. The evaluator found that the TOE references were consistent. The evaluator evaluated [FW1_CM] to determine that a configuration list was provided; and that the list described and uniquely identified the configuration item for the TOE. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.3 Delivery and Operation

The objectives of this activity is:

- to determine whether the delivery documentation describes all procedures used to maintain integrity when distributing the TOE to the user's site and

- to determine whether the procedures and steps for the secure installation, generation, and start-up of the TOE have been documented and result in a secure configuration.

4.3.1 ADO_DEL.1 – Delivery Procedures

ADO_DEL.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ADO_DEL.1 because the evaluator action elements ADO_DEL.1.1E and the implied evaluator action were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ADO_DEL.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ADO_DEL.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADO_DEL.1.1E Rationale:

The evaluation team reviewed the [FW1_DEL]. The delivery procedures depicted in [FW1_DEL] reflect and enhance the vendor's current secure delivery processes and procedures. The evaluator determined that the requirements for this activity were satisfied.

Implied Evaluator Action Verdict:

The evaluation team successfully completed the implied evaluator action. Therefore, a **pass** verdict has been issued for this evaluator action element.

Implied Evaluator Action Rationale:

The evaluation team reviewed the [FW1_DEL]. Although the TOE is currently not available for delivery to customers, it was assumed that the delivery procedures utilized will be those that are currently in place. [FW1_DEL] depicted those procedures. The evaluator determined that the requirements for this activity were satisfied.

4.3.2 ADO_IGS.1 – Installation, Generation, and Start-up Procedures

ADO_IGS.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ADO_IGS.1 because the evaluator action elements ADO_IGS.1.1E and ADO_IGS.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ADO_IGS.1.1.E Verdict:

The evaluation team successfully completed the evaluator action element ADO_IGS.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADO_IGS.1.1.E Rationale:

The evaluation team reviewed [FW1_IGS] and [FW1_QGS]. The information provided within [FW1_IGS] was compared to the functionality described in [FW1_FSP] in order to ensure completeness of [FW1_IGS]. In addition, [FW1_IGS] was examined for consistency with the Administrator Guidance as part of completing the AGD_ADM work units. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ADO_IGS.1.2.E Verdict:

The evaluation team successfully completed the evaluator action element ADO_IGS.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADO_IGS.1.2.E Rationale:

The evaluation team reviewed [FW1_IGS] and [FW1_QGS]. The [FW1_IGS] was used to actually install the TOE in preparation of testing and thus was verified as containing the necessary steps for installation, generation, and startup. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.4 Development

The objective of this activity is:

- to determine whether Check Point has provided an adequate description of the security functions of the TOE and whether the security functions provided by the TOE are sufficient to satisfy the functional requirements of the ST;

- to determine whether the high-level design is sufficient to satisfy the functional requirements of the ST, provides a description of the TSF in terms of major structural units with functional coherence, and is a realization of the functional specification; and

- to determine whether Check Point has correctly and completely implemented the requirements of the ST and functional specification in the high-level design.

4.4.1 ADV_FSP.1 – Informal functional specification

ADV_FSP.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ADV_FSP.1 because the evaluator action elements ADV_FSP.1.1E and ADV_FSP.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ADV_FSP.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ADV_FSP.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADV_FSP.1.1E Rationale:

The evaluation team checked and examined [FW1_ST], [FW1_FSP], [FW1_AGD_003], and [FW1_AGD_001]. The functional specification was examined and found to contain all necessary informal explanatory text. The [FW1_FSP] was examined and found to identify the TSF and TOE external interfaces and describes their security characteristics using an informal style. The evaluator interpreted text and graphics as informal style. The evaluator found through the successful performance of the [CEM_PART2] ADV_FSP work units that a consistent description for the TOE had been provided, that a complete description of externally visible interfaces, a correct description of externally visible interfaces, a complete description of security functions, a complete description of the TOE, and an accurate description of the TOE had been provided.

