Check Point Software Technologies Ltd. FireWall-1 Version 4.0

Security Target

Version 2.4

Final

October 1999

Prepared for:

Check Point Software Technologies Ltd.

Prepared by:

Computer Sciences Corporation
7471 Candlewood Road
Hanover, MD 21076

Table of Contents

List of Tables

Check Point FireWall-1 Version 4.0 Security Target

1 SECURITY TARGET INTRODUCTION

1 This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

2 An ST document provides the basis for the evaluation of an *information technology (IT)* product or system (e.g., TOE). An ST principally defines:

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

3 The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for an ST may include not only evaluators but also developers and "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE,"[1] this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluation* (CC).

4 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5.

5 An ST, like a Protection Profile (PP), contains sections which address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements Rationale sections. Under certain conditions, the contents of these sections of the ST may be identical with those of the PP, namely, when the ST:

- Claims compliance with the PP.
- Performs no additional operations[2] on the PP security functional requirements.

[1] ***Common Criteria for Information Technology Security Evaluation*** **(CC), Part 1, C.1, par. 2.**

[2] **The CC allows controlled tailoring of its security functional requirements, by means of four *operations* (namely, refinement, selection, assignment, and iteration; see CC, Part 2, par. 2.1.4).**

- Does not extend the PP by adding security objectives and/or security requirements.

6 Under these conditions, the CC states that "*reference* to the PP is sufficient to define and justify the TOE objectives and requirements. *Restatement* of the PP contents is unnecessary" [italics added].[3]

7 The methodology used to develop and present this ST includes the following steps:[4]

- Those PP security objectives and requirements with which the ST claims compliance and for which no additional operations are to be performed are restated within the ST verbatim.
- If the ST will perform additional operations on PP requirements, the ST restates the requirements, performs the operations, and identifies the change by convention.
- If the ST extends the PP by adding security objectives and/or security requirements, the ST states the objectives and/or requirements, makes any needed additions to the Security Environment section, and documents suitable Rationale sections.

1.1 ST and TOE Identification

8 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the Check Point FireWall-1 Version 4.0. This ST targets an Evaluation Assurance Level (EAL) 2 level of assurance.

- **ST Title:** Check Point Software Technologies Ltd. FireWall-1 Version 4.0 Security Target
- **ST Version:** 2.4
- **TOE Identification:** Check Point FireWall-1 Version 4.0, SP5 for Windows NT 4.0.
- **CC Identification:** Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998
- **PP Identification (1):** U.S. Government Application-level Firewall Protection Profile for Low-Risk Environments, Version 1.d.1, Draft, September, 1999 (referred to as ALFPP)
- **PP Identification (2):** U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (referred to as TFFPP)
- **ST Evaluation:** Computer Sciences Corporation (CSC)
- **Keywords:** information flow control, firewall, packet filter, application level, proxy filtering, network security, traffic filter, security target

[3] CC, Part 1, Annex C, par. C.2.8, b.

[4] The TFFPP contains a subset of the security functional requirements and all the assurance requirements of the ALFPP. For simplicity, references to the PP imply the ALFPP if appropriate. It is assumed by showing compliance to the ALFPP, the TOE is also compliant with the TFFPP.

1.2 Conventions, Terminology, and Acronyms

9 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

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

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

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by <u>*underlined italicized text.*</u>
- The security target writer operation is used to denote points in which the final determination of attributes was left up to the writer of the security target. Target writer operations are indicated by braces { }.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, i.e., FMT_MOF.1.1 (1) and FMT_MOF.1.1 (2).

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

1.2.2 Terminology

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

- ***User*** - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- ***Human user*** - Any person who interacts with the TOE.
- ***External IT entity*** - Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

- ***Role*** - A predefined set of rules establishing the allowed interactions between a user and the TOE.

- ***Identity*** - A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.

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

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

- ***Authorized Administrator*** - A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

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

1.2.3 Acronyms

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

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

1.3 Security Target Overview

16 The Checkpoint FireWall-1 Suite is comprised of two modules:

- The *Management Module* includes the Graphic user interface (GUI) and the Management Server. The Management Module can also be deployed in a Client/Server configuration, where a GUI client running in a Windows 95, Windows NT or X/Motif platform[5] controls a Management Server running on either a Windows NT or Unix platform[6].

- The *FireWall Module* includes the Inspection Module, FireWall-1 daemons, and the FireWall-1 Security Servers.

17 A FireWall-1 security policy is defined in terms of firewalls, services, users, resources and the rules that govern the interactions between them. Once these have been specified, the inspection code is generated and then installed on the firewalled gateways, hosts, routers, switches or packet filters that will enforce the Security policy.

18 A single Management Module can control and monitor multiple FireWall Modules. The FireWall Module operates independently of the Management Module. FireWall Modules can operate on additional Internet gateways, interdepartmental gateways, and critical servers, thus providing peripheral defense as well as in-depth security compartmentalization[7].

1.4 Common Criteria Conformance Claims

19 The TOE conforms to:

- the U.S. Government Application-level Firewall Protection Profile for Low-Risk Environments, Version 1.d.1, Draft.

- the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1.

It also conforms to Parts 2 and 3 of the CC, Version 2.0.

1.5 ITSEC Evaluation Traceability

20 FireWall-1 has been successfully evaluated to the E3 level of assurance under the European Information Technology Security Evaluation and Certification (ITSEC) scheme. In order to maintain traceability between the deliverables supplied for the ITSEC evaluation and those supplied for this evaluation, the ITSEC Security Enforcing Functions (SEFs), that were used to state security requirements for the ITSEC evaluation are listed in Table 1. Only those SEFs that have a corresponding functionality in this evaluation have been included.

[5] NT is the evaluated configuration GUI platform

[6] NT is the evaluated configuration SMS platform

[7] The evaluated configuration consists of one (1) FireWall-1 Module that implements the Security Policy, logs events, and communicates with the Management Module; one (1) 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; and two (2) network interfaces with one designated as internal and the other as external.

Table 1 SEFs for ITSEC E3 Evaluation

SEF	Security Functionality	Description
[AC1]	Access Control Administration	Identifies several security management functions
[AC2]	Traffic Flow Control	Defines a Traffic Flow Security Policy
[AC4]	Traffic Flow Control	Defines the operation and action of the Traffic Flow Security Policy.
[AC6]	IP Source Routing Protection	States that Source Routed Packets will be denied access.
[AUD2]	Audit Events	States that audit events will be recorded for each attempt to send or receive an IP packet.
[AUD3]	Audit Records	Identifies the information that must be contained in each audit record.
[AUD4]	Displaying Audit Logs	Identifies selection criteria for searching and sorting the log files.

2 TOE DESCRIPTION

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

2.1 Architecture

22 The FireWall-1 Architecture is comprised of two primary software modules, the Management Module and the FireWall Module.

23 The Management Module includes

- the Graphical User Interface (GUI), and
- the Management Server.

24 The FireWall Module includes

- the Inspection Module,
- FireWall-1 Daemons, and
- the FireWall-1 Security Servers.

25 The GUI is the front end to the Management Server, which manages the FireWall-1 database: the Rule Base, network objects, services, users, etc.

26 The Inspection Module implements the Security Policy, logs events, and communicates with the Management Module using daemons.

27 The GUI Client, the Management Server and the FireWall Module can be installed on different computers, or on the same computer. For the evaluated configuration of the TOE, these modules are all contained on a single platform executing Windows NT Server 4.0 operating system with service pack 4 installed.

28 The system administrator uses the Management Module to define the Security Policy, but it is the FireWall Module that enforces the Security Policy.

29 No claims are made in this ST regarding FireWall-1 functionality not included in this ST. It is therefore emphasized that *operating the TOE outside its evaluated configuration negates the security claims made in this ST*.

2.2 Scope and Boundaries of the Evaluated Configuration

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

2.2.1 Physical Scope and Boundary

31 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. and
- 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.

32 The physical scope of the TOE includes the hardware and software elements identified 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

2.2.2 Logical Scope and Boundary

33 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.

34 Software and hardware features outside the scope of the defined TOE Security Functions (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.

2.3 Application Context

35 The evaluated TOE has the GUI Client, the Management Server and the FireWall Module installed on the same computer platform providing integrated Internet and Intranet access control as well as authentication. The Management Module can control and monitor multiple FireWall Modules.

36 The FireWall Module operates independently of the Management Module. The FireWall Module comprises the Inspection Module, FireWall-1 daemons and the FireWall Security Servers. The evaluated configuration requires that FireWall-1 be installed on a dual-homed host (a gateway). Since the Inspection Module is loaded in the operating system kernel, it intercepts packets before they are forwarded. In addition, processes and daemons on the gateway need not be killed, since FireWall-1 controls connections to them at the lowest layer, the network layer. FireWall-1 implements full security with connectivity.

2.4 Product Type

37 The FireWall-1 is a firewall employing a hybrid application-level gateway and packet filtering called Stateful Multilayer Inspection. The technology utilizes packet filtering's performance and scalability and the security of an application gateway.

- *Application-level Firewall* – mediates flows between clients and servers located on internal and external networks governed by the firewall. An application-level firewall may employ proxies to screen information flows. Proxy servers on the firewall for services such as FTP and Telnet, require authentication at the firewall by client users before requests for such services can be authorized. Only valid requests are relayed to the actual server by the proxy server on either an internal or external network.