The [FW1_FSP] was examined and found to identify all TOE security function interfaces. This examination found that the [FW1_FSP] identified and described six externally visible TOE interfaces. The first four interfaces include the FireWall-1 GUI Interface, FireWall-1 Command Line Interface, NT GUI Interface, and NT Command Line Interface are visible to the FireWall-1 administrator to configure and manage TOE. The fifth interface, called Network Interface, is used to pass network traffic. The sixth interface, called Users Interface, is visible to users using SMTP, TELNET, FTP, and HTTP protocol services.

The evaluator verified that the six identified interfaces constituted a complete list of externally visible TOE interfaces by examining the [FW1_ST], [FW1_AGD_003], and [FW1_AGD_001] for identification of other/different interfaces. The evaluator examination of these documents found that the FireWall-1 Command Line, FireWall-1 GUI, User Interface, and Network Interface were explicitly identified to a finer granularity by describing window panes, commands, and RFCs. The evaluator also mapped SFRs that may require an administrative interface to the external security function interfaces and found that all such SFRs mapped to an identified interface. This examination led the evaluator to conclude that the [FW1_FSP] had provided a complete list of externally visible interfaces.

The [FW1_FSP] was examined and adequately and correctly describe the effects, exceptions, and error messages of the TOE at each external interface. The evaluator developed a table to verify that the supporting description provide with each interface description adequately and correctly identified each interface effects, exceptions, and error messages. The [FW1_FSP] reference, in many cases, identified other documentation to complete the description of externally visible effects, exceptions, and error messages. The evaluator consulted the identified references to ensure that each interface effects, exceptions, and error messages were adequately and correctly specified.

As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ADV_FSP.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ADV_FSP.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADV_FSP.1.2E Rationale:

The [FW1_FSP], [FW1_AGD_003], and [FW1_AGD_001] documents were examined and found to be an accurate instantiation of the TOE security functional requirements. This evaluator verified that the functional specification was an accurate instantiation of the TOE security functional requirements by constructing a table where TOE security functional requirements were mapped to [FW1_FSP] security functions and interface descriptions or references. The references were checked and verified that SFRs was fully satisfied. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.4.2 ADV_HLD.1 – Descriptive high level design

ADV_HLD.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ADV_HLD.1 because the evaluator action elements ADV_HLD.1.1E and ADV_HLD.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ADV_HLD.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ADV_HLD.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADV_HLD.1.1E Rationale:

The evaluation team checked and examined [FW1_ST], and [FW1_HLD]. The [FW1_HLD] was examined and was found to describe the security characteristics of the FireWall-1 subsystems, subsystem interfaces, externally visible subsystem interfaces, and information flow between subsystems and across interfaces using an informal style. The evaluator interpreted text and graphics as an informal style.

The [FW1_HLD] document was examined and found to describe the functional behavior of the TSF in terms of subsystems. The [FW1_HLD] described the functional behavior of the Kernel, Daemon, Management, GUI, and Security Server, NT Authentication, NT Access Control, NT Audit, and NT Utilities subsystems. The [FW1_HLD] was examined and found to describe the functional behavior of each subsystem. The evaluator constructed a table to verify that the functional behavior of each subsystem was described. This table identified each of the six subsystems and the identified the location within the [FW1_HLD] where a description of its functional behavior was provided. The [FW1_HLD] document was checked and was found to identify the interfaces to the TSF subsystems. The evaluator checked the [FW1_HLD] to verify that it identified the interfaces to the TSF subsystems by constructing a table that verified that each subsystem had at least one interface, and that the interfaces specified between subsystems were balanced. The [FW1_HLD] document was checked and was found to identify the externally visible interfaces of the TSF subsystems. Since the ST does not include requirements on the IT environment, the evaluator determined that descriptions concerning the underlying hardware, firmware, or software was not applicable.

As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ADV_HLD.1.2E Verdict:

The evaluation team successfully completed the evaluator action element ADV_HLD.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADV_HLD.1.2E Rationale:

The evaluation team checked and examined [FW1_ST], and [FW1_HLD]. By successfully completing the [CEM_PART2] ADV_HLD work units the evaluator concluded that the evidence demonstrates that the TSF is described in terms of subsystems, functional behavior is the subsystems is described, subsystems interfaces are accurately described, and the externally visible subsystem interfaces are identified and the TOE is an accurate and complete instantiation of SFRs. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.4.3 ADV_RCR.1 – Informal correspondence demonstration

ADV_RCR.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ADV_RCR.1 because the evaluator action element ADV_RCR.1.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ADV_RCR.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ADV_RCR.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ADV_RCR.1.1E Rationale:

The evaluation team checked and examined [FW1_ST], [FW1_RCR], [FW1_FSP], and [FW1_HLD]. The [FW1_RCR] correspondence analysis between the TOE summary specification and the functional specification document was examined and the functional specification was found to be a correct and complete representation of the TOE security functions and interfaces. The evaluator, per [CEM_PART2] paragraph 648 guidance, performed this work unit in conjunction within 2:ADV_FSP.1-7 and 2:ADV_FSP1-8. The correspondence analysis developed by the developer was independently verified by comparing its analysis [FW1_RCR, Table 5 Mapping of SFRs to Security Functions] to the evaluator's independent 2:ADV_FSP.1-7 evaluation work unit table that mapped security functionality and interfaces to SFRs. The evaluator also verified the completeness and correctness of the [FW1_RCR, Table 2 Mappings of Security Functions to Interfaces] by independently developing an identical mapping as part of the 2:ADV_FSP.1-5 evaluator action. The independent confirmation provide by these two analysis leads the evaluator to conclude that the mappings provided within the [FW1_RCR] document are correct and thus the functional specification is a correct and complete representation of the TOE security functions.

The [FW1_RCR] document was examined and the correspondence analysis between the functional specification and the high-level design was found to be a correct and complete representation of the functional specification. The evaluator verified the correctness and completeness the [FW1_RCR] correspondence analysis by independently verifying that SFR mapping to subsystems [FW1_RCR, Table 3 &4] and the externally visible interface and interface components mapping to subsystems [FW1_RCR, Table 5]. The evaluator independently verified the correctness of the [FW1_RCR, Table 3 & 4] while performing 2:ADV_HLD.1-9 and 2:ADV_HLD.1-10. Within those two evaluation work units the evaluator independently developed tables that were consistent with those developed by the developer that show that all SFRs can be allocated to subsystems. The evaluator independently verified the completeness and correctness [FW1_RCR, Table 5, Mapping of Subsystems to External Interfaces] by verifying that all SFRs are allocated to subsystems, that the [FW1_HLD] documented externally visible interfaces to be consistent with the identified externally visible interfaces presented within the [FW1_FSP], and that [FW1_RCR Table 5] to be consistent with the interface descriptions provided within the [FW1_HLD] document.

As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.5 Guidance Documents

The objectives of this activity is:

- to determine whether the administrator guidance to system administrative personnel describes how they administer the TOE in a secure manner and
- to determine whether the user guidance describes the security functions and interfaces provided by the TSF for non-administrative users and whether this guidance provides instructions and guidelines for the secure use of the TOE.

4.5.1 AGD_ADM.1 – Administrator guidance

AGD_ADM.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of AGD_ADM.1 because the evaluator action element AGD_ADM.1.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

AGD_ADM.1.1E Verdict:

The evaluation team successfully completed the evaluator action element AGD_ADM.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AGD_ADM.1.1E Rationale:

The evaluation team checked and examined the following evidence [FW1_AGD_001], [FW1_AGD_002] [FW1_AGD_003], [FW1_IGS], [FW1_ST], and [FW1_FSP]. The evaluator examined the evidence and by mapping each SFR to a set of administrator functions and interfaces, as appropriate determined that the evidence describes the administrative security functions and interfaces available based on the security functional requirements stated in the ST. The evaluator examined the evidence and determined that it describes how to administer the TOE in a secure manner by describing audit trail management, setting up information flow rules, backup and recovery, and account management. The evaluator examined the administrator guide to determine that appropriate warnings were included. The evaluator examined the evidence to determine that assumptions regarding the user behavior with regards to single-use authentication were described. The evaluator examined the evidence and found that security parameters and values were described. The evaluator examined the evidence and determined that security relevant events relating to administrative functions were described. The evaluator examined the evidence and found that the administrative guidance was consistent with other evaluation evidence by reading the ST, Functional Specification, User Guide, and Installation Procedures. 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 the requirements for this activity were satisfied.