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

38 The FireWall-1 Inspection Engine applies full application-level security but doesn't permit packets to reach the operating system of the machine the firewall sits on. Additionally, the firewall imposes traffic-filtering controls on information flows mediated by the firewall.

3 TOE SECURITY ENVIRONMENT

39 The TOE is intended to be used either in environments in which sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent. To clarify and define the FireWall-1 security environment, assumptions about the security environment and/or the manner in which the FireWall-1 will be used are provided.

40 Identification of known or assumed threats to the assets requiring FireWall-1 or its environments to provide specific protection further defines the FireWall-1 security environment. The assumptions and threat identification combined with any organization security policy statement or rules requiring FireWall-1 compliance completes the definition of the security environment. It is necessary that a comprehensive security policy be established for the site(s) in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- ***Physical security*** - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.

- ***Procedural security*** - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.

- ***Personnel security*** - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.1 Assumptions

41 The TOE claims the following assumptions delineated within Section 3.1 of the ALFPP. Those assumptions that are claimed are stated verbatim in Table 3 below:

Table 3 Assumptions from the ALFPP

Name	Description
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE

42 Four security environment assumptions described in the ALFPP have been modified in this ST. Table 4 states these modified assumptions. The refined assumptions are applicable to the architecture of this specific TOE.

Table 4 Modified Assumptions

Name	Description
A.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT	The TOE is available to authorized administrators only.
A.NOREMO	Human users can not access the TOE remotely from the internal or external networks.

43 An additional security assumption for the environment not described in the ALFPP has been included in this ST. Table 5 states this additional assumption.

Table 5 Additional Assumptions

Name	Description
A.ESECFUN	With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.

3.2 Threats

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

3.2.1 Threats Addressed by the TOE

45 The TOE addresses all threats delineated within Section 3.2.1 of the ALFPP. For clarity, these threats are restated verbatim in Table 6.

Table 6 Threats

Name	Description
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

Name	Description
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in information flows mediated by the TOE between clients and servers located on internal and external networks governed by the TOE, by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized user may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

3.2.2 Threats Addressed by the Operating Environment

46 The TOE Operating Environment addresses the same ALFPP, Section 3.2.2 Threats. These threats are restated verbatim in the following Table 7.

Table 7 Threats Addressed by Operating Environment

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

3.3 Organizational Security Policies

47 The ALFPP states one Organizational Security Policy (OSP) relating to the use of cryptographic modules. Because this TOE is not providing remote administration, this OSP does not apply. Therefore, no organizational security policy is specified.

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

49 The TOE accomplishes a subset of the security objectives delineated within Section 4.1 of the ALFPP. For clarity, these security objectives are restated in Table 8.

Table 8 Security Objectives

Name	Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

50 Eleven security objectives for the TOE environment and the assumptions met by the objectives are those specified in the following tables. The eight objectives in Table 9 are derived from the ALFPP, Sections 4.1 and 4.2.

Table 9 Security Objectives for the Environment

Name	Description	Assumption(s) /Threats
O.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	A.LOWEXP
O.PUBLIC	The TOE does not host public data.	A.PUBLIC
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	A.NOEVIL
O.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE	A.SINGEN
O.ESECFUN	With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.	A.ESECFUN
O.NOREMO	Human users can not access the TOE remotely from the internal or external networks.	A.NOREMO
O.GUIDAN	Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, and operated in a manner that maintains security.	T.TUSAGE
O.ADMTRA	Authorized administrators are trained as to establishment and maintenance of sound security policies and practices.	T.TUSAGE

51 The three security objectives contained in Table 10 are new security objectives for the TOE environment.

Table 10 Additional Security Objectives for the Environment

Name	Description	Assumption(s) Met
O.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.	A.PHYSEC
O.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	A.GENPUR
O.DIRECT	The TOE and associated direct-attached console are available to authorized administrators only.	A.DIRECT

5 TOE IT SECURITY REQUIREMENTS

52 IT security requirements include:

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

53 These requirements are discussed separately below.

5.1 TOE Security Requirements

54 The CC divides security requirements into two categories:

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

55 This section presents the security functional and assurance requirements for the TOE.

5.1.1 TOE Security Functional Requirements

56 This section presents the SFRs for the TOE. This section has the following four subsections:

- *Restated PP SFRs*: those PP security functional requirements with which the ST claims compliance[8] and for which no additional operations are to be performed. These PP SFRs are included in the ST verbatim.
- *Tailored PP SFRs*: those PP security functional requirements with which the ST claims compliance but for which additional operations are to be performed.
- *Additions to PP SFRs* (optional): any security functional requirements additional to those of the PP.
- *SFRs With Strength of Function (SOF) Declarations:* any security functional requirement that requires a SOF declaration.

5.1.1.1 Restated PP SFRs

57 The TOE shall satisfy the SFRs stated in Table 11 which lists the CC names of the SFR *components*[9] contained in the ALFPP. Following the table, the individual functional requirements are restated from the ALFPP.

[8] Compliance is based on incorporation of the changes recommended in ORs against the TFFPP.

Table 11 Restated Security Functional Requirements

Functional Component ID	Functional Component Name
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FDP_RIP.1	Subset residual information protection
FIA_UAU.1	Timing of authentication
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior (1)
FMT_MOF.1	Management of security functions behavior (2)
FMT_MSA.1 (1)	Management of security attributes (1)
FMT_MTD.1	Management of TSF data (1)
FMT_MTD.1	Management of TSF data (2)
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FMT_MTD.2	Management of limits on TSF data

58 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

59 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

60 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall *prevent auditable events except those taken by the authorized* ***administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

61 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following

[9] In CC parlance, a *component* is "the smallest set of selectable [requirements] elements that may be included in a PP" or an ST (CC, Part 1, 2.3). An element is "An indivisible security requirement" (*ibid*.).

objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

62 **FIA_UAU.1 Timing of authentication**

FIA_UAU.1.1 The TSF shall allow

a) [information flow control decisions and subsequent passing or dropping of non-FTP and non-Telnet traffic;

b) identification as stated in FIA_UID.2]

on behalf of the **authorized administrator or authorized external IT entity accessing the TOE** to be performed before the **authorized administrator or authorized external IT entity** is authenticated.

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

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

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

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

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

65 **FPT_SEP.1 TSF domain separation**

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

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

66 **FPT_STM.1 Reliable time stamps**

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

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

FMT_MSA.1.1 (1) - The TSF shall enforce the [UNAUTHENTICATED SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule,] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized administrator].

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

FMT_MTD.1.1(1) - The TSF shall restrict the ability to [query, modify, delete, and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

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

FMT_MTD.1.1(2) - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

70 **FMT_MTD.2 Management of limits on TSF data**

FMT_MTD.2.1 - The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

71 **FMT_MOF.1 (1) Management of security functions behavior (1)**

FMT_MOF.1.1(1) - The TSF shall restrict the ability to [enable, disable] the functions:

a) [operation of the TOE;

b) single-use authentication function described in FIA_UAU.4;]

to [an authorized administrator].

Application Note: By “Operation of the TOE” in a) above, we mean having the TOE start up (enable operation) and shut down (disable operation).

72 **FMT_MOF.1 (2) Management of security functions behavior (2)**

FMT_MOF.1.1(2) - The TSF shall restrict the ability to [enable, disable, determine and modify the behaviour of] the functions:

a) [audit trail management;

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

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

5.1.1.2 Omitted PP SFRs

73 The AFLPP specifies that some functional requirements are optional and may be omitted from compliant TOEs. Table 12 identifies the SFRs that have been omitted from this ST because the evaluated configuration of Check Point FireWall-1 4.0 does not support Remote Administration of the TOE.

Table 12 Functional Components Omitted from the TOE

Reference	Description
FCS_COP.1	Cryptographic operation

5.1.1.3 Tailored PP SFRs

74 The ALFPP identifies several SFRs that contain operations to be completed in PP-compliant security targets. This section identifies those ALFPP requirements and performs the required operations. In addition, this section contains PP SFRs that were refined to specifically capture TOE functionality. The TOE shall satisfy the resultant requirements.

75 Table 13 names the SFRs for which the ST is required to perform operations. The table also identifies the operations (assignment, iteration, refinement, and selection) performed on them in this ST. Following the table, the individual functional requirements are restated from the ALFPP, and the operations completed.