4.5.2 AGD_ADM.1 – Administrator guidance

AGD_USR.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of AGD_USR.1 because the evaluator action element AGD_USR.1.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

AGD_USR.1.1E Verdict:

The evaluation team successfully completed the evaluator action element AGD_USR.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AGD_USR.1.1E Rationale:

The evaluation team checked and examined the following evidence [FW1_AGD_001], [FW1_AGD_002] [FW1_AGD_003] [FW1_AGD_004], [FW1_IGS], [FW1_ST], and [FW1_FSP]. The evaluator examined the evidence and determined that it describes the security functions and interfaces (i.e., FTP and Telnet login) for non-administrative users of the TOE. The evaluator examined the evidence and determined that the use of the authentication functions was described. The evaluator examined the evidence and found the appropriate warnings described. The evaluator examined the evidence and determined that all user responsibilities and assumptions regarding single-use authentication and user behavior was adequately described. The evaluator examined the evidence and determined that the user guidance was consistent with other evaluation evidence by reading the ST, Functional Specification, Administrator Guide, and Installation Procedures. 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 the requirements for this activity were satisfied.

4.6 Testing

The objectives of this activity is:

- to determine whether the test coverage evidence shows correspondence between the tests identified in the test documentation and the functional specification;
- to determine whether Check Point’s functional testing demonstrates that all security functions perform as specified; and
- to determine whether the TOE behaves as specified and to gain confidence in Check Point’s test results by independently testing a subset of the TSF and by performing a sample of the developer’s tests.

4.6.1 ATE_COV.1 – Evidence of coverage

ATE_COV.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ATE_COV.1 because the evaluator action element ATE_COV.1.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ATE_COV.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ATE_COV.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ATE_COV.1.1E Rationale:

The evaluation team checked and examined [FW1_TST] and [FW1_FSP]. The twenty tests contained in [FW1_TST] were organized by security function and span four of the five security functions identified in [FW1_FSP]. The fifth security function, ***FW1_PSF*** is identified as being tested across the other four security functions. The individual tests within [FW1_TST] identify the SFRs covered within the test. The evaluators compared the SFRs covered to the SFRs within each security function, and to the totality of SFRs within the TOE. Examination of the individual tests and the data provided showed that the identified mapping was complete and accurate. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.6.2 ATE_FUN.1 – Functional testing

ATE_FUN.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ATE_FUN.1 because the evaluator action element ATE_FUN.1.1E was successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ATE_FUN.1.1E Verdict:

The evaluation team successfully completed the evaluator action element ATE_FUN.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ATE_FUN.1.1E Rationale:

The evaluation team thoroughly checked and examined [FW1_TST], comparing it as required to [FW1_FSP], [FW1_ST], and [FW1_IGS]. The test documentation provided in [FW1_TST] contained test plans, test procedures, and expected and actual results for each test. The document identified the security functions and SFRs to be tested, the goals of each test, and provided adequate instruction to ensure proper repeatability of all tests with the exception of ***FW1_SMAN_3***. Actual results achieved were consistent with expected results, with the exception of ***FW1_AUD_2*** (for which the vendor later released a patch). The expected results achieved were appropriate for successful completion of the tests, and adequately demonstrated the security functionality being tested. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

4.6.3 ATE_IND.2 – Independent testing – sample

ATE_IND.2 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of ATE_IND.2 because the evaluator action elements ATE_IND.2.1E, ATE_IND.2.2E, and ATE_IND.2.3E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

ATE_IND.2.1E Verdict:

The evaluation team successfully completed the evaluator action element ATE_IND.2.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ATE_IND.2.1E Rationale:

Check Point setup the test configuration in CSC lab spaces to match the TOE description in the ST and executed their tests as specified in [FW1_TST]. The evaluation team used the same test bed and set up and installed the TOE in accordance with [FW1_IGS] in order to ensure proper installation and knowledge of the initial test state. Because Check Point conducted their tests in CSC lab spaces, the evaluation team was able to ensure that the resources provided by the developer are equivalent to the set of resources used by the developer to functionally test the TSF. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ATE_IND.2.2E Verdict:

The evaluation team successfully completed the evaluator action element ATE_IND.2.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ATE_IND.2.2E Rationale:

The evaluation team conducted independent testing with the intent of ensuring (a) coverage of all SFRs via the combination of vendor and evaluator testing; and (b) an appropriate level of rigor of testing for critical security functions. After examination of [FW1_TST], the evaluators decided to test [FW1_SOFT] in the following areas:

- **FW1_AUDIT**. Evaluator focus was to ensure full testing of Windows NT - related functionality; verify selectable audit review; and determine the status of the vendor's TOE fixes relating to traffic flow stoppage once the audit trail becomes full (Patch 1).

- **FW1_I&A.** Evaluator focus was to test S/Key implementation and the TOE's authentication failure handling mechanism

- **FW1_UDP**. Evaluator focus was to ensure that the TOE adequately met the requirements associated with its handling of malformed service requests. Also, the evaluators wanted to conduct testing to verify that the TOE met the requirements for residual information protection – the one function not tested by the vendor.

The following actions were taken to prepare the laboratory for testing:

- [FW1_SOFT] was installed upon the host machine in accordance with [FW1_IGS].
- A series of administrator and user accounts were created on the TOE, and on the internal and external network PCs.

All tests within the test suite were executed a minimum of three (3) times against the TOE with consistent results. As patches arrived and were loaded, regression testing was conducted to ensure that the changes did not adversely impact the TOE. Each test was run at least once against each patched version of FireWall-1. Actual test results mirrored expected results. As a result of these activities, the evaluator determined that the requirements for this activity were satisfied.

ATE_IND.2.3E Verdict:

The evaluation team successfully completed the evaluator action element ATE_IND.2.3E. Therefore, a **pass** verdict has been issued for this evaluator action element.

ATE_IND.2.3E Rationale:

The developer's approach was to test all TSFs of the TOE within the laboratory environment. Developer testing, though appropriate and accurate, was deemed to be of insufficient depth in the area of testing for malformed service requests. The vendor subsequently provided a series of tests designed to further verify the TOE's functionality in this area.

All testing results achieved were successful, with the exception of ***FW1_AUD_2***; the vendor produced a patch for the TOE that rectified this problem, but opted not to re-test the functionality. The evaluators did test this functionality during independent testing and achieved successful results.

4.7 Vulnerability Assessment

4.7.1 AVA_SOF.1 – Strength of TOE security functions

AVA_SOF.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of AVA_SOF.1 because the evaluator action elements AVA_SOF.1.1E and AVA_SOF.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

AVA_SOF.1.1E Verdict:

The evaluation team successfully completed the evaluator action element AVA_SOF.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AVA_SOF.1.1E Rationale:

The evaluation team examined the following evidence: [APPL_PP], [TFF_PP], [FW1_AGD_003], [FW1_FSP], [FW1_HLD], [FW1_SOF], and [FW1_ST] The evaluator identified three strength of function (SOF) claims made by the developer in [FW1_ST]: an overall claim of SOF-basic, and two metrics for probabilistic or permutational security mechanisms satisfying the FIA_UAU.1 and FIA_UAU.4 SFRs. The evaluator further examined the assumptions, threats, and objective security policy assertions in [FW1_ST] and determined that the claimed overall SOF of SOF-basic is appropriate. This determination was based on the low attack potential of the threat agents and the assumed security environment of [ALF_PP] and [TFF_PP], to which the TOE is claiming conformance.