Table 13 Tailored ALFPP SFRs

Functional Component ID	Functional Component Name	Operation
FAU_GEN.1	Audit data generation	Refinement
FAU_SAR.3 (1)	Selectable audit review (1)	Iteration Selection
FAU_SAR.3 (2)	Selectable audit review (2)	Assignment Iteration
FDP_IFC.1 (1)	Subset information flow control (1)	Refinement Iteration
FDP_IFC.1 (2)	Subset information flow control (2)	Refinement Iteration
FDP_IFC.1 (3)	Subset information flow control (3)	Refinement Iteration
FDP_IFF.1 (1)	Simple security attributes (1)	Assignment Iteration
FDP_IFF.1 (2)	Simple security attributes (2)	Assignment Iteration
FDP_IFF.1 (3)	Simple security attributes (3)	Assignment Iteration

Functional Component ID	Functional Component Name	Operation
FIA_AFL.1	Authentication failure handling	Assignment
FIA_ATD.1	User attribute definition	Assignment
FIA_UAU.4	Single-use authentication mechanisms	Assignment
FMT_MSA.1 (2)	Management of security attributes (2)	Iteration
FMT_MSA.1 (3)	Management of security attributes (3)	Iteration
FMT_MSA.1 (4)	Management of security attributes (4)	Iteration
FMT_MSA.1 (5)	Management of security attributes (5)	Iteration
FMT_MSA.1 (6)	Management of security attributes (6)	Iteration
FMT_MSA.3	Static attribute initialization	Refinement
FMT_SMR.1	Security roles	Refinement

76 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

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

c) [the events listed in **Table 14**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of **Table 14**].

Table 14 Auditable Events[10]

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	All use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication	The identity of the offending user and the authorized administrator

[10] *The auditable event(s) related to FCS_COP.1 has been removed as this requirement is optional and has been omitted from this ST because the TOE does not support remote administration.*

Functional Component	Auditable Event	Additional Audit Record Contents
	attempts and the subsequent **restoration by the authorized administrator of the users capability to authenticate**.	
FDP_IFF.1 (1)	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1 (2)	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1 (3)	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	**Use of the functions listed in this requirement pertaining to audit**.	The identity of the authorized administrator performing the operation

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

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

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses.]

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

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

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

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

FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] on:

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

b) information: **non-FTP, non-Telnet, non-HTTP and non-SMTP** traffic sent through the TOE from one subject to another;

c) operation: pass information].

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

FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED_APPL SFP] on:

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

b) information: **HTTP and SMTP** traffic sent through the TOE from one subject to another;

c) operation: pass information].

81 **FDP_IFC.1 (3) Subset information flow control (3)**

FDP_IFC.1.1 The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: an external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.4,

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

c) operation: initiate service and pass information.]

82 **FDP_IFF.1 (1) Simple security attributes (1)**[11]

FDP_IFF.1.1 (1) The TSF shall enforce the [UNAUTHENTICATED SFP] based on the following types of subject and information security attributes:

a) [SUBJECT attributes:

[11]. *The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 (1) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1 (1).*

FDP_IFF.1.3 - *The TSF shall enforce the [none].*

FDP_IFF.1.4 - *The TSF shall provide the following [none].*

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

- presumed address;
- {no other subject attributes}.

b) INFORMATION attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- **all** service**s except FTP, Telnet, HTTP and SMTP**;
- {no other information security attributes}].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

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

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules:

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

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

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

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

83 **FDP_IFF.1 (2) Simple security attributes (2)**[12]

FDP_IFF.1.1 (2) The TSF shall enforce the [UNAUTHENTICATED_APPL SFP] based on the following types of subject and information security attributes:

a) [SUBJECT attributes:

- presumed address;
- {no other subject attributes}.

b) INFORMATION attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service**s: HTTP, SMTP**;
- {no other information security attributes}].

[12]. The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 (1) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1 (1).

FDP_IFF.1.3 **-** *The TSF shall enforce the [none].*

FDP_IFF.1.4 **-** *The TSF shall provide the following [none].*

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

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

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

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules:

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

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

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

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

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

f) The TOE shall reject **service commands not identified in Table 15**:]

Table 15 Valid HTTP and SMTP commands.

HTTP Commands	SMTP Commands	
OPTIONS	HELO	NOOP
GET	MAIL	QUIT
HEAD	RCPT	
POST	DATA	
PUT	RSET	
DELETE	VRFY	
TRACE	EXPN	
CONNECT	HELP	

84 FDP_IFF.1 (3) Simple security attributes (3)[13]

FDP_IFF.1.1 (3) The TSF shall enforce the [AUTHENTICATED SFP] based on the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;
- {no other subject attributes}

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service**s: FTP, Telnet**;

[13]. *The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 (2) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1 (2).*

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

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

- **commands: FTP: PUT, GET, PASV, PORT; Telnet: N/A**
- {[no other information attributes]}].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

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

- the human user initiating the information flow authenticates according to FIA_UAU.4;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

- the human user initiating the information flow authenticates according to FIA_UAU.4;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network].

FDP_IFF.1.6 (3) The TSF shall explicitly deny an information flow based on the following rules:

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

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

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

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

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

f) The TOE shall reject **service commands not identified in Table 16:**]

Table 16 Valid FTP and Telnet commands.

FTP Commands				Telnet Commands	
USER	STOR	RNTO	MKD	EOF	EL
PASS	APPE	ABOR	XMKD	SUSP	GA
ACCT	RETR	DELE	RMD	ABORT	SB
REIN	ALLO	CWD	XRMD	EOR	WILL
QUIT	RNFR	XCWD	PWD	SE	WONT
PORT	LIST	NOOP	SIZE	NOP	DO
PASV	NLST	XPWD	MDTM	DM	DON’T
TYPE	SYST	CDUP		BRK	IAC
STRU	STAT	XCUP		IP	AYT
MODE	HELP	STOU		AO	EC

85 **FIA_AFL.1 Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [**a non-zero number settable by** {an authorized administrator}] **of** unsuccessful authentication attempts occur related to [users not associated with the authorized administrator role attempting to authenticate from an internal or external network].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question].

86 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [Identity

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

c) {no other user security attributes}].

87 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

a) authorized administrators;

b) authorized external IT entities;

c) human user attempting to access the following services through the TOE:

- File Transfer Protocol (FTP);
- Telnet;
- {no other services}].

88 FMT_MSA.1 (2) Management of security attributes (2)

FMT_MSA.1.1 (2) - The TSF shall enforce the [UNAUTHENTICATED_APPL SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule,] the security attributes [listed in section FDP_IFF1.1(2)] to [the authorized administrator].

89 FMT_MSA.1 (3) Management of security attributes (3)

FMT_MSA.1.1(3) - The TSF shall enforce the [AUTHENTICATED SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule] the security attributes [listed in section FDP_IFF1.1(3)] to [the authorized administrator].

90 FMT_MSA.1 (4) Management of security attributes (4)

FMT_MSA.1.1(4) - The TSF shall enforce the [UNAUTHENTICATED SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

91 **FMT_MSA.1 (5) Management of security attributes (5)**

FMT_MSA.1.1(5) - The TSF shall enforce the [UNAUTHENTICATED_APPL SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

92 **FMT_MSA.1 (6) Management of security attributes (6)**

FMT_MSA.1.1(6) - The TSF shall enforce the [AUTHENTICATED SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in FDP_IFF.1(3)] to [the authorized administrator].

93 **FMT_MSA.3 Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the [**information flow** UNAUTHENTICATED SFP, **UNAUTHENTICATED_APPL SFP**, and AUTHENTICATED SFP,] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

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

94 **FMT_SMR.1 Security roles**

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

FMT_SMR.1.2 The TSF shall be able to associate **human** users with **the authorized administrator** role.

5.1.1.4 Additions to PP SFRs

95 An additional SFR from CC Part 2 is identified for the TOE. Table 17 identifies the SFR added to the ST. The ALFPP specifies some of the characteristics required of the two authentication mechanisms that may be used via the FIA_UAU.1 and FIA_UAU.4 SFRs. The additional SFR identifies the types of authentication mechanisms that may be used and the conditions requiring their use.

Table 17 Additional CC Part 2 Functional Component for TOE

Reference	Description
FIA_UAU.5	Multiple authentication mechanisms

96 **FIA_UAU.5 Multiple authentication mechanisms**

FIA_UAU.5.1 The TSF shall provide [password and single-use authentication mechanisms] to support user authentication

FIA_UAU.5.2 The TSF shall authenticate any user’s claimed identity according to the [following multiple authentication mechanism rules:

a) Single-use authentication mechanism shall be used when services requiring single-use authentication, according to the AUTHENTICATED SFP of the ALFPP, are enable and the user attempts to use one of those services;

b) Reusable password mechanism shall be used only when the authorized administrator is attempting to access the TOE via a directly connected terminal (e.g., to manage the TOE through its management console)].

5.1.1.5 SFRs With SOF Declarations

97 The FIA_UAU.1 SFR requires that the TOE have an authentication mechanism that has a probability of authentication data being guessed will be less than one in a million.

98 The FAU_UAU.4 SFR requires that the single-use authentication mechanism comply with the "Statistical random number generator tests" and the "Continuous random number generator test" found in section 4.11.1 of FIPS PUB 140-1.

99 The overall Strength of function claim for the TOE is SOF-basic.

5.1.2 TOE Security Assurance Requirements

100 Table 18 identifies the security assurance components drawn from CC Part 3: Security Assurance Requirements, EAL2. With the exception of AVA_VLA.1, the assurance requirements are stated verbatim from ALFPP section 5.1.2, TOE Security Assurance Requirements.

Table 18 EAL2 ALFPP SARs

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

101 **ACM_CAP.2 Configuration items**

Developer action elements :

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

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

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements :

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

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

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

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

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

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

Evaluator action elements :

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

102 ADO_DEL.1 Delivery procedures

Developer action elements :

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

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

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

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

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

104 ADV_FSP.1 Informal functional specification

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

Evaluator action elements :

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

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

105 ADV_HLD.1 Descriptive high-level design

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

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

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

Evaluator action elements :

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

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

106 ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

107 **AGD_ADM.1 Administrator guidance**

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

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

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

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

Evaluator action elements :

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

108 **AGD_USR.1 User guidance**

Developer action elements :

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements :

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

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

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

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

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

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

Evaluator action elements :

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

109 ATE_COV.1 Evidence of coverage

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

110 ATE_FUN.1 Functional testing

Developer action elements :

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements :

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

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

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

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

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

Evaluator action elements :

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

111 ATE_IND.2 Independent testing – sample

Developer action elements :

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

Content and presentation of evidence elements :

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

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

Evaluator action elements :

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

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

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

112 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements :

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

Content and presentation of evidence elements :

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

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

Evaluator action elements :

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

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

113 AVA_VLA.1 Developer vulnerability analysis

Developer action elements :

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

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

Content and presentation of evidence elements :

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, including **those identified in Appendix A of ALFPP v1.d.1**, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements :

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

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

5.2 Security Requirements for the IT Environment

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

6 TOE SUMMARY SPECIFICATION

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

6.1 TOE Security Functions

116 This section presents the security functions performed by the TOE. To aid evaluation of the TOE, traceability to SFRs is provided. In addition, traceability of ITSEC defined SEFs is provided to support reusability of ITSEC evaluation evidence.

6.1.1 Security Management [FW1_SMAN]

117 The Windows NT 4.0 operating systems maintains security attributes for all administrators. The NT User Management module maintains identity, authentication data, and a method of associating human users with the authorized administrator role for human users. The following administrative functions require successful login to the TOE:

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

b) Create, delete, modify, and view user attributes;

c) Enabling and disabling of the single use authentication mechanism for human user authentication;

d) Modify and set the threshold for the number of permitted authentication attempts by administrators and normal users;

e) Restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures;

f) Enable and disable external IT entities from communicating with the Firewall Host.

g) Modify and set the time and date;

h) Archive, create, delete, review, and empty the audit trail;

118 Default values for the TOE are such that all flow (inbound and outbound) is denied. The Management Module provides the only avenue to modify the TOE configuration by changing parameters on the **Kernel.** An authorized administrator must successfully log into the Management Module in order to adjust the configuration to permit the flow of information. In addition, the [FW1_IGS] document provides a set of administrative procedures for ensuring that the default installation of the TOE is restrictive.

119 **Functional Requirements Satisfied**: FMT_MOF.1 (1) and (2); FMT_MSA.1 (1), (2), (3), (4), (5) and (6); FMT_MSA.3; FMT_MTD.1 (1)and (2); FMT_MTD.2; and FMT_SMR.1

120 **ITSEC Traceability**: Functionality described for this security functions maps, in part, to the [AC1] SEF.

6.1.2 Identification and Authentication [FW1_INA]

121 There are two aspects of this security function that require strength of function rating. The authentication mechanisms used to authenticate the administrator and the single-use authentication mechanism have a probabilistic nature. Their SOF claim is SOF-basic. In addition, they must satisfy the following requirements:

a) the probability of authentication data being guessed will be less than one in a million, and

b) The single-use authentication mechanism must comply with the "Statistical random number generator tests" and the "Continuous random number generator test" found in section 4.11.1 of FIPS PUB 140-1.

122 The Identification and Authentication requirements address authentication failure handling, user attribute definition, timing of authentication, single-use authentication, and user identification before any action.

123 Windows NT 4.0 associates human users with specific identities (userid and password). NT maintains an *administrator* users group with unique access and privileges to records, programs, and functions on the Management Module. An authorized administrator may also set a threshold for unsuccessful authentication attempts for users accounts. Windows NT denies all human users the ability to perform any actions on the Management Module prior to successful authentication.

124 FireWall-1 provides user authentication, which enables an administrator to grant specific users special access privileges. FireWall-1 also enables the administrator to define a Security Policy on a per-user basis, where not only a packet's source, destination and service are verified. Additionally, individual users of interactive sessions (TELNET and FTP) are authenticated.

125 When the FireWall-1 Security Server – running at the application layer – detects a connection request, it utilizes SKEY to initiate an authentication procedure. If no Authentication scheme is specified for a user, the user is denied access. SKEY denies all human users the ability to perform any actions prior to successful authentication.

126 Even after the user has been authenticated, FireWall-1 does not allow the user to open an interactive session directly on the specified host. Instead, the FireWall-1 Security Server starts 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. At each point, packets can be logged and alerts can be issued. In this way, the interactive session is mediated and secured by the FireWall-1 Security Server, but the user is unaware of the Security Server and has the illusion of working directly on the target host.

127 Auto Shut-Out is a feature designed for compliance with Common Criteria requirements. In this feature, if a user fails to enter the correct password after several attempts (with the number set in advance by the administrator), the user is thenceforth blocked from being successfully authenticated. The block remains until the administrator takes action to clear it. This is accomplished by entering a set of commands via the command line to specifically unlock an individual user account.

128 The Authentication Failure Handling mechanism can be configured to lock out the individual users that have been installed within the user database. The users are locked and unlocked individually when a specified number of unsuccessful authentication attempts have been reached.

129 The NT User Management Module allows the administrator to set an authentication policy, which is enforced for all administration accounts on the TOE. The authentication policy required to meet the assurance requirements of AVA_SOF.1 is described below:

- Minimum of 8 characters
- The possible characters are a-z, A-Z, 0-9 and !@#$%^&*()_+
- The passwords must be changed every 12 months

130 If these rules are followed, the probability of guessing the password is less than one in one million.

131 The SKEY authentication mechanism used by the TOE to authenticate general users of the Security Services (i.e. Telnet and FTP) has the following characteristics,

- Secret key length of 10 or more characters
- The possible characters are a-z, A-Z, 0-9 and !@#$%^&*()_+
- Minimum of 100 passwords generated
- Hash algorithm is MD5

132 In addition, the random number generator used to develop the SKEY password sets, complies with the *"Statistical random number generator tests"* and the *"Continuous random number tests"* found in section 4.11.1 of FIPS PUB 140-1 [5]. This ensures that the SKEY implementation meets the requirements of the AVA_SOF.1 assurance requirement.

133 **Functional Requirements Satisfied**: FAU_STG.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5 and FIA_UID.2.

134 **ITSEC Traceability**: none.

6.1.3 User Data Protection [FW1_UDP]

135 The User Data Protection requirements are composed of subset information flow control, simple security attributes, and full residual information protection.

136 The FireWall-1 Security servers (proxies) provide authentication and filtering of malformed service request. When a FireWall-1 Security Server is invoked, the Kernel Module diverts all the packets in the connection to the Security Server, which performs the required proxying of the service and/or authentication. If the connection is allowed, then the Security Server opens a second connection to the final destination. Altogether, there are two connections: one from the client to the Security Server, and another from the Security Server to the final destination.

137 The **Kernel** component of the firewall is where the Stateful Inspection process is implemented and where information flow control occurs. The Kernel.Attachment sits in the packet stream and makes sure that all packets arriving at the NIC and destined for the IP module, or arriving from the IP module and destined for the NIC, move first into the firewall. Upon receipt of a packet, **Kernel.Attachment** takes note of the interface and the direction, and creates a larger entity to hold both packet and context information.

138 Virtual defragmentation is performed here; the larger entity is not sent onward for processing until all packets identified as fragments have been received and have been successfully reassembled into a single packet. Packet fragments are dropped if defragmentation can not be completed within a short period.

139 After virtual defragmentation, **Kernel.Attachment** then launches the **Kernel.Address_Translation** basic component for packets in the inbound direction. There are two procedures for producing and applying translations of addresses. One procedure, used for the first packet in a connection, applies the address translation rules in compiled form to generate a new translation. Translation rules specify ranges of addresses and the ranges into which they are to be mapped. The rules create a set of tables that are used in the translation process.

140 When a *static* mode is used, translations are one-to-one and remain the same so long as the translation rule has not been modified. A dynamic mode allows multiple machines to use the address of a single machine, normally that of the firewalled gateway.

141 Once the translation is generated and used for the first packet, updates are made to a dynamically created forward table and a backward table of original addresses and their translations. These tables provide the second address translation procedure. Packets in the same connection consult the table of existing connections with previously generated addresses, and apply the existing address translation to the current packet. Back-connecting packets find matching entries in the backward table, and forward-connecting packets find matching entries in the forward table. **Kernel.Virtual Machine** basic component is then called.

142 The Kernel.Virtual_Machine is where stateful inspection takes place. Packets received by **Kernel.Virtual_Machine** are pre-inspected by performing basic tests.

- One test directed in the firewall flow policy is *anti-spoofing*.
- Another is to test for packets containing IP options and drop all.

143 **Kernel.Virtual_Machine** then carries out the inspection process itself. Here the rules of the firewall flow 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,* or *drop*. The **Kernel.Virtual_Machine** also generates any necessary monitoring information, such as logs and alerts for SNMP traps.

144 The **INSPECT** engine is a huge switch that uses virtual machine language (INSPECT ML code) to carry out the operations of the firewall flow policy files. Its temporary data is maintained in a large stack.