The evaluator mapped the assumptions used for the analysis performed in [FW1_SOF] to the policies expressed in [FW1_ST], the design expressed in [FW1_FSP] and [FW1_HLD], and the guidance provided in [FW1_IGS] and [FW1_AGD_003]. Further, the evaluator reproduced the calculations performed by the vendor in [FW1_SOF] to verify that the calculations were correct, and demonstrated that the TOE satisfied the metrics for the reusable and single-use passwords.

By performing these actions, the evaluator determined that the TOE satisfies the Strength of Function requirements specified for the FIA_UAU.1 and FIA_UAU.4 SFRs in the [FW1_ST], [ALF_PP], and [TFF_PP].

AVA_SOF.1.2E Verdict:

The evaluation team successfully completed the evaluator action element AVA_SOF.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AVA_SOF.1.2E Rationale:

By mapping all probabilistic or permutational mechanisms identified in the evaluator's examination of the [FW1-FSP] and [FW1_HLD] to those in [FW1_SOF], the evaluator determined that these claims covered all probabilistic or permutational mechanisms in the TOE.

4.7.2 AVA_VLA.1 – Vulnerability analysis

AVA_VLA.1 Verdict:

The evaluation team concluded that the TOE has met the assurance requirements of AVA_VLA.1 because the evaluator action elements AVA_VLA.1.1E and AVA_VLA.1.2E were successfully completed. Therefore, a **pass** verdict has been issued for this assurance component.

AVA_VLA.1.1E Verdict:

The evaluation team successfully completed the evaluator action element AVA_VLA.1.1E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AVA_VLA.1.1E Rationale:

The evaluation team examined the following evidence: [APPL_PP], [TFF_PP], [FW1_AGD_001], [FW1_AGD_003], [FW1_AGD_005], [FW1_FSP], [FW1_HLD], [FW1_IGS], [FW1_SOF], [FW1_ST], [FW1_TST], and [FW1_VUL]. The evaluator examined [FW1_VUL] and by creating a mapping table checked that the attack scenarios described in Appendix A of both the [TFF_PP] and [APPL_PP] were adequately addressed. The evaluator performed an independent search of the internet to locate reports of vulnerabilities with the FireWall-1 to confirm the vendor's search for FireWall-1 vulnerabilities identified in the public domain. The evaluation team concluded that the vendor performed an adequate check, and their claims for why vulnerabilities were not applicable or not exploited in the intended TOE environment were acceptable.

AVA_VLA.1.2E Verdict:

The evaluation team successfully completed the evaluator action element AVA_VLA.1.2E. Therefore, a **pass** verdict has been issued for this evaluator action element.

AVA_VLA.1.2E Rationale:

The evaluation team's approach for penetration testing took into account the analysis presented in [FW1_VUL], the unique services provided by an application level firewall versus a traffic filter firewall, and any published vulnerabilities that were not included in [FW1_VUL]. The penetration test was broken down into the following areas:

- Vulnerability List Analysis. The evaluator checked and examined vendor claims and TOE behavior to the [ALF_PP] and [TF_PP] Appendix A identified vulnerabilities and conducted tests to try to disprove the developer's analysis.
- Attack Malformed Service Requests. The evaluator independently checked and examined the security functions of [ALF_PP] FDP_IFF.1.6 (f) for both the AUTHENTICATED and UNAUTHENTICATED services for the vendor advertised services defined in [FW1_ST].
- Check Strength of SKEY. The evaluator checked for and examined known vulnerabilities in the S-Key authentication processes.

- Check Security of Network Interface Card. The evaluator checked for and examined known vulnerabilities in the 3COM Etherlink III 3C509TP and 3COM Fast Etherlink XL 10/100MB 3C905B-TX TOE network cards.
- Attack Operating System based on published vulnerabilities. The evaluator checked and examined interfaces and components critically relied by the TOE that may circumvent TOE security functions (such as startup and shut down risks).