145 After INSPECT, a Post-Inspect process is applied. Here the terminal actions (accept, reject, drop) are enforced by calling the functions associated with each action.

146 Kernel.Logging is used for transmitting logs and kernel traps generated by **Kernel.Virtual_Machine** up to the **Daemon** component for further processing.

147 The Kernel.Ioctl is used for receiving the firewall flow policy from the **Utilities** component. *Ioctls* are Input Output Controls, made available by the operating system for communication with kernel modules. As the **Kernel** component is isolated from other system devices by the interprocess separation mechanism, ioctls provide the only means by which information may be passed to it. The GUI serves as the front end of the Management Server. The authorized administrator interfaces with the **Utilities** component via the GUI to control and adjust firewall flow policies; address translation schemes; and the operation of the **Kernel** component. The **Utilities** component installs user-directed rules and changes onto the **Kernel** component. Rather than writing INSPECT code from the beginning for each rule, the product comes with files in a Library which define services, protocols, log behavior, table formats and how the **Kernel.Virtual_Machine** will react when encountering packets with the relevant parameters.

148 Unless a conduit is explicitly created by an authorized administrator, the TOE rejects all requests for services by external, unprotected networks. The TOE will also forward packets requesting access or services from the external to internal interface which comply with a conduit that has been pre-established by the administrator. Unless the administrator configured the firewall to specifically accept requests from the addresses mentioned in the requirement, the TOE will successfully reject any such request.

149 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 Firewall.

150 **Functional Requirements Satisfied**: FDP_IFC.1, FDP_IFF.1, FDP_IFC.1 (2), FDP_IFF.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (3) and FDP_RIP.1

151 **ITSEC Traceability**: Functionality described for this security functions maps, in part, to SEFs [AC2], [AC4], and [AC6].

6.1.4 Protection of Security Functions [FW1_PSF]

152 Protection of Security Functions requirements are composed of non-bypassability of the TSP, TSF domain separation, and reliable time stamps.

153 Data is not permitted to flow through the TOE after initial connection of power and network connections and when the Installation, Generation, and Startup (IGS) are complete. This provides the most restrictive default values for data flow through the TOE. Using the **GUI** and **Utilities** component the administrator can modify the initial configuration to allow traffic to flow through the TOE.

154 After Installation, Generation, and Startup are completed, the configuration is saved to non-volatile memory and will be invoked on subsequent system startup.

155 The TOE does not permit un-trusted subjects to execute on the TOE. The TOE only stores and executes security–relevant applications and only stores data required for its secure operation. In addition, the TOE is assumed to be located within controlled access facilities that mitigate unauthorized, physical access.

156 The TOE scope of control is defined as the following: connections between subjects mediated by the TSF such that each connection is a separate domain. Access through the TOE is only permitted based on security policy enforced by the FireWall-1 configuration defined by an authorized administrator.

157 A time stamp is derived from the Firewall Host to apply to audit events. The time stamp is considered to be reliable as the order of audit events is accurately reflected within the audit files. The TOE does not have physically separated components.

158 Packet encapsulation ensures no residual information is available from a previously sent packet as the packet is reconstructed from block data elements. The firewall is connected directly to each physical interface and traffic must go through the firewall module. NIC binding forces traffic through the firewall, protecting the TOE from tampering.

159 **Functional Requirements Satisfied**: FPT_RVM.1, FPT_SEP1, and FPT_STM.1.

160 **ITSEC Traceability**: none.

6.1.5 Audit [FW1_AUDIT]

6.1.5.1 Audit Generation

161 The Audit security functional requirements are composed of audit data generation, audit review, selectable audit review, protected audit trail storage, and prevention of audit data loss.

162 The TOE is able to generate an audit record for each of the auditable events in Table 19.

Table 19 TOE Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	basic	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	minimal	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users capability to authenticate.	The identity of the offending user and the authorized administrator
FDP_IFF.1	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

163 The TOE records, in the log message, the date and time of the event, type of event, subject identity, and outcome (success or failure) of the event.

164 Audit data generation, is implemented by the FireWall-1 and the NT operating system. NT logs events as pertain to accessing the Management Module. FireWall-1 provides logging for all activities pertaining to the actions to or through the product.

165 The **Kernel.Virtual_Machine** generates any necessary monitoring information, such as logs and alerts for SNMP traps. **Kernel.Logging** is the component used for transmitting logs and kernel traps generated by **Kernel.Virtual_Machine** up to the **Daemon** component for further processing.

166 The following events all generate audit records either through the NT or FireWall-1:

- Startup and Shutdown of the TOE
- Modifications to the group of users that are part of the authorized administrator role
- All use of the user identification mechanism, including the user identity provided
- All use of the authentication mechanism
- All decisions on request for information flow
- Create, delete, modify, and view information flow security policy rules that permit or deny information flows
- Create, delete, modify, and view user attributes
- Modify and set the time and date
- Archive, create, delete, review, and empty the audit trail
- Backup and recovery, where the backup capability shall be supported by automated tools.

167 **Functional Requirements Satisfied**: FAU_GEN.1

168 **ITSEC Traceability**: Functionality described for this security functions maps, in part, to SEFs [AUD2], and [AUD3].

6.1.5.2 Audit Review

169 Audit review of the NT log files is accomplished via the Event Viewer application. The Event Viewer permits the administrator to view, search and sort the audit files on all required parameters.

170 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. The [FW1_IGS] provides a set of procedures for searching and sorting the audit files using a range of IP addresses.

171 The audit data is presented in human-readable form within the log file. The authorized administrator is the only user allowed on the NT Workstation and therefore is the only user who has access to the audit trail. The Log Viewer is a graphical tool on the GUI used to search the log file and provides the ability to search and sort based on event type and on date and time.

172 **Functional Requirements Satisfied**: FAU_SAR.1 and FAU_SAR.3 (1) and (2)

173 **ITSEC Traceability**: Functionality described for this security functions maps, in part, to SEF [AUD4]

6.1.5.3 Audit Storage

174 Only authorized administrators are able to login to the firewall host and, subsequently, access the audit files.

175 The audit trail is protected by the NT workstation. The NT Workstation uses Microsoft's secure files system, NTFS. At user logon NT generates an access token for the user. The win32 subsystem uses that token to determine the user's access to all files on the NTFS disk. If the user does not belong to a group that has permission to access a file then NTFS denies the user access. All the FireWall-1 system and log files are protected by NTFS. Only users belonging to the Administrator group can access and manipulate the audit files. The only users allowed on the NT workstation are the authorized administrators, and authorized administrators are the only users that can modify, archive, and delete audit records.

176 The TOE is able to detect modifications to the audit trail by enabling file operation audit through the NTFS. The following success or failure of the following actions are audited: read, write, execute, delete, change permissions, take ownership.

177 Prevention of audit data loss is implemented by the FireWall-1 by stopping operation of the FireWall Module when it is unable to write to the appropriate audit files. Only actions taken by the authorized administrator are permitted and logged until disk space is available. The thresholds are based on percentage of disk space. If the proper threshold is set by the administrator, no audit data will be lost.

178 **Functional Requirements Satisfied**: FAU_STG.1 and FAU_STG.4

179 **ITSEC Traceability**: none.

6.2 Assurance Measures

180 The TOE satisfies the SARs specified in the ALFPP. This section identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Testing, and Vulnerability Analysis measures applied by Check Point to satisfy the CC EAL2 assurance requirements.

6.2.1 Configuration Management

181 The Configuration Management measures applied by Check Point include assigning a unique product identifier for each release of the TOE. Associated with this Product Identifier is a list of Hardware and Software configuration items that compose a single instance of the TOE. These configuration management measures are documented within the following Check Point documents:

- FW-1 Configuration Management

182 **Assurance Requirements Satisfied**: ACM_CAP.2

6.2.2 Delivery and Operation

183 Check Point provides Delivery and Operation documentation that describes what components are delivered with the FireWall-1, guidance for initially installing it, and warnings about the importance of properly unpacking, installing, and configuring the TOE. The Installation and Start-up document provides a set of procedures for initially installing and configuring the TOE into the evaluated configuration These delivery and operation measures are documented within the following Check Point documents:

- FW-1 Secure Delivery
- FW-1 Installation, Generation and Startup Guide

184 **Assurance Requirements Satisfied**: ADO_IGS.1 and ADO_DEL.1

6.2.3 Development

185 The Development documents provided by Check Point satisfy the CC functional specification and high-level design development requirements, as well as provide a correspondence between that information and this ST. These architecture measures are documented within the following Check Point documents:

- Check Point FireWall-1 Version 4.0 Functional Specification
- Check Point FireWall-1 Version 4.0 High Level Design
- FW-1 Informal Correspondence Demonstration

186 **Assurance Requirements Satisfied:** ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1

6.2.4 Guidance

187 The Guidance Documents provided by Check Point include both Installation and Configuration manuals that guide administrators through the process of unpacking, installing, and configuring the FireWall-1. These documents also warn the administrator about common mistakes that could lead to an insecure configuration. These guidance measures are documented within the following Check Point documents:

- Getting Started with FireWall-1 Quick Start Guide
- Account Management Client – User Guide
- Getting Started with FireWall-1 – User Guide
- Managing FireWall-1 – Using the Windows GUI

188 **Assurance Requirements Satisfied**: AGD_USR.1 and AGD_ADM.1

6.2.5 Test

189 Check Point performs extensive Testing of the FireWall-1. The testing performed includes both functional and penetration testing to ensure that the FireWall-1 meets its design goals. These tests are documented in the following Check Point documents:

- Check Point FireWall-1 Functional Testing
- Check Point FireWall-1: Additional Functional Testing

190 **Assurance Requirements Satisfied:** ATE_FUN.1, ATE_COV.1, and ATE_IND.2

6.2.6 Vulnerability Assessment

191 As part of the design and testing process, Check Point performs Vulnerability Analysis of the FireWall-1. The goal of this analysis is to identify any obvious weaknesses that could be exploited by an attack. The vulnerability analysis is documented within the following Check Point document:

- FW-1 Vulnerability Analysis

192 The Strength of Function Analysis performed on administrator authentication mechanism and the user authentication mechanism is provided within the following Check Point document:

- Check Point FireWall-1 Strength of Function Analysis

193 **Assurance Requirements Satisfied**: AVA_SOF.1 and AVA_VLA.1

7 PP CLAIMS

194 This section provides the PP conformance claim statements.

7.1 PP Claim – Application Level Firewall

7.1.1 PP Reference

195 The TOE conforms to the following PP:

- U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments, Version 1.d.1 draft, September, 1999.

7.1.2 PP Refinements and Additions

196 The following PP SFRS, SARs, and assumptions were further refined or added for this Security Target:

a)	FAU_GEN.1	Audit data generation
b)	FAU_SAR.3 (1)	Selectable audit review (1)
c)	FAU_SAR.3 (2)	Selectable audit review (2)
d)	FDP_IFC.1 (1)	Subset information flow control (1)
e)	FDP_IFC.1 (2)	Subset information flow control (2)
f)	FDP_IFC.1 (3)	Subset information flow control (3)
g)	FDP_IFF.1 (1)	Simple security attributes (1)
h)	FDP_IFF.1 (2)	Simple security attributes (2)
i)	FDP_IFF.1 (3)	Simple security attributes (3)
j)	FIA_AFL.1	Authentication failure handling
k)	FIA_ATD.1	User attribute definition
l)	FIA_UAU.4	Single-use authentication mechanisms
m)	FIA_UAU.5	Multiple authentication mechanisms
n)	FMT_MSA.1 (2)	Management of security attributes (2)
o)	FMT_MSA.1 (3)	Management of security attributes (3)
p)	FMT_MSA.1 (4)	Management of security attributes (4)

q)	FMT_MSA.1 (5)	Management of security attributes (5)
r)	FMT_MSA.1 (6)	Management of security attributes (6)
s)	FMT_MSA.3	Static attribute initialization
t)	AVA_VLA.1	Developer vulnerability analysis
u)	A.ESECFUN	Added assumption
v)	A.PHYSEC	Modified assumption
w)	A.GENPUR	Modified assumption
x)	A.DIRECT	Modified assumption
y)	A.NOREMO	Modified assumption

197 In the case of FAU_SAR.3, the refinement interprets the ALFPP SFR to require that FireWall-1 be capable of searching the audit data for user identity, presumed subject address, ranges of dates, ranges of time, and ranges of IP address and sorting audit data based on chronological order of occurrence. FireWall-1 satisfies this SFR interpretation.

198 In the case of FDP_IFC.1 and FDP_IFF.1, three (3) iterations were required to identify the traffic filter unauthenticated SFP (1), the application level unauthenticated SFP (2), and the application level authenticated SFP security attributes (3). Six (6) iterations of FMT_MSA.1 are needed to manage the security attributes identified in the three iterations of IFC and IFF.

FMT_MSA.1 (1) manages FDP_IFC.1 (1) attributes.

FMT_MSA.1 (2) manages FDP_IFC.1 (2) attributes.

FMT_MSA.1 (3) manages FDP_IFC.1 (3) attributes.

FMT_MSA.1 (4) manages FDP_IFF.1 (1) attributes.

FMT_MSA.1 (5) manages FDP_IFF.1 (2) attributes.

FMT_MSA.1 (6) manages FDP_IFF.1 (3) attributes.

199 In the case of AVA_VLA.1 the refinement specifies the minimum identified vulnerabilities for which the evaluated FireWall-1 must be analyzed.

200 The following security objectives for the environment were added in this ST: O.PHYSEC, O.GENPUR, and O.DIRECT.

201 Additionally, the FIA_UAU.5, multiple authentication mechanisms, was included within the set of SFRs. This was used to address the fact that the TOE uses two separate

authentication mechanisms. The ALFPP specifies some of the characteristics required of the two authentication mechanisms (reusable and single-use) that may be used via the FIA_UAU.1 and FIA_UAU.4 security functional requirements (SFRs). However, it fails to provide an SFR identifying what types of authentication mechanisms may be used or the conditions requiring their use.

7.1.3 Rationale for not implementing all PP security objectives

202 The ST does not include the following TOE and environment security objectives: O.ENCRYP, O.LIMEXT, and O.REMACC. These security objectives are relevant to secure remote administration of the TOE. These objectives are beyond the scope of this evaluation.

7.2 PP Claim – Traffic Filter Firewall

7.2.1 PP Reference

203 The TOE conforms to the following PP:

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

7.2.2 PP Refinements and Additions

204 The ALFPP contains a superset of SFRs identified in the TFFPP. However, the refinements of similar SFRs differ between the profiles. Where the refinement is different, the SFR refinement was taken from the ALFPP, except for FMT_SMR.1, that was taken from the TFFPP. The ALFPP refinements are such that they permit both traffic filter and application level functionality. The iteration convention has been utilized for several SFRs to ensure compliance with both PPs.

205 FAU_GEN.1 and FMT_MOF.1 are significantly different in the ALFPP from the TFFPP. Although the FAU_GEN.1 was taken from the ALFPP, the requirement captures the intent of the TFFPP requirement because the same set of security functions are audited. The TFFPP FMT_MOF.1 requirement is captured in the following ALFPP requirements: FMT_MOF.1 (1) and FMT_MOF.1 (2); FMT_MSA.1 (1), (2), (3), and (4); FMT_MTD.1 (1) and (2); FMT_MTD.2. Because the ST includes these ALFPP requirements, it satisfies the TFFPP FMT_MOF.1 requirement.

206 The Information Flow Control policy as stated in the TFFPP by FDP_IFF.1 and FDP_IFC.1 is captured in this ST as FDP_IFF.1 (1) and FDP_IFF.1 (2) with refinement to identify services that are controlled by traffic filtering techniques.

8 RATIONALE

207 This section demonstrates the completeness and consistency of this ST.

- *Traceability* The security objectives for the IT and environment are explained in terms of threats countered and assumptions met. The SFR are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:
  - ➢ security objectives to threats countered
  - ➢ objectives to assumptions met
  - ➢ SFRs to objectives met
- *Modifications* A justification is provided for assumptions that are modified in this ST.
- *Assurance Level* A justification is provided for selecting an EAL2 level of assurance for this ST.
- *SOF* A rationale is provided for the SOF level chosen for this ST.
- *PP Conformance* A justification is provided as to why the ST is conformant to both the ALFPP and TFFPPs.
- *Dependencies* A justification is provided for all requirement dependencies not met.

8.1 Rationale For IT Security Objectives

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.SINUSE This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF, which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.SECSTA This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

Table 20: Mapping of threats to security objectives

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X								
O.SINUSE		X	X						
O.MEDIAT				X	X	X			
O.SECSTA	X							X	
O.SELPRO								X	X
O.AUDREC							X		
O.ACCOUN							X		
O.SECFUN	X		X						X

8.2 Rationale For Security Objectives For The Environment

208 The security objectives for the environment are a restatement of the assumptions for the environment with the exception of two additional objectives: O.GUIDAN and O.ADMTRA.

O.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training.

Table 21: Mappings Between Threats/Assumptions and Security Objectives for the Environment

	T.TUSAGE	A.LOWEXP	A.PUBLIC	A.NOEVIL	A.SINGEN	A.ESECFUN	A.NOREMO	A.PHYSEC	A.GENPUR	A.DIRECT
O.GUIDAN	X									
O.ADMTRA	X									
O.LOWEXP		X								
O.PUBLIC			X							
O.NOEVIL				X						
O.SINGEN					X					
O.ESECFUN						X				
O.NOREMO							X			
O.PHYSEC								X		
O.GENPUR									X	
O.DIRECT										X

8.3 Rational for Modified Assumptions for Environment

209 Three security environment assumptions described in the ALFPP (A.PHYSEC, A.GENPUR, and A.DIRECT) were modified in this ST. The refined assumptions are applicable to the architecture of this specific TOE while maintaining the intent of the PP.

8.4 Rationale For Security Requirements

210 The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this Security Target. Those security objectives imply probabilistic or permutational security mechanism and that the metrics defined are the minimal “industry” accepted (for the passwords) and government required (for the encryption) metrics they should be good enough for SOF-Basic.