After conducting penetration tests against the TOE, the evaluation team concluded that the TOE has no exploitable vulnerabilities in the intended TOE environment.

5 CONCLUSIONS AND RECOMMENDATIONS

The TOE was evaluated against the [FW1_ST]. The assurance component verdicts presented in Chapter 5 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. The ST was found to be conformant to [ALF_PP] and [TFF_PP]. As defined by [CC_PART1] Chapter 5, the TOE was found to be Part 2 conformant, Part 3 conformant, and conformant to PP. The evaluation team recommends that an EAL 2 certificate rating be issued for the TOE.

6 ACRONYMNS AND GLOSSARY OF TERMS

The following acronyms are used throughout this document.

CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CEM	Common Evaluation Methodology
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
IP	Internet Protocol
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
TSC	TOE Scope of Control
TSF	TOE Security Functions

7 PROBLEM REPORTS

7.1 Evaluation Discovery Reports

This section of contains all EDRs raised as a result of work performed during the evaluation. Table 10 provides the EDRs unique identifier, the work package in which the problem was discovered, a brief summary of the problem, and their status.

Table 10: EDR Status Register

Identifier	Work Package	Description	Status
FW1_EDR_001	ST Evaluation	Incomplete description of TOE	Closed
FW1_EDR_002	ST Evaluation	Incomplete list of Threats	Closed
FW1_EDR_003	ST Evaluation	Version number missing	Closed
FW1_EDR_004	ST Evaluation	Typographical errors	Closed
FW1_EDR_005	ST Evaluation	Incomplete threat mapping	Closed
FW1_EDR_006	ST Evaluation	Rationale section not completed	Closed
FW1_EDR_007	ST Evaluation	Incomplete PP claim	Closed
FW1_EDR_008	ST Evaluation	Missing dependency statement	Closed
FW1_EDR_009	ST Evaluation	Missing strength statement	Closed
FW1_EDR_010	Del and Oper	Shortcoming in Delivery Procedures Documentation	Closed
FW1_EDR_011	Del and Oper	Shortcomings in IGS Documentation	Closed
FW1_EDR_012	Guidance	Incomplete descriptions for administrative security functions and interfaces	Closed
FW1_EDR_013	Guidance	Incomplete description to administer TOE in secure manner	Closed
FW1_EDR_014	Guidance	Incomplete presentation of warnings for functions and privileges	Closed
FW1_EDR_015	Guidance	No assumptions of user behavior provided	Closed
FW1_EDR_016	Guidance	Incomplete description of security parameters	Closed
FW1_EDR_017	Guidance	Inconsistency between Guidance and IGS	Closed
FW1_EDR_018	Guidance	Separate User's Guide	Closed
FW1_EDR_019	Guidance	Missing descriptions of security-relevant events	Closed
FW1_EDR_020	Development	Fragmented subsystem descriptions	Closed
FW1_EDR_021	Development	Missing hardware, software, firmware identification	Closed
FW1_EDR_022	Development	Subsystem interfaces are unbalanced	Closed
FW1_EDR_023	Development	Explicit statements needed to identify externally visible interfaces	Closed
FW1_EDR_024	Development	Missing presentation of the functions provided by the supporting protection mechanisms	Closed
FW1_EDR_025	Development	ST errors	Closed
FW1_EDR_026	Development	User lock out after failure threshold	Closed
FW1_EDR_027	Development	Auditable event table incorrectly identifying requirements	Closed
FW1_EDR_028	ST Evaluation	Requirement inconsistencies	Closed
FW1_EDR_029	Development	Kernel.Attachment effects, exceptions, and error messages missing	Closed