FMT_SMR.1 Security roles

211 Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

212 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_UID.2 User identification before any action

213 This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.1 Timing of authentication

214 This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the authentication mechanism

chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_AFL.1 Authentication failure handling

215 This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After finite number of failures (determined by OSP and se by the authorized administrator), the user is prevented from further attempts to authenticate. This authentication for that user is suspended until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.4 Single-use authentication mechanisms

216 This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanism is of adequate cryptologic strength. This component traces back to and aids in meeting the following objective: O.SINUSE.

FIA_UAU.5 Multiple authentication mechanisms

217 This component was chosen to ensure that separate authentication mechanisms will be used to authenticate administrators of the TOE and users of the FTP and Telnet services. This component traces back to and aids in meeting the following objective: O.IDAUTH and O.SINUSE.

FDP_IFC.1 (1) Subset information flow control

218 This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP that are using all services except HTTP, SMTP, FTP, and Telnet (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 (1) Simple security attributes

219 This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP for all services except HTTP, SMTP, FTP and Telnet, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 (2) Subset information flow control

220 This component identifies the entities involved in the UNAUTHENTICATED_APPL information flow control SFP that are using the HTTP and SMTP services (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 (2) Simple security attributes

221 This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED_APPL SFP using the HTTP and SMTP services, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 (3) Subset information flow control

222 This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 (3) Simple security attributes

223 This component identifies the attributes of the users sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.1 Management of security attributes (1)

224 This component ensures the TSF enforces the UNAUTHENTICATED SFP to restrict the ability to change specified security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

225 This component ensures the TSF enforces the UNAUTHENTICATED_APPL SFP to restrict the ability to change specified security attributes that are listed in section

FDP_IFF1.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (3)

226 This component ensures the TSF enforces the AUTHENTICATED SFP to restrict the ability to change specified security attributes that are listed in section FDP_IFF1.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (4)

227 This component ensures the TSF enforces the UNAUTHENTICATED SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (5)

228 This component ensures the TSF enforces the UNAUTHENTICATED_APPL SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (6)

229 This component ensures the TSF enforces the AUTHENTICATED SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in FDP_IFF.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN

FMT_MSA.3 Static attribute initialization

230 This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT , O.SECSTA, and O.SECFUN.

FMT_MTD.1 Management of TSF data (1)

231 This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN

FMT_MTD.1 Management of TSF data (2)

232 This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data

233 This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Full residual information protection

234 This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FPT_RVM.1 Non-bypassability of the TSP

235 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

236 This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

237 FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

238 This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

239 This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review (1)

240 This component ensures that a variety of searches can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review (2)

241 This component ensures that a variety of sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

242 This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

243 This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be

recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FMT_MOF.1 (1) Management of security functions behavior (1)

244 This component was chosen to enable and disable the operation of the TOE and single use authentication functions. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.

FMT_MOF.1 (2) Management of security functions behavior (2)

245 This component was chosen to address audit trail management and back-up and restore capabilities provided by the TOE. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.ACCOUN.

Table 22: Mappings Between TOE Security Functions and IT Security Objectives

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN
FMT_SMR.1								X
FIA_ATD.1	X	X						
FIA_UID.2	X						X	
FIA_UAU.1	X	X						
FIA_AFL.1					X			
FIA_UAU.4		X						
FIA_UAU.5	X	X						
FDP_IFC.1(1)			X					
FDP_IFF.1(1)			X					
FDP_IFC.1(2)			X					
FDP_IFF.1(2)			X					
FDP_IFC.1(3)			X					
FDP_IFF.1(3)			X					
FMT_MSA.1 (1)			X	X				X
FMT_MSA.1 (2)			X	X				X
FMT_MSA.1 (3)			X	X				X
FMT_MSA.1 (4)			X	X				X
FMT_MSA.1 (5)			X	X				X
FMT_MSA.1 (6)			X	X				X
FMT_MSA.3			X	X				X
FMT_MTD.1 (1)								X
FMT_MTD.1 (2)								X
FMT_MTD.2								X
FDP_RIP.1			X					
FPT_RVM.1					X			
FPT_SEP.1					X			
FPT_STM.1						X		
FAU_GEN.1						X	X	
FAU_SAR.1						X		
FAU_SAR.3 (1)						X		
FAU_SAR.3 (2)						X		
FAU_STG.1					X			X
FAU_STG.4					X			X
FMT_MOF.1 (1)				X				X
FMT_MOF.1 (2)							X	X

8.5 Rationale For Assurance Requirements

246 EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing and vulnerability testing verification. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

8.6 Rationale for TOE Summary Specification

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

8.6.1 TOE Security Functions

248 The specified TOE security functions work together so as to satisfy the TOE security functional requirements. Table 23 provides a mapping of SFRs to the security functional requirements to show that all SFRs are captured within a security function.

Table 23: Mapping of SFRs to Security Functions

Security Function	Security Functional Requirement
Audit	FAU_GEN.1
	FAU_SAR.1
	FAU_SAR.3 (1)
	FAU_SAR.3 (2)
	FAU_STG.1
	FAU_STG.4
Identification & Authentication	FIA_AFL.1
	FIA_ATD.1
	FIA_UAU.1
	FIA_UAU.4
	FIA_UAU.5
	FIA_UID.2
Security Management	FMT_MOF.1 (1)
	FMT_MOF.1 (2)
	FMT_MSA.1 (1)
	FMT_MSA.1 (2)
	FMT_MSA.1 (3)
	FMT_MSA.1 (4)
	FMT_MSA.1 (5)
	FMT_MSA.1 (6)
	FMT_MSA.3
	FMT_MTD.1 (1)
	FMT_MTD 1 (2)
	FMT_MTD.2
	FMT_SMR.1
Data Protection	FDP_IFC.1 (1)
	FDP_IFF.1 (1)
	FDP_IFC.1 (2)
	FDP_IFF.1 (2)
	FDP_IFC.1 (3)
	FDP_IFF.1 (3)
	FDP_RIP.1
Protection of Security Functions	FPT_RVM.1
	FPT_SEP.1
	FPT_STM.1

249 The following paragraphs briefly summarize which security functions implement specific functional requirements specified in Section 5.1.1, TOE Security Functional Requirements:

250 Component **FAU_GEN.1**, audit data generation, is implemented by the FireWall-1 and the NT operating system. The FireWall Module and the NT operating system produce the audit records necessary to meet this requirement. (FW1_AUDIT)

251 Component **FAU_SAR.1**, audit review, is accomplished via the graphic user interface (GUI) of the management server. The FireWall-1 GUI interface permits the administrator to view, search and sort the FireWall-1 generated audit files. Additionally,

the NT Event Viewer provides a graphical user interface for searching and sorting of the NT generated audit records. (FW1_AUDIT)

252 Component **FAU_SAR.3 (1) and (2)**, selectable audit review, is implemented through the FireWall-1 Log Viewer. This application with a graphical user interface provides a mechanism to search and sort the FireWall-1 generated audit records using all identified attributes. Additionally, the NT Event Viewer provides the same functionality for the NT audit records. (FW1_AUDIT).

253 Component **FAU_STG.1**, protected audit trail storage, is implemented by the NT identification and authentication mechanisms. Only authorized administrators are able to login to the firewall host. (FW1_INA; FW1_AUDIT)

254 Component **FAU_STG.4**, prevention of audit data loss, is implemented by FireWall-1 stopping the flow of packets when the allocated disk space has been reached and the firewall is unable to continue storing audit records. (FW1_AUDIT)

255 Component **FDP_IFC.1 (1)**, The UNAUTHENTICATED subset information flow control, is implemented by the Inspection Module which forms part of the Firewall Host. In addition, the Management Module will support this functionality by allowing the authorized administrator to configure the associated rule set. (FW1_UDP)

256 Component **FDP_IFC.1 (2)**, The UNAUTHENTICATED_APPL subset information flow control, is implemented by the Inspection Module which forms part of the Firewall Host. The HTTP and SMTP security servers (proxies) also play a role in enforcing this requirement. In addition, the Management Module will support this functionality by allowing the authorized administrator to configure the associated rule set. (FW1_UDP)

257 Component **FDP_IFC.1 (3)**, The AUTHENTICATED subset information flow control, is implemented by the Inspection Module which forms part of the Firewall Host. The FTP and Telnet security servers (proxies) also play a role in enforcing this requirement. In addition, the Management Module will support this functionality by allowing the authorized administrator to configure the associated rule set. (FW1_UDP)

258 Component **FDP_IFF.1 (1)**, The UNAUTHENTICATED simple security attributes is implemented by the Kernel subsystem. (FW1_UDP)

259 Component **FDP_IFF.1 (2)**, The UNAUTHENTICATED_APPL simple security attributes is implemented by the Kernel subsystem and the HTTP and SMTP security servers. (FW1_UDP)

260 Component **FDP_IFF.1 (3)**, The UNAUTHENTICATED simple security attributes is implemented by the Kernel subsystem and the FTP and Telnet security servers. (FW1_UDP)

261 Component **FDP_RIP.1**, full residual information protection, is implemented by the Kernel subsystem of the Firewall. The packet is intercepted by the FireWall Module and

the management of the packet through the Firewall Host ensures that this requirement is met. (FW1_UDP)

262 Component **FIA_AFL.1**, authentication failure handling functionality is provided by the FireWall-1 Security Servers when User Authentication has been implemented. A user's account is locked when a settable number of unsuccessful authentication attempts have been made. (FW1_INA)

263 Component **FIA_ATD.1**, user attribute definition associated with the authorized administrators is managed by the Management Server and the NT operating system. The user attributes associated with human users are maintained by the firewall's Management Module. (FW1_INA).