Identifier	**Work Package**	**Description**	**Status**
FW1_EDR_030	CM	Incomplete configuration list	Closed
FW1_EDR_031	ST Evaluation	Security Target Meeting 8-2-1999	Closed
FW1_EDR_032	Development	Authorized administrator unlocking user accounts	Closed
FW1_EDR_033	Development	Missing audit event mapping	Closed
FW1_EDR_034	Development	Incomplete NT subsystem descriptions	Closed
FW1_EDR_035	Development	Correspondence evidence incomplete	Closed
FW1_EDR_036	Development	Incomplete information flow descriptions	Closed
FW1_EDR_037	Development	TFS subsystem interface require names	Closed
FW1_EDR_038	Development	Malformed service descriptions needed for Telnet, FTP, SMTP, and HTTP	Closed
FW1_EDR_039	Development	Kernel.Attachment SMTP and HTTP interface effects, exceptions, and error messages missing	Closed
FW1_EDR_040	Development	FW1_FS revision date	Closed
FW1_EDR_041	Guidance	Configuring unauthenticated SFP	Closed
FW1_EDR_042	Vulnerability	Vulnerability search sources missing	Closed
FW1_EDR_043	Security Target	Errors found in Version 1.5	Closed
FW1_EDR_044	Delivery & Ops.	Problems with creation of drivespace.conf file	Closed
FW1_EDR_045	Guidance	Backup recommendation violates TSF domain separation	Closed
FW1_EDR_046	Penetration	Ambiguous Security Policy rulebase state and FTP Authentication Bypass Risk	Closed
FW1_EDR_047	Penetration	No HTTP and SMTP Proxying	Closed
FW1_EDR_048	Penetration	Ambiguous security policy rulebase state creates service proxy bypass risk	Closed
FW1_EDR_049	Penetration	Telnet Malformed Service Request Failure during Authentication	Closed
FW1_EDR_050	Penetration	Telnet Malformed Service Request Failure post Authentication	Closed
FW1_EDR_051	Testing	Non-repeatability of vendor test *FW1_SMAN_3*	Closed
FW1_EDR_052	Penetration	Overlooked Appendix A Vulnerabilities	Closed
FW1_EDR_053	ST Evaluation	Errors found in version 2.0	Closed
FW1_EDR_054	Penetration	TOE Bypass Ability through NIC	Closed
FW1-EDR_055	Development	Correspondence analysis to function specification	Closed
FW1-EDR_056	Development	Correspondence analysis to high-level design	Closed
FW1-EDR_057	Vulnerability	Description of reusable password policy incorrect	Closed
FW1-EDR_058	ST Evaluation	Errors found in version 2.3	Closed

7.2 Observation Reports

This section of contains all ORs raised as a result of work performed during the evaluation. Table 11 provides the ORs unique identifier with corresponding Scheme identifier in parenthesis, as appropriate, a brief summary of the problem, and an indication of the problem's current status.

Table 11: OR Status Register

Identifier	Title	Status
FW1_OR_001 (OR 80)	Enumeration of requirements	Closed
FW1_OR_002 (OR 81)	Synonymous use of "service request" versus "command"	Closed
FW1_OR_003 (OR 82)	Interpretation of audit requirements	Closed
FW1_OR_004	Interpretation of ADV_RCR.1	Closed
FW1_OR_005 (OR 84)	Definition of "malformed service request"	Closed
FW1_OR_006 (OR 85)	Allocation of requirements for support services to IT Security Environment	Closed
FW1_OR_007	Residual Information Protection-RIP.2	Closed
FW1_OR_008	Firewall Protection Profiles lack SFRs required for strength of function analysis	Closed
FW1_OR_009 (OR 88)	Request for interpretation of ATE_COV.1	Closed
FW1_OR_010	"Obvious" Vulnerabilities for ALG-PP	Closed
FW1_OR_011	Definition of Security Domain for FPT_SEP	Closed
FW1_OR_012	Initialization of Default Values	Closed
FW1_OR_013 (OR 144)	Request for interpretation of FIA_ATD.1	Closed
FW1_OR_014 (OR 145)	FDP_IFF.1 (1) not correctly state from the CC	Closed
FW1_OR_015 (OR 146)	Request for interpretation of FMT_MOF.1	Closed
FW1_OR_016 (OR 147)	Request for interpretation of FAU_SAR.3	Closed
FW1_OR_017 (OR 148)	I&A requirements not complete in PP	Closed