264 Component **FIA_UAU.1**, timing of authentication for the administrators will be provided by the NT identification and authentication mechanism. (FW1_INA)

265 Component **FIA_UAU.4**, single-use authentication mechanism functionality is provided by an SKEY implementation (FTP and Telnet). (FW1_INA)

266 Component **FIA_UAU.5**, multiple authentication mechanisms. The TOE identifies two separate authentication mechanisms. The NT authentication mechanisms is used to authenticate the administrator. A second authentication mechanism, S/Key, is used to authenticate user of the FTP and Telnet services. (FW1_INA)

267 Component **FIA_UID.2**, user identification before any action for the administrators is provided by the NT operating system. The SKEY authentication mechanism provides this functionality for the human users (FTP and Telnet). (FW1_INA).

268 Component **FMT_MOF.1 (1)**, management of security functions behavior has several security functions associated with this SFR. Both the NT operating system and the Management Module combine to provide this functionality. (FW1_SMAN)

269 Component **FMT_MOF.1 (2)**, management of security functions behavior has several security functions associated with this SFR. Both the NT operating system and the Management Module combine to provide this functionality. (FW1_SMAN)

270 Component **FMT_MSA.3** static attribute initialization functionality is provided by the TOE. Specific instructions are provided in the IGS documentation to ensure this requirement is met. (FW1_SMAN)

271 Component **FMT_SMR.1**, security roles, is provided by the NT operating system and the FireWall-1 Management Server. (FW1_SMAN)

272 Component **FPT_RVM.1**, non-bypassability of the TSP of the TOE s provided by the FireWall Module and the NT operating system. (FW1_PSF)

273 Component **FPT_SEP.1**, TSF domain separation is implemented by the TOE. Both the NT operating system and the FireWall Module combine to perform this security functionality. (FW1_PSF)

274 Component **FPT_STM.1**, Reliable time stamps is implemented by the NT operating system. The FireWall Module interfaces with NT to provide a reliable time stamp for the audit records. The TOE does not have physically separated components. (FW1_PSF)

275 Component **FMT_MSA.1 (1)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

276 Component **FMT_MSA.1 (2)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

277 Component **FMT_MSA.1 (3)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

278 Component **FMT_MSA.1 (4)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

279 Component **FMT_MSA.1 (5)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

280 Component **FMT_MSA.1 (6)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

281 Component **FMT_MTD.1 (1)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

282 Component **FMT_MTD.1 (2)** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

283 Component **FMT_MTD.2** management of security attributes is provided by the NT operating system and the Management Module. (FW1_SMAN)

8.6.2 TOE SOF Claims

284 The Strength of TOE function claims are both valid. The AFLPP and the TFFPP both require an overall SOF claim of SOF-basic. This is a requirement set by the authors of the PP. This ST is claiming conformance to both of these PPs and is therefore claiming the same SOF.

285 Additionally, the PP authors have provided specific metrics for both mechanisms that require a SOF claim. The identified metrics and SOF claim is commensurate with the EAL2 level of assurance.

286 If the rules specified in the TOE summary specification governing passwords are followed, the probability of guessing the password is less than one in one million. Also, the random number generator used to develop the SKEY password sets, complies with

the *"Statistical random number generator tests"* and the *"Continuous random number tests"* found in section 4.11.1 of FIPS PUB 140-1 [5]. This ensures that the SKEY implementation meets the requirements of the AVA_SOF.1 assurance requirement.

8.6.3 TOE Assurance Requirements

287 The TOE satisfies the SARs specified in the ALFPP. Section 5.2 of this document identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Testing, and Vulnerability Analysis measures applied by Check Point to satisfy the CC EAL2 assurance requirements. The following Table 24 illustrates the assurance measures compliance with the assurance requirements as stated in Section 5.2.

Table 24. Assurance Measure Compliance Matrix

	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ACM_CAP.2	✓					
ADO_DEL.1		✓				
ADO_IGS.1		✓				
ADV_FSP.1,			✓			
ADV_HLD.1,			✓			
ADV_RCR.1			✓			
AGD_ADM.1				✓		
AGD_USR.1				✓		
ATE_COV.1,					✓	
ATE_FUN.1					✓	
ATE_IND.2					✓	
AVA_SOF.1						✓
AVA_VLA.1						✓

8.7 Rational for PP Conformance

288 The ST is conformant to the ALFPP because it contains all the functional requirements with appropriate refinements and security objectives as identified in the ALFPP with the exceptions noted and justified in Section 7. As noted in Section 7, objectives, assumptions and requirements in addition to those identified in ALFPP were also identified in this ST.

289 The ALFPP identifies the same set of SFRs as the TFFPP. However, in many cases the refinement differs between the profiles. Where the refinement is different the SFR refinement was taken from the ALFPP, as this provides a more restrictive refinement. There is no conflict between the set of SFRs identified in either the ALFPP or the TFFPP.

290 Because the TFFPP contains a subset of the security functional requirements and all the assurance requirements of the ALFPP, the assumption is made that by showing compliance to the ALFPP, the TOE is also compliant with the TFFPP.

8.8 Rationale For SFR Dependencies

291 All dependencies identified in the CC have been met by this ST as evidenced by the following Table 25.

Table 25 SFR Dependency Satisfaction

Functional Component ID	Functional Component Name	Dependency(ies)	Satisfied
FAU_GEN.1	Audit data generation	FPT_STM.1	**YES**
FAU_SAR.1	Audit review	FAU_GEN.1	**YES**
FAU_SAR.3 (1)	Selectable audit review (1)	FAU_SAR.1	**YES**
FAU_SAR.3 (2)	Selectable audit review (2)	FAU_SAR.1	**YES**
FAU_STG.1	Protected audit trail storage	FAU_GEN.1	**YES**
FAU_STG.4	Prevention of audit data loss	FAU_STG.1	**YES**
FDP_IFC.1 (1)	Subset information flow control (1)	FDP_IFF.1	**YES**
FDP_IFC.1 (2)	Subset information flow control (2)	FDP_IFF.1	**YES**
FDP_IFC.1 (3)	Subset information flow control (3)	FDP_IFF.1	**YES**
FDP_IFF.1 (1)	Simple security attributes (1)	FDP_IFC.1 FMT_MSA.3	**YES** **YES**
FDP_IFF.1 (2)	Simple security attributes (2)	FDP_IFC.1 FMT_MSA.3	**YES** **YES**
FDP_IFF.1 (3)	Simple security attributes (3)	FDP_IFC.1 FMT_MSA.3	**YES** **YES**
FDP_RIP.1	Subset residual information protection	NONE	NA
FIA_AFL.1	Authentication failure handling	FIA_UAU.1	**YES**
FIA_ATD.1	User attribute definition	NONE	NA
FIA_UAU.1	Timing of authentication	FIA_UID.1	**YES**
FIA_UAU.4	Single-use authentication mechanisms	NONE	NA
FIA_UID.2	User identification before any action	NONE	NA
FMT_MOF.1	Management of security functions behavior (1)	FMT_SMR.1	**YES**
FMT_MOF.1	Management of security functions behavior (2)	FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (1)	Management of security attributes (1)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (2)	Management of security attributes (2)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (3)	Management of security attributes (3)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (4)	Management of security attributes (4)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (5)	Management of security attributes (5)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.1 (6)	Management of security attributes (6)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	**YES** **YES**

Functional Component ID	Functional Component Name	Dependency(ies)	Satisfied
FMT_MTD.1	Management of TSF data (1)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MTD.1	Management of TSF data (2)	FDP_IFC.1 FMT_SMR.1	**YES** **YES**
FMT_MTD.2	Management of limits on TSF data	FMT_SMR.1	**YES**
FMT_SMR.1	Security roles	FIA_UID.1	**YES**
FPT_RVM.1	Non-bypassability of the TSP	NONE	NA
FPT_SEP.1	TSF domain separation	NONE	NA
FPT_STM.1	Reliable time stamps	NONE	NA

8.9 Internal Consistency and Mutually Supportive Rationale

292 The set of security requirements provided in this ST for the FireWall-1 form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.4 and 8.5. The choice of SFR and SARs were made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. This ST provides evidence the security objectives counter threats to the TOE (Table 20), and also, the assumptions and objectives counter threats to the TOE environment (Table 21).

b) The security functions of FireWall-1 satisfy the SFRs as shown in Table 23. All SFR dependencies have been satisfied as shown in Table 25.

c) The SOF claims are valid and are satisfied as shown in Section 8.6.2. The AFLPP and the TFFPP both require an overall SOF claim of SOF-basic. The PP authors have provided specific metrics for both mechanisms that require a SOF claim. The identified metrics and SOF claim is commensurate with the EAL2 level of assurance.

d) The SARs are appropriate for the assurance level of EAL2 and are satisfied by FireWall-1 as shown in Table 24. EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor.