Common Criteria EAL4 Evaluation

Nortel Networks.
Alteon Switched Firewall (Version 2.0.3.0)
Security Target 1.2

Brad Black
Senior Network Engineer
Nortel Networks
PO Box 3511, Station C
Ottawa, Ontario
CANADA
K1Y 4H7
email: brad@nortelnetworks.com

Radha Sethuraman
Product Manager
Nortel Networks
4655 Great America Parkway
Santa Clara, California
USA
95054
email: rad@nortelnetworks.com

Contents

Revision History

Issue	Date	Author	Comments
0.0A	18-07-02	P. Taylor	Initial Draft prepared for discussion with Nortel.
0.0B	23-07-02	P. Taylor	First revision to provide overview to the CB
0.0C	28-08-02	P. Taylor	Third draft for Nortel review
1.0	05-09-02	P. Taylor	Issue for release to evaluators and to Certification Body
1.1	10-03-03	P. Taylor	Revised in response to ORs and re-issue of [VPN1/FW1-ST]
1.2	03-06-03	P. Taylor	Revised in response to CB review

References

[CC]	Common Criteria for Information Technology Security Evaluation Parts 1-3, CCIMB-99-031, 032 and 033, Version 2.1, August 1999
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM-99/045, Version 1.0, August 1999
[CC-Install]	Addendum: Alteon Switched Firewall, Release 2.0.3, Part No. 215287-A Rev 01, May 2003, Nortel Networks – Common Criteria Alteon Switched Firewall Software.
[GUIDE]	Installation and User Guide Alteon Switched Firewall Release 2.0.3, Part No: 212535-C, October 2002, Nortel Networks.
[REL-NOTES]	Release Notes: Alteon Switched Firewall, Version 2.0.3, Part No: 213028-E, November 2002, Nortel Networks.
[GET-START]	Check Point Getting Started Guide NG FP3, September 2002 Part No: 700510, Check Point Software Technologies Ltd.
[CPMANAGEMENT]	Check Point SmartCenter Guide NG FP3, September 2002 Part No: 700526, Check Point Software Technologies Ltd.
[CP-VPN]	Check Point Virtual Private Networks Guide NG FP3, September 2002 Part No: 700528, Check Point Software Technologies Ltd.
[VPN1/FW1-ST]	Common Criteria EAL4 Evaluation VPN-1/Firewall-1 Next Generation (Feature Pack 1) Security Target Issue 1.8, 24 February 2003, Check Point Software Technologies Ltd.

Abbreviations

ASF	Alteon Switched Firewall
NAAP	Nortel Appliance Acceleration Protocol
SFA	Switched Firewall Accelerator
SFD	Switched Firewall Director
SIC	Secure Internal Communication
VLAN	Virtual Local Area Network
VNIC	Virtual Network Interface Card
VPN	Virtual Private Network

1. ST Introduction

1.1 ST Identification

Title:	Common Criteria EAL4 Evaluation Nortel Networks Alteon Switched Firewall (Version 2.0.3.0).
Target of Evaluation (TOE):	Alteon Switched Firewall (Version 2.0.3.0) with Check Point NG FP3.
Version of Components:	Switched Firewall Director (for Models 5010, 5008) including Check Point VPN-1/Firewall-1 NG FP 3 Firewall Module, Firewall OS Alteon SFA (for Models 5700, 5600, 5400, 5300) including Accelerator OS
Hardware Platforms:	Switched Firewall Director (Models 5010, 5008) Alteon SFA (Models 5700, 5600, 5400, 5300)

An Alteon Switched Firewall (ASF) requires that an SFD component be paired with a compatible SFA component as indicated by the table below:

ASF	SFD	SFA
5308	5008	5300
5408	5008	5400
5610	5010	5600
5710	5010	5700

1 This document serves as the Security Target (ST) for the EAL4 Common Criteria evaluation of the Nortel Networks Alteon Switched Firewall Version 2.0.3.0, hereafter referred to as ‘the product’.

2 For convenience, throughout this document the words ‘he’, ‘his’ etc. are intended to represent ‘he or she’, ‘his or hers’ etc.

3 Specific terms presented in *italic* font are defined in Annex A.

4 It should be noted that a major part of the security enforcing functionality of this product is provided by the Check Point VPN-1/Firewall-1 NG FP3 Firewall Module. This is a component of the Check Point VPN-1/Firewall-1 NG FP3 product, manufactured by Check Point Software Technologies Ltd. Future occurrences in this document of the term ‘Firewall-1 NG Module’ and ‘Check Point’ should be interpreted as references to this product and its manufacturer, as incorporated within the ASF product.

1.2 ST Overview

1.2.1 Introduction

5 Readers are assumed to be familiar with general computer security and evaluation terms and concepts; in particular, those described in [CC] and [CEM].

6 Readers are also assumed to be familiar with basic networking, Internet, TCP/IP terms and concepts.

1.2.2 Overview

7 The Alteon Switched Firewall (ASF) is a high-performance firewall system for network security. The system uses a versatile, multi-component approach to deliver accelerated firewall processing power.

8 A basic system cluster is composed of a Switched Firewall Director (SFD) and a Switched Firewall Accelerator (SFA). The SFD is an SFD 5010 or 5008 with Firewall OS and Check Point Firewall-1 NG FP3 software, which handles firewall policies and inspects network traffic. The SFA is an Alteon SFA 5700, 5600, 5400 or 5300 switch with Accelerator OS software, which offloads the processing of secured traffic and speeds up firewall performance.

9 The Check Point Firewall-1 NG Module is a stateful inspection firewall. It supervises the traffic passing between networks physically connected to the product and belonging to the complete “IP” family of protocols. Supervision is based on information contained in protocol headers and the product’s computer system, including state information derived from one or more associated packets.

10 The Check Point Firewall-1 NG Module is a component of the Alteon Switched Firewall which does policy checking for every new connection request, manages the connection table and specifies the rules for handling subsequent packets in a session. Once a session is active, the policy checking for packets is handled by the SFA. Thus, after the SFD inspection engine accepts the setup packets in a session, subsequent packets belonging to the session are inspected by the SFA without the involvement of the SFD. This solution achieves a tremendous improvement in firewall performance, because approximately 90% of the data can be switched at wire speed.

11 The product is configured and generally administered by means of a remote connection to a Check Point VPN-1/Firewall-1 NG Management Server and Management GUI. (Note these are further components of the Check Point firewall product). This connection is protected by encryption.

1.3 CC Conformance

12 The ST is Part 2 extended with respect to the functional requirements in Section 5, and is Part 3 conformant with respect to the assurance requirements (EAL4) identified in [CC] Part 3. The structure of this ST is in accordance with [CC], and is as follows:

a) Section 1 is this introduction.

b) Section 2 describes the TOE.

c) Section 3 describes the TOE security environment.

d) Section 4 provides the security objectives.

e) Section 5 provides the IT security requirements.

f) Section 6 provides the TOE summary specification.

g) Section 7 specifies any Protection Profile claims.

h) Section 8 provides the TOE rationale.

2. TOE Description

13 The Alteon Switched Firewall supports the capability for providing controlled connections between untrusted and trusted networks, based upon the use of the

Check Point Firewall-1 NG product. The evaluated configuration of the TOE consists of:

- an Alteon Switched Firewall (ASF) composed of a single Switched Firewall Director (SFD) connected to a single Switched Firewall Accelerator (SFA) in accordance with the instructions provided in the User Guidance [GUIDE], [REL-NOTES] and [CC-Install]. The ASF itself requires some local configuration, such as associating networks with specific hardware ports of the SFA, prior to the installation of a Firewall Security Policy. Establishing this local configuration is achieved using a local terminal connected via a serial interface. One aspect of the local configuration enables the use of remote connections via a SSH or a SSL and a browser to inspect and modify this local configuration of the ASF, although it should be noted that this mode of operation is not covered by the evaluated configuration.
- a connection to a trusted network that hosts a compatible Check Point VPN-1/Firewall-1 NG FP3 Management Server and Check Point VPN-1/Firewall-1 NG FP3 Management GUI. The connection between the ASF and Check Point Management Components is via the Check Point Secure Internal Communication (SIC) Functionality. The SIC connection is established in accordance with the instructions provided in [GUIDE] and [CPMANAGEMENT]. The Check Point Firewall-1 Management components are used to configure policies and monitor the status of the TOE in accordance with the instructions provided in [CPMANAGEMENT].
- physical connections to trusted and untrusted networks established via the remaining unallocated ports on the SFA, configured in accordance with the instructions provided in [GUIDE] and [REL-NOTES].
- if the Firewall Security Policy identifies the use of these; external directory, authentication or content checking services, either located upon a locally accessed trusted network or accessed via VPN connection to a trusted network.

14 NOTE: The Checkpoint Management Components do not form part of the TOE. However policy, status and log data is exchanged with these in accordance with Check Point interface definitions.

15 The Alteon Switched Firewall is distributed between two hardware platforms, the Switched Firewall Director (SFD) and the Switched Firewall Accelerator (SFA). Both of these platforms are packaged for installation into a standard rack.

16 The hardware platforms that host the SFD and the SFA are both generic components that are customised by software to provide the Firewall Security Functions. The SFD is hosted upon a standard x86 based PC (Dell Model 1650), whilst the SFA is hosted upon a Nortel proprietary “intelligent switch”. The hardware is relied upon to operate correctly in order to support all of the functionality of the product, including the security enforcing functionality. All of the security enforcing functionality arises from how the hardware is driven by the software installed upon it, so that failure of the hardware would not compromise the security provided by the TOE but result in a general failure to provide the functions of the ASF product.

17 In the SFD, the Check Point Firewall Module and Nortel software for managing the configuration of the ASF and for implementing the interface to the SFA run upon Firewall OS, which is a customised build of the Linux OS with security clampdown. The SFD has the following hardware interfaces:

1. CD ROM and Floppy Disk drives, located behind a lockable bezel. The CD-ROM drive is used to install the TOE, see [CC-Install].
2. A serial port, via which a terminal or a terminal emulator can be connected to provide access for configuring the ASF via a Unix style command line.
3. Connections for a keyboard and a monitor, which provide an alternative to the serial port for local access to the ASF.
4. For the 5010, a high speed (1000Base-SX Gigabit Ethernet) fibre-optic port used to provide the physical connection with a compatible SFA component.
5. For the 5008, a high-speed (10/100Base-T) copper ethernet port is used to provide the physical connection with a compatible SFA component.

18 The SFA supports the physical connection to the communication networks and incorporates hardware and software for handling the physical network connections and for implementing the accelerated connections. The SFA supports the following connections.

- For the SFA 5700 and the 5600, a set of 9 paired Ethernet ports, each pair consisting of a 10/100Base-T copper Ethernet port and a 1000Base-SX Gigabit fibre-optic Ethernet port. The preferred connectivity is via the fast optical cable, but the copper cable can be used in a primary or a backup role i.e. either one or both ports in a pair can be used but, if live, the optical port will be the port monitored.
- For the SFA 5400 and 5300, 8 10/100Base-T copper Ethernet ports and a single 1000Base-SX Gigabit fibre-optic Ethernet port, used only for connections to a second SFA in high availability configurations.

By default, the first 5 ports are used to provide connections to those networks, whose traffic the ASF mediates, and the remaining 4 ports are used to connect to SFD and SFA components in a local network. (In the most general Alteon Switched Firewall configuration for reliability and throughput, a local network of SFDs and SFAs may be employed, and these can all be accessed and configured via a single Master IP address, the MIP)

19 The logical connection between the SFD and SFA is maintained by means of the bespoke Nortel Appliance Acceleration Protocol (NAAP).

20 An Alteon Switched Firewall, e.g. a configured SFD and SFA pair, acts as a single extremely high performance Check Point Firewall-1 NG Module. In configuring the ASF, each physical port is associated with a set of Virtual Local Area Networks (VLAN) and for the processing of the connections by the Check Point firewall, the VLANs are in turn associated with Virtual Network Interface Cards (VNIC).

21 When an ASF is operating in a non-accelerating mode, the SFA component effectively acts as a network interface to the Check Point Firewall-1 NG Module hosted upon the SFD. The SFA detects the IP packets arriving at the hardware ports, assigns them to a VLAN and sends them encapsulated via NAAP to the SFD for processing. At the SFD the packet is assigned to a VNIC from which it is received by the firewall module. If the firewall does not block or drop the packet, it will be transmitted forward via the appropriate VNIC and the SFD will assign the ongoing packet to a VLAN and send it via NAAP to the SFA. Here the packet will be transmitted by the appropriate physical port to its next destination.

22 When an ASF is operating in accelerated mode, the SFA component is able to process directly IP packets that have already been assigned to a connection validated by the Check Point Firewall-1 NG Module. To achieve this, the SFA implements a copy of the firewall module's connection table. The connection table specifies for an active connection the constraints and transformations which must be applied in relation to the IP traffic associated with that connection, i.e. the stateful inspection. Thus where a connection has been validated, the SFA performs stateful inspection using its own copy of the table. An IP packet that initiates a session cannot be associated with a validated connection, therefore it is forwarded to the SFD and thence to the Check Point Firewall-1 NG Module as with no acceleration. If the firewall policies allow the connection to be established, then connection table information will be returned to the SFA allowing for the acceleration of the subsequent packets associated with that connection. Finally when packets are received indicating termination of a connection (e.g. TCP SYN/FIN/RST), these are also directed to the Firewall-1 NG Module so that connections can be dropped and synchronised connection tables maintained between each of the components of the ASF. Also the occurrence of default timeout values assigned to TCP or UDP sessions can cause connection table entries to be removed.

23 As noted above, the ASF implements an accelerated but otherwise standard Check Point Firewall-1 NG Module. Thus it supports the following functionality:

a) Control and Monitoring of the firewall module via commands originating from a Firewall Management server. This includes ability to:

- Start/Stop the Firewall;
- Elicit status reports from the Firewall;
- Install and revise the Firewall Security Policy enforced at the Firewall.

b) Implementing Firewall Policies that allow traffic through the Firewall to be allowed or blocked on the basis of origin and /or destination of the packet and service requested.

c) Implementing Firewall Policies for active and passive NAT translation.

d) Detecting and blocking Spoofing attacks.

e) Detecting and blocking IP fragmentation and source routing attacks.

f) Supporting VPN connections to external VPN clients.

g) Implementing a Security Server for:

- Authentication of connections for the telnet/ftp protocols, inputing user details provided via a LDAP interface;
- CVP protocol for active examination of content.

h) Generation of log reports and alerts as specified by policies and forwarding the log reports to a management server.

i) Establishing an authenticated and encrypted communication channel between the TOE and the Check Point Management Server by means of the Secure Internal Communication (SIC) functionality.

2.1 TOE Exclusions

24 Remote administration of the local configuration of the ASF hardware by the SSH, telnet or browser based interfaces is not included in the scope of the evaluation.

25 Configurations of the SFA that bypass inspection by the Firewall module are not included in the scope of the evaluation. These include:

- Configuration of port filters.
- Configuration of multiple IP interfaces on ports that share a VLAN.

26 ASF configurations where the local network consists of more than a single SFD and SFA assigned to a single MIP are not included in the scope of the evaluation.

27 The authentication of end-users which allows an administrator to grant users access privileges to specific client services (please see discussion of Security Function [AC10] later in this document) is to be evaluated to the interface level only; the actual authentication mechanism is not included in the scope of the evaluation.

28 Also, in the case of the Security Server, the Security Server functionality only is part of the TOE. That is, the evaluation is not concerned with the actual services that the Security Server is used to arbitrate requests for.

3. TOE Security Environment

3.1 Assumptions

3.1.1 Introduction

29 This section presents the TOE security environment assumptions either as ‘environmental’ assumptions, labelled [E_…], or as ‘ method of use’ assumptions, labelled [M_..]. The reader should consult with ASF Installation and User Guide [GUIDE], VPN-1/FireWall-1 Next Generation Getting Started Guide [GET-START] and Check Point Next Generation Virtual Private Networks [CP-VPN] for further information on the administrator’s interaction with the product.

3.1.2 Environment Assumptions

[E_AS1] The product, its users and environs comply with any applicable directives regarding physical, procedural or personnel security defined in the relevant site security policies.

[E_AS2] The product is being operated as an evaluated ‘trusted configuration’, where ‘trusted configuration’ is as defined in paragraph 13, and is adequately protected against physical threats (e.g. fire, flood, disruption to power supplies, temperature and humidity fluctuations, electromagnetic emanations).

[E_AS3] The computer system, associated devices and equipment function correctly.

[E_AS4] Any servers external to the TOE which the TOE consults for subscriber authentication or content analysis purposes are physically secure, protected by one or more CC EAL4 Certified firewalls (which are configured in accordance with [E_AS1]) and accessible only by authorised administrators.

3.1.3 Method of Use Assumptions

[M_AS1] The product is installed, configured, used and maintained in accordance with the procedures and guidelines defined in Installation and User Guide for Alteon Switched Firewall [GUIDE] and associated documents [REL-NOTES], [CC-Install], [GET-START] and [CPMANAGEMENT] in particular:

a) the correct version of the product is installed

b) IP Forwarding is enabled in the product’s computer system only when the product is running.

c) the *FireWall Security Policy* for the VPN-1/Firewall-1 Modules has been manually verified by an administrator

d) appropriate audit event logging and alerts have been defined, and the audit logs are regularly examined, to enable adequate and timely detection of attempted security breaches.

[M_AS2] the product is configured with the minimum of operating system features installed and the minimum of operating system features enabled to permit operation of the product i.e. the stripped down customised version of Linux is maintained.

[M_AS3] computer system privileges are assigned to programs in accordance with the site security policy.

[M_AS4] physical security controls prevent unauthorised access to the product, Management Server or consoles and system devices.

[M_AS5] the product is configured with user accounts only for authorised administrators and no end-user accounts are provided.

[M_AS6] the administrators’ use of privileged accounts conforms to the site security policy.

[M_AS7] restrictions imposed by relevant security policies concerning the choice of system password are enforced by the computer system configuration.

[M_AS8] guidelines consistent with the site security policy are followed for operating system controlled ownership and restrictions on access to operating system and product directories and files, especially those relating to the product’s security databases.

[M_AS9] computer system backup and recovery procedures are followed, which are sufficient to enable the product to be restored to a secure state after a failure of the product.

[M_AS10] appropriate use is made of the Management Server’s facilities to examine the audit log file and associated file system sizes, to periodically close the current audit log file and switch to a new audit log file, and if necessary to stop the product, such that audit records are not lost when file or file system size limits are reached and the product is stopped if it is unable to continue recording audit events.

[M_AS11] the product or FireWall Security Policy will be configured to deny all network connections aimed directly at the firewall host, except from the Management Server.

[M_AS12] administrators have knowledge of the product, the Linux operating system and networking technologies, and remain current with new developments in these technologies, specifically IP, IP protocols (for example, TCP, UDP, RPC, ICMP), and services (for example, FTP, Telnet, HTTP and others).

3.1.4 Threats

30 The statements labelled [Tn] identify the security threats that the product is designed to counter. Each of these threats represent attempts by persons external or internal to the organisation, owning an instance of the TOE, to obtain unauthorised access to data or services hosted on the network owned by that organisation. The attacks are envisaged as being from a low level of sophistication, where persons either intentionally or accidentally may attempt using standard interfaces to access network assets. Alternatively, attacks may also be at a moderate level of sophistication, where low level tools relating to the IP protocols may be used to generate network traffic or modify legitimate network traffic in attempts to access network assets.

31 The threats are as follows:

[T1] a host on one of the physically connected networks may attempt to establish unauthorised communications with a host on another physically connected network

[T2] a host on one of the physically connected networks may attempt to access services on another physically connected network that are not intended to be available

[T3] a person on the *external* network may attempt to gain access to one of the physically connected *internal* networks by employing *network address spoofing* attacks

[T4] a person on the *external* network may attempt to gain access to one of the physically connected *internal* networks by employing *IP source routing* attacks

[T5] a person on the *external* network may attempt to gain access to one of the physically connected *internal* networks by employing IP packet fragmentation attacks

[T6] attempts to establish communications with the product or via the product between physically connected networks, which may lead to a breach of the product's security policy, may not be detected in a timely manner

[T7] a person on the *external* network may generate enough auditable events to overload the audit logging mechanism thus preventing the correct audit of future activity

[T8] unauthorised disclosure of information being transmitted between an instance of the product and a *VPN enabled client.*

[T9] undetected attempts to modify the contents of data being transmitted between an instance of the product and a *VPN enabled client*

[T10] attempts by unauthorised users to bypass defined subscriber authentication measures

[T11] the establishment of connections which bypass defined packet content analysis measures

[T12] attempts to exploit extended periods when the product:

a) has failed

b) has not been updated with a new *FireWall Security Policy*

c) is experiencing difficulties communicating with the Management Server

[T13] unauthorised disclosure of information being transmitted between the product and the Management Server

[T14] undetected attempts to modify the contents of data being transmitted between the product and the Management Server.

3.2 Organisational Security Policies

32 There is no requirement for the TOE to comply with any organisational security policy statements or rules.

4. Security Objectives

4.1 Security Objectives for the TOE

33 The TOE security objectives [SOn] for the evaluation of the product are:

[SO1] provide controlled access between physically connected networks by permitting or denying the flow of packets

[SO2] translate between selected invalid IP addresses on *internal* networks and valid IP addresses

[SO3] *hide* selected IP addresses on *internal* networks from the *external* network

[SO4] provide the capability to generate audit logs and alerts for all attempts to communicate between physically connected networks

[SO5] invoke a Secure Internal Communications (SIC) facility for communication between the product and Check Point Management Server

[SO6] invoke a Virtual Private Network (VPN) facility for communication between the product and a *VPN enabled client*

[SO7] invoke the use of services that can enforce the authentication of a user and/or validate or filter data, such that all information flows are handled according to the *FireWall Security Policy*

[SO8] participate in real-time monitoring of the product.

4.2 Security Objectives for the Environment

34 The environmental objectives identified in this section are formulated to ensure that the TOE is operated in a “secure manner”, and specifically in accordance with the ‘environmental’ and ‘method of use’ assumptions identified in section 3.1. These environmental security objectives must be met by the establishment and

implementation of policies and procedures for the installation and operation of the TOE.

[ESO1] The functionality provided by the environment includes that the product has to be used in a 'trusted configuration' (as defined in paragraph 13). (The detail of [E_AS2], [E_AS3], [M_AS1], [M_AS2], [M_AS11] is understood to be implicit in this objective).

[ESO2] It is necessary that a comprehensive security policy is established for the environments (and in particular all sites) 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:

a) physical security - to restrict physical access to areas containing the product and associated equipment and protect physical resources, including media and hardcopy material, from unauthorised access, theft or deliberate damage

b) procedural security - to control the use of the product and associated equipment, and information stored and processed by the product, including use of the product's security features and physical handling of information

c) personnel security - to limit a user's access to the product 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.

(The detail of [E_AS1], [E_AS2], [E_AS4], [M_AS1], [M_AS3], [M_AS4], [M_AS5], [M_AS6], [M_AS7], [M_AS8], [M_AS9], [M_AS10], [M_AS11] and [M_AS12] is understood to be implicit in this objective).

[ESO3] Provide a Secure Internal Communications (SIC) facility which is used to establish trust and secure communication between the product and a Check Point Management Server via the implementation of internal certificates for authentication and standards based TLS for encryption.

[ESO4] Provide confidentiality and integrity of data (and authentication of the connected firewalls) between the product and a *VPN enabled client*, through the implementation of *symmetric* and *asymmetric encryption* and *message digesting*.

[ESO5] Provide services that can enforce the authentication of a user and/or validate or filter data, and ensure secure communication with the services, such that all information flows are handled according to the *FireWall Security Policy*.

[ESO6] Provide a reliable time stamping mechanism.

35 Application Note: In addressing the environmental objectives (specifically [ES01], [ES02] and [ES06]) it should be noted in respect to the TOE, namely the ASF product, that the SFD is the platform hosting the Firewall-1 Module. The SFD has been selected and configured to ensure that the security assumptions required for the environment of the Firewall-1 Module are achieved. These assumptions are in respect to both local properties of the platform and the underlying interface provided to the network. Specifically:

a) The only user accounts configured on the operating environment (Linux) implemented in the TOE are accounts required for the local administration of the platform. Prior to the provision of any local access by administrators to the TOE function, password based authentication of user logon is enforced.

b) The operating environment (Linux) implemented in the TOE provides the underlying services required to execute the processes of the Firewall-1 Module. Notably the operating environment provides an API to the local platform clock, via which time stamps are provided to the Firewall-1 Module for accounting log records. Administrators locally logged on to the platform can use a command line interface to set the local clock.

c) The product provides a hardened operating environment (Linux), with the minimal services installed necessary to support the operation of the TOE. Specifically the TOE, on boot, will have:

- only those network services enabled required to allow its initialisation as part of a networked Check Point VPN-1/Firewall-1 configuration.
- IP-Forwarding disabled.

The assumption of competent management of the TOE identified in [M_AS1] requires that administrators do not modify the configuration of the platform in ways that would compromise the secure settings.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

36 The table below, Table 5-1, identifies the Security Functional Requirements claimed by the TOE. The majority of these requirements are derived from the requirements presented in [CC] Part 2. In the statement of the requirements, text in square brackets represents specific instantiation of the associated Part 2 requirement. Explicitly stated requirements are labelled ‘(EXP)’.

37 As a consequence of the wide range of functionality provided by the TOE it has been necessary to have multiple instantiations of many of the SFRs. Different instances of SFRs are distinguished by a number in brackets and usually a descriptive comment, also in brackets, attached to their title. In Table 5.1 and in their statement the SFRs are grouped by means of the main areas of functionality claimed for the TOE.

SFR	Title (description)
FDP_IFC.1 (1)	Subset information flow control (Firewall Security Policy)
FDP_IFF.1 (1)	Simple security attributes (Firewall Security Policy)
FMT_MSA.1 (1)	Management of security attributes (Firewall Security Policy)
FMT_MSA.3 (1)	Static attribute initialization (Firewall Security Policy)
FPT_RVM.1	Non-bypassability of the TSP
EDP_ITT.1(1)(EXP)	Invocation of internal transfer protection (SIC)
EDP_ITT.1(2)(EXP)	Invocation of internal transfer protection (VPN)
FMT_MOF.1 (1)	Management of security functions behaviour (Firewall Components)
FMT_MSA.1 (2)	Management of security attributes (Remote Monitoring)
FAU_GEN.1	Audit data generation

SFR	Title (description)
FAU_SAA.1	Potential violation analysis
FMT_MOF.1 (2)	Management of security functions behaviour (Audit)

Table 5-1 TOE Security Functional Requirements

38 It should be pointed out that the management related SFRs (FMT_MSA.1 (1), FMT_MOF.1 (1), FMT_MSA.1 (2), FMT_MOF.1 (2)) have been duplicated between the security requirements for the TOE and for the environment of the TOE, see section 5.4. This is to draw attention to the fact that management commands originate from the Check Point Management Server and GUI in the environment of the TOE whilst the TOE itself is required to respond correctly to management commands.

39 The TOE is associated with a number of different flow control and access control policies which regulate access to and through the TOE. In the presentation of the SFRs, this is modelled by means of a number of information flow and access control Security Function Policies (SFPs). In summary these are:

- The FIREWALL-SFP, which controls the flow of network traffic through a TOE.
- The SIC-SFP, which ensures that secure (TLS) connections are established between the TOE and the Management Server.
- The VPN-SFP, which ensures that secure (IPSec) connections can be established between the TOE and a *VPN enabled client.*

5.1.1 Flow Control VPN-1/Firewall Module

40 This section identifies the SFRs associated with the firewall function of the VPN-1/Firewall-1 Module, namely the capability to enforce *Firewall Security Policies* that have been defined at the Management Server, together with the associated standard information flow control measures specified in FDP_IFF.1.6 b) and FDP_IFF.1.6 c). The FIREWALL-SFP is the policy that models this aspect of information flow control.

5.1.1.1 FDP_IFC.1 (1) Subset information flow control (Firewall Security Policy)

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

a) [subjects: external IT entities that send and receive information through the TOE to one another (and TOE components, where FIREWALL-SFP supports the management of security attributes of other SFPs);

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

c) operation: pass information].

5.1.1.2 FDP_IFF.1 (1) Simple security attributes (Firewall Security Policy)

FDP_IFF.1.1 The TSF shall enforce the [FIREWALL-SFP] based on the following types of subject and information security attributes:

a) [subject security attributes:

- presumed address;

- user authentication credentials associated with the subject (only for the case where connection to a service via a Firewall requires authentication).

b) information security attributes:

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

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

a) [Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only 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; and
- the presumed address of the destination subject, in the information, translates to an address on some other connected network.]

FDP_IFF.1.3 The TSF shall enforce the

a) [rules that specify static or dynamic translation schemes for the IP address information, in respect to packets originating from or destined for specific subjects upon an internal network.;

b) rules that (on the basis of subject and information attributes, specifically in respect to the ftp, http and smtp services) permit the information flow if confirmation of the successful checking of the application level data content of the TCP/IP packets is received from an external content checking service invoked by the TOE;

c) rules that (in the case that the policy rule explicitly requires authentication for the connection) permit the information flow if confirmation of the successful authentication of the subscriber is received from an external authentication service invoked by the TOE.]

FDP_IFF.1.4 The TSF shall provide the following:

a) [the capability to modify the flow of TCP/IP packets in response to the validation or filtering performed by external servers supporting the content verification protocol.]

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules:

a) [None].

FDP_IFF.1.6 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 a TOE network interface, and the presumed address of the source subject is incompatible with the network addressing that the TOE has been configured to associate with that network interface;

b) The TOE shall drop IP packets that include a source routing option, and

c) The TOE shall reject fragment IP packets which cannot be reassembled within a bounded time interval into a single consistent IP packet.]

5.1.1.3 FMT_MSA.1 (1) Management of security attributes (Firewall Security Policy)

FMT_MSA.1.1 The TSF shall enforce the [FIREWALL-SFP and SIC-SFP] to restrict the ability to [create and delete rules and delete attributes from a rule, modify attributes in a rule and add attributes to a rule] to the security attributes [the configurable flow control rules described in FDP_IFF.1(1)] to [the authorized administrator].

41 Application Note: The FIREWALL-SFP facilitates the creation, modification and deletion of firewall security policy rules. Also, as Firewall Module enforces the Firewall Security Policy pushed to it from a Management Server; the FIREWALL-SFP is providing protection against unauthorised network access to the platform hosting the Firewall Module, whilst the SIC-SFP is ensuring protected network access from the management server and to the Management Server from a Management GUI.

5.1.1.4 FMT_MSA.3 (1) Static attribute initialization (Firewall Security Policy)

FMT_MSA.3.1 The TSF shall enforce the [FIREWALL-SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

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

42 Application Note. The generic wording of the SFR must be related to the terms used by Check Point in describing the functionality of the product. ‘Restrictive default values’ refers to the product’s default firewall security policy (enforced during booting of the firewall) and the product’s initial firewall security policy (enforced prior to supply of a customised policy, if a customised policy is not resident prior to a reboot). ‘Alternative initial values’ refers to a customised firewall security policy.

5.1.1.5 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.

5.1.2 Flow Control Secure Internal Communication

43 This section identifies the SFRs associated with the flow control function in relation to the Secure Internal Communication (SIC) between the Management Server and the TOE. The SIC-SFP is the policy that models this aspect of information flow control. There is an environmental requirement for cryptographic functionality to enforce this policy. The TOE merely invokes the use of this functionality.

5.1.2.1 EDP_ITT.1 (1) (EXP) Invocation of internal transfer protection (SIC)

EDP_ITT.1.1 The TSF shall invoke the [SIC-SFP] to prevent the [disclosure or modification] of [traffic sent between the Management Server and the physically separated TOE].

44 Application Note. This explicit SFR is directly modelled on the [CC] Part 2 SFR FDP_ITT.1, and reflects the fact that TOE functionality only relates to the invocation of standards based protocols and cryptographic algorithms that underlie the information flow policy identified by SIC-SFP. Identification of these is provided in section 5.4.3

5.1.3 Flow Control VPN Connectivity

45 This section identifies the SFRs associated with the flow control function in relation to the Virtual Private Network (VPN) connections between the TOE and *VPN enabled clients*. The VPN-SFP is the policy that models this aspect of information flow control. There is an environmental requirement for cryptographic functionality to enforce this policy. The TOE merely invokes the use of this functionality.

5.1.3.1 EDP_ITT.1 (2) (EXP) Invocation of internal transfer protection (VPN)

EDP_ITT.1.1 The TSF shall invoke the [VPN-SFP] to prevent the [disclosure or modification] of [user data when it is transmitted the TOE and a physically separated *VPN enabled client.*]

46 Application Note. This explicit SFR is directly modelled on the [CC] Part 2 SFR FDP_ITT.1, and reflects the fact that TOE functionality only relates to the invocation of standards based protocols and cryptographic algorithms that underlie the information flow policy identified by VPN-SFP. Identification of these is provided in section 5.4.4

5.1.4 General Management Facilities

47 This section provides SFRs relating to the general management of the TOE.

5.1.4.1 FMT_MOF.1 (1) Management of security functions behaviour (Firewall Components)

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

a) [operation of the TOE]

to [an authorized administrator].

48 Application Note. The SIC-SFP ensures that access to the TOE is constrained to an authorized administrator.

5.1.4.2 FMT_MSA.1 (2) Management of security attributes (Remote Monitoring)

FMT_MSA.1.1 The TSF shall enforce the [SIC-SFP] to restrict the ability to [query] the security attributes [current operational status and active policy of the Firewall Module] to [the authorized administrator].

5.1.5 Audit

49 This section provides SFRs that identify the audit capabilities of the TOE.

5.1.5.1 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) Startup and shutdown of the audit function

b) all auditable events for the [not specified] level of audit: and

c) [Success or failure of attempts to establish a connection via the TSF.]

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, outcome (success or failure) of the event; and

b) For each audit event type, based upon the auditable event definitions of the functional components included in the PP/ST [for connection attempts, the product's host IP address, the network interface, the direction of packet flow].

5.1.5.2 FAU_SAA.1 Potential violation analysis

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

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

a) Accumulation or combination of [no such events specified] known to indicate a potential security violation.

b) [Audit events associated with selected rules in the Firewall which have been specified as giving rise to an alarm.]

5.1.5.3 FMT_MOF.1(2) Management of security functions behaviour (Audit)

FMT_MOF.1.1 The TSF shall restrict the ability to [determine and modify the behaviour of] the functions:

a) [audit record generation]

to [an authorized administrator].

5.2 TOE Strength of Function Claim

5.2.1 Statement of SOF Claims

50 The TOE itself contains no functions for which a Strength of Function Claim is appropriate.

51 However the TOE is envisaged as being resistant to attack via attackers with a moderate attack potential, in that they can, using tools, manipulate the IP traffic at the packet level. On this basis a minimum Strength of Function claim of MEDIUM is appropriate.

5.3 TOE Security Assurance Requirements

5.3.1 Statement of Security Assurance Requirements

52 The security assurance requirements for the TOE comprise the requirements corresponding to the EAL4 level of assurance, as defined in [CC] Part 3. Table 5.2 below summarises the relevant requirements in terms of assurance components.

Assurance Class	Assurance Components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation Support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Table 5-2 TOE Assurance Components

53 Further information on the assurance components may be found in [CC] Part 3.

5.4 Security Requirements for the IT Environment

SFR	Title (description)
FMT_MSA.1 (3)	Management of security attributes (Firewall Security Policy)
FMT_MOF.1 (3)	Management of security functions behaviour (Audit)
FMT_MOF.1 (4)	Management of security functions behaviour (Firewall Components)
FMT_MSA.1 (4)	Management of security attributes (Remote Monitoring)

SFR	Title (description)
FTP_ITC.1(1)	Inter-TSF trusted channel (for connections to Content Verification Servers)
FDP_ITT.1 (1)	Basic internal transfer protection (SIC)
FDP_IFC.1 (2)	Subset information flow control (SIC)
FDP_IFF.1 (2)	Simple security attributes (SIC)
FCS_COP.1 (1)	Cryptographic Operation (SIC)
FDP_ITT.1 (2)	Basic internal transfer protection (VPN)
FDP_IFC.1 (3)	Subset information flow control (VPN)
FDP_IFF.1 (3)	Simple security attributes (VPN)
FCS_COP.1 (2)	Cryptographic Operation (VPN)
FIA_UAU.5	Multiple Authentication Mechanisms
FTP_ITC.1 (2)	Inter-TSF trusted channel (for X.500 directory connections)
FPT_STM.1	Reliable Time Stamps

Table 5-3 Security Functional Requirements for IT Environment

5.4.1 Management Facilities

54 This section provides SFRs relating to the general management of the TOE. These, as compared to [VPN1/FW1-ST], have been identified as environmental SFRs for the TOE in order to make clear the dependency upon a compatible Check Point Firewall-1 Management Server and Management GUI within the environment of the TOE. The management operations originate at the Server and GUI components. The TOE itself is required only to respond appropriately to these management operations.

5.4.1.1 FMT_MSA.1 (3) Management of security attributes (Firewall Security Policy)

FMT_MSA.1.1 The IT environment shall enforce the [FIREWALL-SFP and SIC-SFP] to restrict the ability to [create and delete rules and delete attributes from a rule, modify attributes in a rule and add attributes to a rule] to the security attributes [the configurable flow control rules described in FDP_IFF.1(1)] to [the authorized administrator].

55 Application Note: The FIREWALL-SFP facilitates the creation, modification and deletion of firewall security policy rules. Also, as Firewall Module enforces the Firewall Security Policy pushed to it from a Management Server; the FIREWALL-SFP is providing protection against unauthorised network access to the platform hosting the Firewall Module, whilst the SIC-SFP is ensuring protected network access from the management server and to the Management Server from a Management GUI.

5.4.1.2 FMT_MOF.1(3) Management of security functions behaviour (Audit)

FMT_MOF.1.1 The IT environment shall restrict the ability to [determine and modify the behaviour of] the functions:

a) [audit record generation

b) switching of audit logs]

to [an authorized administrator].

56 Application Note: The wording of this environment SFR differs from that of the corresponding TOE SFR of section 5.1.5.3 by the addition of list item b), since storage and switching of the audit log is located with the Management Server.

5.4.1.3 FMT_MOF.1 (4) Management of security functions behaviour (Firewall Components)

FMT_MOF.1.1 The IT environment shall restrict the ability to [enable, disable] the functions:

a) [operation of the TOE]

to [an authorized administrator].

57 Application Note: The SIC-SFP ensures that access to the TOE is constrained to an authorized administrator.

5.4.1.4 FMT_MSA.1 (4) Management of security attributes (Remote Monitoring)

FMT_MSA.1.1 The IT environment shall enforce the [SIC-SFP] to restrict the ability to [query] the security attributes [current operational status and active policy of the Firewall Module] to [the authorized administrator].

5.4.2 Content Verification Services

5.4.2.1 FTP_ITC.1 (1) Inter-TSF trusted channel (for connections to Content Verification Servers)

FTP_ITC.1.1 The IT environment shall provide a communication channel between the TOE and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The IT environment shall permit [the TOE] to initiate communication via the trusted channel.

FTP_ITC.1.3 The IT environment shall initiate communication via the trusted channel for [communicating with a product compliant with the Content Vectoring Protocol being used to provide an external data content validation service (such as URL checking or virus checking)].

5.4.3 Flow Control Secure Internal Communication

58 The SFRs in this section relate to EDP_ITT.1.1 (1), and identify the standard protocols and cryptographic functions invoked by this SFR.

5.4.3.1 FDP_ITT.1 (1) Basic internal transfer protection (SIC)

FDP_ITT.1.1 The IT environment shall enforce the [SIC-SFP, via an implementation of the standard TLS protocol defined in RFC 2246] to prevent the [disclosure or modification] of user data when it is transmitted between physically-separated parts of the TOE

59 Application Note. The above use of FDP_ITT.1.1 provides consistency with [VPN1/FW1-ST] (i.e. for the Check Point VPN-1/Firewall-1 NG FP1 product, in which the Management Server is a physically-separated part of the TOE). However, since the ASF product incorporates only the Firewall Module, the communication is between the TOE and a physically-separated Management Server in the environment of the TOE.

5.4.3.2 FDP_IFC.1 (2) Subset information flow control (SIC)

FDP_IFC.1.1 The IT environment shall enforce the [SIC-SFP] on:

a) [subjects: Management Server and TOE;

b) information: traffic sent between the Management Server and the TOE; and

c) operation: establish and maintain trusted communication channel].

5.4.3.3 FDP_IFF.1 (2) Simple security attributes (SIC)

FDP_IFF.1.1 The IT environment shall enforce the [SIC-SFP] based on at least the following types of subject and information security attributes:

a) [subject security attributes:

- X.509 certificates installed upon the subjects]

b) information security attributes:[none].]

FDP_IFF.1.2 The IT environment shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [Subjects can cause information to flow through the subjects if based on the subjects certificates a trusted connection can be negotiated between the subjects via the TLS protocol]

FDP_IFF.1.3 The IT environment shall enforce [no additional information flow control rules].

FDP_IFF.1.4 The IT environment shall provide the following [None].

FDP_IFF.1.5 The IT environment shall explicitly authorise an information flow based on the following [None].

FDP_IFF.1.6 The IT environment shall explicitly deny an information flow based on the following rules: [None].

5.4.3.4 FCS_COP.1 (1) Cryptographic Operation (SIC)

FCS_COP.1.1 The IT environment shall perform [

- data encryption,
- cryptographic key agreement,
- authentication,
- message digesting]

in accordance with a specified cryptographic algorithm [

- data encryption : DES, 3-DES,
- cryptographic key agreement: Diffie-Hellman,

- digital signatures: RSA,
- message digesting: MD5]

and cryptographic key sizes [

- DES: 56-bit,
- 3-DES: 168-bit,
- RSA: 1024-bit]

that meet the following [

- DES: FIPS PUB 46-2,
- 3-DES: FIPS PUB 46-2,
- Diffie Hellman: PKCS #3,
- RSA: PKCS#1,
- MD5: RFC 1321].

5.4.4 Flow Control VPN Connectivity

60 The SFRs in this section relate to EDP_ITT.1.1 (2), and identify the standard protocols and cryptographic functions invoked by this SFR.

5.4.4.1 FDP_ITT.1 (2) Basic internal transfer protection (VPN)

FDP_ITT.1.1 The IT environment shall enforce the [VPN-SFP, via an implementation of the standard IPSec protocol defined at http://www.ietf.org/html.charters/ipsec-charter] to prevent the [disclosure or modification] of user data when it is transmitted between physically-separated parts of the TOE.

61 Application Note. The above use of FDP_ITT.1.1 provides consistency with [VPN1/FW1-ST] (i.e. for the Check Point VPN-1/Firewall-1 NG FP1 product, in which the *VPN enabled client* is a physically-separated part of the TOE). However, since the ASF product incorporates only the Firewall Module, the communication is between the TOE and a physically-separated *VPN enabled client* in the environment of the TOE.

5.4.4.2 FDP_IFC.1 (3) Subset information flow control (VPN)

FDP_IFC.1.1 The IT environment shall enforce the [VPN-SFP,] on:

a) [subjects: the TOE and *VPN enabled clients*;

b) information: traffic sent between subjects; and

c) operation: establish and maintain trusted communication channel].

5.4.4.3 FDP_IFF.1 (3) Simple security attributes (VPN)

FDP_IFF.1.1 The IT environment shall enforce the [VPN-SFP] based on at least the following types of subject and information security attributes:

a) [subject security attributes:

- a shared secret (password) installed out band upon a pair of communicating subjects, or;
- a signed X.509 certificate that can be associated with the subject.]

FDP_IFF.1.2 The IT environment shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [Subjects on distinct hosts connected via the network can cause information to flow between their hosts if via the IKE protocol the subjects' security attributes can be used to established an encrypted connection between the subjects via the IPSEC protocol.]

FDP_IFF.1.3 The IT environment shall enforce [no additional information flow control rules].

FDP_IFF.1.4 The IT environment shall provide the following [None].

FDP_IFF.1.5 The IT environment shall explicitly authorise an information flow based on the following [None].

FDP_IFF.1.6 The IT environment shall explicitly deny an information flow based on the following rules: [None].

5.4.4.4 FCS_COP.1 (2) Cryptographic Operation (VPN)

FCS_COP.1.1 The IT environment shall perform [

- data encryption,
- cryptographic key agreement,
- authentication,
- message digesting]

in accordance with a specified cryptographic algorithm [

- data encryption : DES, 3-DES, AES (128 and 256 bit)
- cryptographic key agreement: IKE,
- digital signatures: RSA,
- message digesting: HMAC-SHA-1, HMAC-MD5]

and cryptographic key sizes [

- DES: 56-bit,

- 3-DES: 168-bit,
- AES: 128 and 256 bit,
- RSA: 1024-bit
- HMAC-SHA-1: 20 byte,
- HMAC-MD5, 16 byte]

that meet the following [

- DES: FIPS PUB 46-2,
- 3-DES: FIPS PUB 46-2,
- AES: FIPS PUB 197,
- IKE: RFC 2409,
- RSA: PKCS#1,
- HMAC-SHA-1: RFC 2104, RFC 2404, FIPS PUB 180-1,
- HMAC-MD5: RFC 2104, RFC 2405, RFC 1321]

62 Application Note. AES 256 is not supported where the *VPN enabled client* has the Secure Remote software. The RSA 1024 bit constraint is consistent with the use of IKE mode 2 only.

5.4.5 Authentication Services

63 These services are required to support FDP_IFF.1 (1).

5.4.5.1 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The IT environment shall provide [an authentication checking service offering multiple authentication options] to support user authentication.

FIA_UAU.5.2 The IT environment shall authenticate any user's claimed identity according to the [following authentication checking rules.

The subscriber Id is supplied by the product to an LDAP compliant directory (database) which returns data that enables one of the following options:

a) identifies an external authentication service which authenticates the subscriber using the supplied Id

b) specifies that the product verify the password supplied by the subscriber

c) specifies that the product verify the digital signature of the certificate supplied by the subscriber].

Application Note: The VPN-1/Firewall-1 product functionality specified under b) and c) above is excluded from the evaluated TOE.

5.4.5.2 FTP_ITC.1(2) Inter-TSF trusted channel (for X.500 directory connections)

FTP_ITC.1.1 The IT environment shall provide a communication channel between the TOE and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The IT environment shall permit [the TOE] to initiate communication via the trusted channel.

FTP_ITC.1.3 The IT environment shall initiate communication via the trusted channel for [querying via the LDAP protocol an external X.500 database for the authentication method and credentials associated with a purported user.]

5.4.6 Audit

5.4.6.1 FPT_STM.1 Reliable Time Stamps

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

6. TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Introduction

64 This Section defines the product's security functions. Each section contains a set of labelled statements, one for each security function or sub-function.

65 The security functions specified in this Security Target are derived primarily from the following documents:

- Check Point Next Generation Smart Center Guide [CPMANAGEMENT].
- Alteon Switched Firewall Installation and User Guide [GUIDE]

66 The Alteon Switched Firewall includes in its SFD component a Check Point Firewall-1 module, which enables it to support the enforcement and logging functions required for the Firewall and VPN capabilities of the Firewall-1 Module. The SFA component is involved in security enforcing functionality in that certain ongoing checks are delegated to it once a connection has been approved and established by the Firewall module on the SFD.

67 The labelled statements are essentially those of [VPN1/FW1-ST], which continue to apply to the ASF since this includes a Check Point Firewall-1 module. Further information that interprets or elaborates these statements in the context of the ASF product is provided in the form of application notes to the Security Function.

6.1.2 Access Control

6.1.2.1 Access Control Administration

[AC1] The product shall provide the capability for administrators via a Check Point Management Server to:

a) start and stop the product

b) load the *FireWall Security Policy* onto the TOE

c) apply address translation rules.

These concepts may be described as follows:

"**Load**" means to create INSPECT code from the text representation of the FireWall Security Policy, to compile it and to place it on the firewall.

"**Stop**" means to leave the firewall in place so that packets must pass through the firewall but without any enforcement on them of the FireWall Security Policy. (No traffic is allowed to pass).

"**Start**" means to activate the firewall's security policy and begin FireWall Security Policy enforcement.

"**Address Translation rules**" are administrator-defined rules which map the actual IP addresses of hosts protected by the firewall to valid IP addresses; during FireWall Security Policy enforcement these mappings are applied to replace the address and port fields within packet headers

68 Application Note. The Firewall Module component of the SFD implements this functionality by receiving and responding to commands transmitted from the Check Point Management Server via the secure communication channel. The *Firewall Security Policy* will be a file containing INSPECT code, which is pushed from the Management Server to the SFD when a policy is installed and which will be loaded when the Firewall module is started. Note the Firewall Security Policy will be formulated in terms of the VNICs and VLANs, which will have been specified and related to the actual physical network interfaces of the ASF during the initial configuration of the product.

6.1.2.2 Traffic Flow Control

[AC2] The product shall enforce the *FireWall Security Policy* (including initial, default and customised policies) on the individual IP packets involved in all *operations* among subjects and objects covered by the *FireWall Security Policy*, where subject refers to the subscriber attempting to traverse the FireWall and object refers to the intended destination of the subscriber's attempt or request, e.g. the mail server protected and residing behind the FireWall.

[AC3] The product shall enforce the *FireWall Security Policy* based on items of *information* involved in an *operation* that are accessible to the product in accordance with the syntax and semantics of the VPN-1/FireWall-1 Language (INSPECT).

[AC4] The product shall enforce the *FireWall Security Policy* by taking one, and only one, of the following *actions* for each IP packet involved in an *operation*:

For the *FireWall Security Policy*:

a) "**Accept**" the IP packet flow between the subject and the object

b) "**Reject**" the IP packet flow between the subject and the object, notifying the subject

c) "**Drop**" the IP packet flow between the subject and the object, without notifying the subject.

69 Application Note.The Firewall Security Policy is enforced in the first instance by the Firewall-1 module on the SFD. However the TOE implements the Check Point SecureXL Architecture that allows Connection Table information created by the Firewall-1 module to be communicated to the SFA, following the initial validation of a new connection request, to enable acceleration of the subsequent IP packets associated with the connection.

6.1.2.3 Network Address Spoofing Protection

[AC5] The product shall have the capability for the administrator to create a filter associating particular interfaces with particular sets of network addresses, such that packets moving through an interface must have source and destination addresses which each conforms to the allowed set of networks for that interface and for the direction of movement (inbound or outbound) and will be dropped otherwise.

70 Application Note. The definition of the network topology and as a consequence the capability for defining spoofing conditions is part of the function provided by the Check Point Management GUI and Server with which the TOE communicates. This information will be included as part of the INSPECT file defining the Firewall Security Policy which is provided to the SFD by the Management server. To define the spoofing protection the administrator will need to be aware of the VLANs configured at the ASF, since the network connectivity at the ASF will be expressed in terms of these.

6.1.2.4 IP Source Routing Protection

[AC6] The product shall drop all IP packets that contain an *IP source routing* option.

6.1.2.5 Virtual Defragmentation

[AC7] The product shall temporarily reassemble IP fragments, before transmission of the original fragments, to ensure that:

a) there are no holes in the reassembled packets

b) no single byte in a reassembled packet has been written twice.

If such a problem is found the packet shall be rejected.

6.1.2.6 IP Address Translation

[AC8] The product shall provide the capability to translate between *IP addresses* on *internal* networks and *IP addresses* on *external* networks including valid *Internet IP addresses.*

[AC9] The product shall provide the capability to *hide* selected IP addresses on *internal* networks from subjects and objects on the *external* network, such that the *internal* networks' selected IP addresses are not visible to subjects and/or objects on the *external* network.

71 Application Note. The definition of NAT is part of the function provided by the Check Point Management GUI and Server with which the TOE communicates. This information will be included as part of the INSPECT file defining the Firewall

Security Policy which is provided to the SFD by the Management server. Determining whether there is an address translation requirement associated with a connection through the Firewall is one of the actions performed when the Firewall module validates the connection request. Address translation requires rewriting of the address *information* within the IP packets, when acceleration is enabled this transformation will be carried out by the SFA based on the entry in the connection table.

6.1.2.7 User Authentication

[AC10] The TOE shall provide the administrator with the capability to select subscriber authentication as an access control criterion. The decisions relating to the diversion of requests shall be made using the *FireWall Security Policy* and *information* relating to the subject.

[AC11] For the purpose of subscriber authentication, the TOE shall invoke an external server (which utilises an RFC 1777 and RFC 1778 compliant interface to services or 3rd party products which use LDAP).

72 Application Note. The user authentication functionality is implemented by the Security Server component which is part of the Firewall module located on the SFD. The ASF will direct connections requiring authentication to the SFD, where the standard processing of the connection will be performed by the Firewall module.

6.1.2.8 Data Filtering

[AC12] The TOE shall provide the administrator with the capability to have FTP, HTTP and SMTP based connections diverted to an interface for packet content analysis as a precondition for permitting information flow. The decisions relating to the diversion of connections shall be made using the *FireWall Security Policy* and *information* relating to the subject.

[AC13] For the purpose of content analysis, the TOE shall invoke an external server (which utilises an application interface compliant with the Content Vectoring Protocol[1] for the purpose of engaging services or 3rd party products).

73 Application Note. Establishing connections to external content analysis services is implemented by the Security Server component which is part of the Firewall module located on the SFD. The ASF will direct connections requiring the intervention of the Security Server to the SFD, where the standard processing of the connection will be performed by the Firewall module.

6.1.2.9 General

[AC14] The TOE shall ensure that all connections to services or 3rd party products external to the TOE which communicate with the TOE for the purpose of subscriber authentication or content analysis are subject to the *FireWall Security Policy*.

74 This security function reflects the architecture of the TOE , specifically the Firewall Module, which ensures that all connections through a firewall including those to external services originated by the firewall itself are subject to the inspection required by [AC2], [AC3], [AC4], [AC5], [AC6], [AC7], [AC8] and [AC9].

6.1.3 Remote Supervision

[1] This is a publicly published protocol available from the Check Point web site - http://www.checkpoint.com

[RS1] The product shall allow an administrator accessing the TOE via a Check Point Management Server to retrieve information in respect to the current status of the TOE. Current Status comprises:

a) the availability of an active network link between the Management Server and gateway

b) the presence or absence of an active FireWall Security Policy upon the gateway

c) the name and loading date of the FireWall Security Policy loaded on the gateway

d) the number of packets inspected, dropped, rejected, and/or logged by that gateway.

75 Application Note. Status requests are generated at the Check Point Management server and communicated to the TOE via the trusted communication channel. The TOE gathers the data required to respond to these status requests. The response is generated and transmitted by the Firewall module component.

6.1.4 Data Exchange

6.1.4.1 Data Confidentiality and Integrity

[VPN1] The product shall invoke establishment of secure and trusted VPN connections between the TOE and a physically-separated *VPN enabled client.*

76 Application Note. The provision of a VPN communication between the TOE and a *VPN enabled client* may be specified within a Firewall Security Policy and identified within the policy file provided by the Management Server to the TOE. The Firewall-1 module included in the SFD component of the TOE provides an implementation of the IPSec protocol for VPN. It is therefore capable of negotiating an exchange of cryptographic credentials and subsequently handling the encryption and decryption of packets transmitted via the VPN channel. The ASF will direct IP packets associated with a VPN connection to the SFD, where all of the processing associated with establishing and maintaining the VPN connection (e.g. negotiation, packet encryption and decryption) will be performed by the Firewall module.

6.1.5 Secure Internal Communication

[SIC1] The product shall allow an administrator to invoke establishment of secure and trusted connections between the Check Point Management Server and the TOE.

77 Application Note. Secure communication between the TOE and the Management Server is implemented by the use of the TLS protocol. When the TOE is started it will negotiate via TLS a secure (authenticated and encrypted) connection with the Management Server. This protocol is based upon the use of digital certificates which are issued by an Internal Certificate Authority (ICA) co-located with the Check Point Management Server. Part of TOE installation procedure ensures that a valid digital certificate is installed upon the TOE.

6.1.6 Audit

6.1.6.1 Audit Data Administration

[AUD1] The product shall provide the capability for administrators via a Check Point Management Server to:

a) specify the creation of audit records (logs) on the basis of individual access control *rule statements* of the *FireWall Security Policy*.

b) specify the generation of audit alerts on the basis of individual access control *rule statements* of the *FireWall Security Policy*.

78 Application Note. Accounting requirements are specified by an administrator during the creation of a *Firewall Security Policy* and this information will be included as part of the INSPECT file defining the Firewall Security Policy which is provided to the SFD by the Management Server. The SFA and the SFD director components of the ASF will gather the data required by audit records, which will be generated by the Firewall within the SFD and forwarded to the external Management Server for storage.

6.1.6.2 Audit Events

[AUD2] The product shall provide the capability to generate audit records for each attempt to receive or send an IP packet through a defined product *network interface*.

6.1.6.3 Audit Records

[AUD3] The product shall record within each audit record the following information:

a) a timestamp (including date and time)

b) the product's host IP address

c) the *network interface*

d) the *direction* of packet flow

e) the *action* taken

f) additional information, as specified by the audit record format. The additional audit record information can be found in the [CPMANAGEMENT] document in the SmartView Tracker section.

[AUD4] Application Note. This Security Function of [VPN-1/FW-1-ST] is omitted since it relates solely to functionality provided by the Check Point Management Server and its GUI.

6.1.6.4 Maintaining Audit Log Files

[AUD5] Application Note: This Security Function of [VPN-1/FW-1-ST] is omitted since the audit records generated by the product are forwarded for storage at the Management Server, which provides administrators with the capability to close the current audit log file and switch recording of audit records to a new audit log file.

6.1.6.5 Generating Audit Alerts

[AUD6] The product shall provide the capability to generate SNMP traps and GUI alerts corresponding to audit events.

6.2 Required Security Mechanisms

79 The TOE itself merely invokes use of authentication, Secure Internal Communication and VPN mechanisms for which requirements are placed on its environment. It incorporates no mechanisms for which an explicit analysis of the strength of functionality is required by CC.

6.3 Assurance Measures

6.3.1 Statement of Assurance Measures

80 No assurance measures are required other than the provision of deliverables to comply with EAL4 assurance requirements.

7. PP Claims

81 No claim of PP compliance is being made for the TOE.

8. TOE Rationale

8.1 Security Objectives Rationale

8.1.1 Introduction

82 This section will demonstrate how the objectives for the TOE and the objectives for the TOE environment (defined in Section 4) are necessary and sufficient to address each of the threats, policies and assumptions identified in Section 3.

83 Table 8-1 shows that all stated security objectives may be mapped to identified threats and assumptions, and that all threats and assumptions are mapped to at least one security objective. The sub-sections following the table describe the coverage of threats and assumptions by the security objectives.

	[SO1]	[SO2]	[SO3]	[SO4]	[SO5]	[SO6]	[SO7]	[SO8]	[ESO1]	[ESO2]	[ESO3]	[ESO4]	[ESO5]	[ESO6]
[E_AS1]										X				
[E_AS2]									X	X				
[E_AS3]									X					
[E_AS4]										X				
[M_AS1]									X	X				
[M_AS2]									X					
[M_AS3]										X				
[M_AS4]										X				
[M_AS5]										X				
[M_AS6]										X				
[M_AS7]										X				
[M_AS8]										X				
[M_AS9]										X				
[M_AS10]										X				
[M_AS11]									X	X				
[M_AS12]										X				
[T1]	X	X	X						X	X				
[T2]	X								X	X				
[T3]	X	X	X						X	X				
[T4]	X								X	X				
[T5]	X								X	X				
[T6]				X					X	X				X
[T7]				X					X	X				
[T8]						X			X	X		X		
[T9]						X			X	X		X		
[T10]							X		X	X			X	
[T11]							X		X	X			X	
[T12]								X	X	X				
[T13]					X				X	X	X			
[T14]					X				X	X	X			

Table 8-1 Objectives Rationale Mapping

8.1.2 [E_AS1] to [E_AS4] inclusive, and [M_AS1] to [M_AS12] inclusive

84 It is asserted that all these assumptions are addressed by the environmental objectives [ESO1], [ESO2]. Meeting these objectives will ensure that the TOE is installed and operated in a fashion that addresses the environmental and method of use assumptions. The mapping of assumptions to objectives is the same as that pointed out during the definition of the objectives in section 4.2.

85 In the analysis of the threats below it should be noted that the environmental objectives [ESO1], [ESO2], which require that all of the environmental assumptions are in practice achieved, is implicit in countering all of the threats. This is because correct functioning of TOE leading to the achievement of the security objectives requires that the components of the TOE be correctly built and configured and protected from tampering. Where a specific assumption is of particular importance for addressing a threat this is emphasised in the discussion of threats below.

8.1.3 [T1]

86 The threat of a host on one of the physically connected networks attempting to establish unauthorised communications with a host on another physically connected network is addressed by [SO1], [SO2], and [SO3]. These objectives implement the firewall filtering rules (control IP packet flow) and so directly control all (and stop unauthorised) communications between connected networks. They also provide network address translation and can hide the addresses present on one connected network from the other connected networks, thereby preventing communication to the network with the hidden addresses.

8.1.4 [T2]

87 The threat that a host on one of the physically connected networks may attempt to access services (that are not intended to be available) on another physically connected network is addressed by [SO1]. [SO1] implements the firewall rules and policies and so directly mediates whether the access is permitted or not.

8.1.5 [T3]

88 The threat that a person on the external network may attempt to gain access to one of the physically connected internal networks by employing network address spoofing attacks is directly addressed by [SO1] (which implements the firewall rules). Also objectives [SO2] and [SO3], hiding and translating internal addresses, minimises the disclosure of the information required to launch an effective address spoofing attack.

8.1.6 [T4]

89 The threat that a person on the external network may attempt to gain access to one of the physically connected internal networks by employing IP Source routing attacks is addressed by [SO1], which directly implements the firewall rules.

8.1.7 [T5]

90 The threat that a person on the external network may attempt to gain access to one of the physically connected internal networks by employing IP packet fragmentation attacks is directly addressed by [SO1] , specifically as refined by requirement FDP_IFF.1 which directly identifies this function as a aspect of flow control.

8.1.8 [T6]

91 The threat that attempts to establish communications which will lead to a breach of the product's security policy may not be detected in a timely manner is addressed by [SO4] and [ESO6]. [SO4] requires that the product is able to record such events and generate alerts thereby providing a means to provide a timely warning. It is supported by [ESO6].

8.1.9 [T7]

92 [SO4], [ESO1] and [ESO2] address the threat that a person on the external network may generate enough auditable events to overload the audit logging and thus prevent the correct audit of future activity. [SO4] will ensure that audit records are generated by the TOE and forwarded to the Management Server in the environment of the TOE, required by [ESO1], that enables the policy for closing and switching audit log files to be enforced. Additionally [ESO2] requires the assumption [M_AS10] be addressed in the policies and this requires that the audit logs are suitably managed or the product stops processing until it is again able to record to its logs.

8.1.10 [T8]

93 The threat that unauthorised disclosure of information may occur when being transmitted between the TOE and a *VPN enabled client*, is addressed by [SO6] and [ESO4]. [SO6] enables the use of [ESO4] cryptographic measures to protect the confidentiality of information transmitted between the product and a *VPN enabled client.*

8.1.11 [T9]

94 The threat that there could be undetected attempts to modify the contents of data being transmitted between the TOE and a *VPN enabled client*, is addressed by [SO6] and [ESO4]. [SO6] enables the use of [ESO4] cryptographic measures to protect the integrity of data transmitted between the product and a *VPN enabled client.*

8.1.12 [T10]

95 The threat that there could be attempts by unauthorised users to bypass defined subscriber authentication measures is addressed by [SO7] and [ESO5]. [SO7] enables the use of [ESO5] user authentication services.

8.1.13 [T11]

96 The threat that connections may be established that bypass defined packet content analysis measures (i.e. the firewall rules or firewall security policy) is addressed by [SO7] and [ESO5]. [SO7] enables the use of [ESO5] content analysis services.

8.1.14 [T12]

97 [SO8] and [ESO2] address the threat that problems with unavailability of the TOE may be exploited. [SO8] requires that remote 'real-time' monitoring is available so that warning of a potential problem is provided, and [ESO2] requires the environmental assumptions are met regarding the configuration, monitoring and general management of components to minimise the risk of such a threat.

8.1.15 [T13]

98 [SO5] and [ESO3] address the threat that there could be unauthorised disclosure of information being transmitted between the TOE and the Management Server. [SO5]

enables the [ESO3] establishment of a trusted secure communications channel between the TOE and the Management Server, and this requirement includes the use of cryptographic measures to protect the confidentiality and integrity of information transmitted.

8.1.16 [T14]

99 [SO5] and [ESO3] address the threat that there could be undetected attempts to modify information being transmitted between the TOE and the Management Server. [SO5] enables the [ESO3] establishment of a trusted secure communications channel between the TOE and a Management Server and this requirement includes the use of message digests to detect integrity violations.

8.2 Security Requirements Rationale

8.2.1 Introduction

100 This section will demonstrate how the security requirements for the TOE and the security requirements for the IT environment are necessary and sufficient to address each of the security objectives in Section 4.

8.2.2 TOE Functional Requirements Rationale

101 Table 8-2 (below) shows that all TOE SFRs may be mapped to stated TOE objectives, and all TOE security objectives are mapped to at least one TOE SFR. The sub-sections following the table, describe the coverage of the security objectives by SFRs.

	[SO 1]	[SO2]	[SO3]	[SO4]	[SO5]	[SO6]	[SO7]	[SO8]
FDP_IFC.1 (1)	X							
FDP_IFF.1 (1)	X	X	X				X	
FMT_MSA.1 (1)	X							
FMT_MSA.3 (1)	X							
FMT_MOF.1 (1)	X							
FPT_RVM.1	X							
EDP_ITT1(1)(EXP)					X			
EDP_ITT1(2)(EXP)						X		
FMT_MSA.1 (2)								X
FAU_GEN.1				X				
FAU_SAA.1				X				
FMT_MOF.1 (2)				X				

Table 8-2 TOE Requirements Rationale Mapping

8.2.3 [SO1]

102 FDP_IFC.1 (1), FDP_IFF.1 (1), FMT_MSA.1 (1), FMT_MSA.3 (1), FMT_MOF.1 (1) identify the information flow requirements for the Firewall Security Policies. The

Firewall Security Policies are directly concerned with the flow control of the IP based packets at the TOE Firewall Modules, and so address this objective.

103 FPT_RVM.1 is also associated with this objective since conforming to a valid Firewall Security policy is a precondition for any onward network connectivity through the TOE.

8.2.4 [SO2]

104 FDP_IFF.1.3(1) identifies a requirement for configurable address translation and so addresses this objective.

8.2.5 [SO3]

105 FDP_IFF.1.3(1) identifies a requirement for configurable address translation by which the use of ‘internal’ addresses can be hidden from an external network and so addresses this objective.

8.2.6 [SO4]

106 FAU_GEN.1, FAU_SAA.1, FMT_MOF.1 (2) identify the requirement to configure and generate logs and alerts to meet this objective.

8.2.7 [SO5]

107 EDP_ITT(1)(EXP) identifies the requirement to support trusted channels between the TOE and Management Server by means of the standard TLS protocol. The TLS protocol makes use of cryptographic algorithms for encryption, key exchange etc. and these play an essential role in achieving this objective. However the evaluation of this TOE concerns itself only with interfaces that allow these algorithms to be invoked and not with their strength or the correctness and security of their implementation.

8.2.8 [SO6]

108 EDP_ITT.1(2)(EXP) identifies the requirement to support VPN connections, between the TOE and *VPN enabled clients*, by means of the standard IPSec protocol. The IPSec protocol makes use of cryptographic algorithms for encryption, message digesting, key exchange etc. However the evaluation of this TOE concerns itself only with interfaces that allow these algorithms to be invoked and not with their strength or the correctness and security of their implementation.

8.2.9 [SO7]

109 FDP_IFF.1 identifies the requirement to access services external to the product and thereby addresses this objective.

8.2.10 [SO8]

110 FMT_MSA.1(2) restricts the ability to query the current operational status and active policy of the Firewall Module to the authorised administrator. By implication, the authorised administrator must be able to initiate these queries, and the product must be able to respond in real-time, i.e. without significant delay, with the status of these attributes.

8.2.11 IT Environment Functional Requirements Rationale

111 Table 8-3 (below) shows that all Environmental SFRs may be mapped to stated environmental IT objectives, and all environmental IT security objectives are mapped to at least one environmental SFR. The sub-sections following the table, describe the coverage of the security objectives by SFRs.

112 Note that environmental objective [ESO2] is primarily concerned with physical, procedural and personnel objectives, and relates only indirectly to the IT. This objective does not therefore map to environmental SFRs.

113 A similar situation to [ESO2] holds in relation to environmental objective [ESO1] which is primarily concerned with physical, procedural objectives, and relates only indirectly to the IT. However [ESO1] also explicitly requires the existence of compatible Check Point management components (Server and GUI) within the environment of the TOE, and these will provide the functionality needed to address the management SFRs duplicated for the environment.

	[ESO1]	[ESO 3]	[ESO4]	[ESO5]	[ESO6]
FMT_MSA.1 (3)	X				
FMT_MOF.1 (3)	X				
FMT_MOF.1 (4)	X				
FMT_MSA.1 (4)	X				
FTP_ITC.1 (1)				X	
FDP_ITT.1 (1)		X			
FDP_IFC.1 (2)		X			
FDP_IFF.1 (2)		X			
FCS_COP.1 (1)		X			
FDP_ITT.1 (2)			X		
FDP_IFC.1 (3)			X		
FDP_IFF.1 (3)			X		
FCS_COP.1 (2)			X		
FIA_UAU.5				X	
FTP_ITC.1 (2)				X	
FPT_STM.1					X

Table 8-3 Environmental IT Requirements Rationale Mapping

8.2.12 [ESO3]

114 The four SFRs together provide the SIC capability, thereby addressing the objective.

8.2.13 [ESO4]

115 The four SFRs together provide the VPN capability, thereby addressing the objective.

8.2.14 [ESO5]

116 FTP_ITC.1 (1) meets the aspects of the objective involving use of a content validation service and secure communication with the service. FIA_UAU.5 and FTP_ITC.1 (2) meet the respective aspects involving user authentication and secure communication with this service.

8.2.15 [ESO6]

117 FPT_STM.1 addresses the objective to provide reliable time stamping.

8.2.16 Security Requirements Dependencies Rationale

118 The table below, Table 8-4, identifies the dependencies between the SFRs identified by the [CC] Part2 in respect to the SFRs selected for this TOE. Note specific instances of a dependency will be satisfied by specific instantiations of a SFR, and these can be determined by the numbers in brackets assigned to SFRs. In a few cases the SFR associated with [CC] Part2 dependency has not been introduced for the TOE, but is addressed by environmental requirements for the TOE and these situations are identified in the fourth column of the table. These also provide the rationale in respect to the SFRs associated with the IT environment.

SFR	CC Part 2 Dependencies Addressed	Missing Dependencies	Rationale
FDP_IFC.1 (1)	FDP_IFF.1(1)		
FDP_IFF.1 (1)	FDP_IFC.1(1), FMT_MSA.3(1)		
FMT_MSA.1 (1) FMT_MSA.1 (3)	FDP_IFC.1(1), FDP_IFC.1(3)	FMT_SMR.1	Note 1
FMT_MSA.3 (1)	FMT_MSA.1(1)	FMT_SMR.1	Note 1
FPT_RVM.1	[CC] Part2 identifies no dependencies.		
EDP_ITT.1(1)	FDP_ITT.1(1)		Note 2
EDP_ITT.1(2)	FDP_ITT.1 (2)		Note 2
FMT_MOF.1 (1) FMT_MOF.1 (4)		FMT_SMR.1	Note 1
FMT_MSA.1 (2) FMT_MSA.1 (4)	FDP_IFC.1(3)	FMT_SMR.1	Note 1.
FAU_GEN.1	FPT_STM.1		
FAU_SAA.1	FAU_GEN.1		
FMT_MOF.1 (2) FMT_MOF.1 (3)		FMT_SMR.1	Note 1

SFR	CC Part 2 Dependencies Addressed	Missing Dependencies	Rationale
FTP_ITC.1(1)	[CC] Part2 identifies no dependencies.		Note 5
FDP_ITT.1(1)	FDP_IFC.1 (2)		
FDP_IFC.1 (2)	FDP_IFF.1 (2)		
FDP_IFF.1 (2)	FDP_IFC.1 (3)	FMT_MSA.3	Note 3
FCS_COP.1(1)		FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Note 4
FDP_ITT.1(2)	FDP_IFC.1 (3)		
FDP_IFC.1 (3)	FDP_IFF.1 (3)		
FDP_IFF.1 (3)	FDP_IFC.1 (3)	FMT_MSA.3	Note 3
FCS_COP.1(2)		FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Note 4
FIA_UAU.5	[CC] Part2 identifies no dependencies.		Note 6
FTP_ITC.1(2)	[CC] Part2 identifies no dependencies		Note 5
FPT_STM.1	[CC] Part2 identifies no dependencies		

Table 8-4 CC Part 2 Dependencies Mapping

119 Duplicated SFRs reflected management functions distributed between the TOE and the Management Server in its environment.

120 Certain of the dependencies identified for the SFRs of [CC] Part2 are not directly addressed by the functionality of the TOE, but are a consequence of the IT environment of the TOE. The rationale for these missing dependencies is provided below:

- Note 1. The missing dependency, FMT_SMR.1, relates to the assignment of security management roles by the TOE, specifically in the case of this TOE to the authorised administrator. Whilst the Check Point VPN-1/Firewall-1 product does include functionality that relates to assignment of Firewall administrator roles these have not been included in the functionality selected for this TOE. The rationale for this is that all access to the administration role is dependent upon gaining direct access to the TOE (i.e. the hardware hosting the TOE) or access to the Management Server or its GUI. In view of this, the requirement is addressed by the environmental and method of use assumptions [E_AS1], [M_AS4], [M_AS6], [M_AS7].
- Note 2. EDP_ITT.1(1) and (2) are explicit SFRs specific to this TOE. Their dependence on the [CC] Part 2 conformant SFRs FDP_ITT.1 (1) and (2) reflects the fact that these requirements require the implementation of the functionality that SFRs EDP_ITT.1(1) and (2) require to be available for invocation.
- Note 3. The missing dependency, FMT_MSA.3, relates to the fact the TOE is secured prior to the initialisation of attributes that underlie the information flow policy. In the case of SIC and VPN connections each of the communicating platforms has to have a PKI certificate and associated public and private key (or shared secret data) installed upon them. This has to be achieved by means of the direct platform access and is thus addressed by the same environmental assumptions identified in Note 1.

- Note 4. The dependencies FCS_CKM.1, FCS_CKM.4, FMT_MSA.2 associated with FCS_COP.1 relate to the key management issues associated with the cryptographic functionality. All of this functionality is based upon PKI protocols, whereby the active cryptographic keys are controlled and generated as required by the activity of the protocols. Thus these dependencies are addressed by the correct implementation of the standard protocols, which is out of scope of the evaluation of this TOE. Ultimately the validity of the key management for these PKI protocols is reliant upon the security of the private key data associated with published keys, and this is covered in part by the protocol standards and the fact that private keys are installed "out band" by a process that requires direct access to a platform needing to communicate; also see Note 3.
- Note 5. The TOE does include the support for the communication interfaces to content verification and LDAP services required by the SFRs, FTP_ITC.1 (1) and (2). However the trust required for these interfaces is not realised solely by the TOE functionality but also by the correct configuration of the environment of the TOE, namely that such external services are installed upon a protected network as required by assumption [E_AS4]. Where a Firewall Module requires remote access to such functions, it would be necessary that the product's VPN functionality shall be configured to provide a protected channel to the protected network hosting these servers, i.e. that a suitable policy etc. is installed at the Firewall module as is implicit in [M_AS1].
- Note 6. Protection of the network connection to an external authentication service e.g. Radius (FIA_UAU.5.2 a) and digital signature verification (FIA_UAU.5.2 c) utilise the product's VPN functionality. Equivalent considerations to those of Notes 4 and 5 thus apply.

8.2.17 Assurance Requirements Rationale

121 The TOE is intended to be used in a variety of environments, including providing protection for networks from the Internet and other third party networks. The EAL4 assurance level is consistent with such threat environments, and generally perceived by the consumer as an adequate and necessary level for such security products.

8.2.18 Security Requirements are Mutually Supportive

122 Security Functional Requirements are shown in Section 8 of this document to address each of the stated security objectives which in turn address each of the identified threats.

123 The security assurance requirements are shown to be appropriate for the TOE.

124 Dependencies between security functional requirements defined in this ST are illustrated, and exceptions explained. By definition these actions are mutually supportive.

125 Thus, the set of security requirements defined in this ST together can be seen to form a mutually supportive and internally consistent whole.

8.2.19 Strength of Function Claim Rationale

126 The rationale for the strength of function claim is provided in Section 5.2.1.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions are Mutually Supportive

127 Table 8-4 demonstrates that all SFRs are mutually supported.

128 Table 8-5 (below) identifies the TOE security functions that are associated with the implementation of each of the SFRs. At the top level the description of the security function can be aligned with the mapped SFR, however where further explanation is required this is provided in the “comment” column of the table. Therefore the Security Functions are mutually supportive.

TOE Security Functional Requirements	TOE Security Functions	Comments
FDP_IFC.1 (1)	See FDP_IFF.1(1)	
FDP_IFF.1 (1)	AC2, AC3, AC4, AC5, AC6, AC7, AC8, AC9, AC10, AC11, AC12, AC13, AC14	The Security Functions identify the various aspects of flow control enforced by the Firewall Module component of the TOE.
FMT_MSA.1 (1)	AC1	The various SFs associated with the FIREWALL-SFP and SIC-SFP also support this functionality.
FPT_RVM.1	AC2, AC4	These SFs are specifically associated with this requirement since their implementation ensures that all requests for information flows through the TOE, even those at startup, are intercepted by the inspection mechanisms and are subject to policy. The environmental objective ESO1 also supports this requirement by ensuring that the platform has been correctly configured to prevent by-passing (i.e. physical ports correctly configured and IP-forwarding by the OS disabled).
FMT_MSA.3 (1)	AC2	
EDP_ITT.1 (1)	SIC1	
EDP_ITT.1 (2)	VPN1	
FMT_MOF.1 (1)	AC1	
FMT_MSA.1 (2)	RS1	
FAU_GEN.1	AUD2, AUD6, AUD3	The audit function cannot be stopped since it is an integral part of the operation of the TOE that starts when the TOE components responsible for audit are started. Startup will be recorded as the first audit event in an audit log upon the start of a TOE Firewall Module or Management Server component. When audit logs are switched, the file name applied to the old audit log identifies the time of switch.
FAU_SAA.1	AUD6	
FMT_MOF.1 (2)	AUD1, AUD2	

Table 8-5 TOE Summary Specification Rationale Mapping

8.3.2 Strength of Function Claims are Appropriate

129 The justification for the strength of function claim is provided in Section 5.2.1.

8.3.3 TOE Assurance Measures

130 This Security Target does not state any assurance requirements other than those compliant with the EAL4 level of assurance.

A Definitions

Action In the context of packet flow through the product, used to indicate the flow control decision taken by the product, which is one, and only one, of: **Accept**; **Reject**; **Drop**.

Asymmetric Encryption Refers to the use of an algorithm to encrypt and decrypt data which requires two different keys, one to encrypt the data and another to decrypt it.

Authorised Administrator Refers to an individual with access to the physically protected LAN hosting the Management Server and GUI, from which secure administration of VPN-1/Firewall-1 is performed.

Direction In the context of packet flow through the product, used to indicate the direction of flow of a packet, at one of the product's *network interfaces*, with respect to the product's computer system. The direction can be either **Inbound** or **Outbound**.

External In the context of networks physically connected to the product, used to refer to the (less protected; unprotected; public) network that constitutes the main source of threat and against which the product is employed to enforce a degree of protection to other, *internal*, networks physically connected to the product.

FireWall Security Policy Refers to the security/access control policy enforced by the product, which is an information flow control policy applied to information flowing between subjects and objects that are not part of the product. A subject and an object participating in an information flow are either located on different networks physically connected to the product or one of them is located on the product's computer system and the other is located on a network physically connected to the product.

Hide, Hidden In the context of the product's IP packet addressing, used to indicate a mode of address translation in which hosts' IP addresses on an *internal* network are not visible to subjects on the *external* network, and in which a subject on an *external* network is unable to initiate a communication with a host at one of the hidden IP addresses.

Information In the context of packet flow through the product, used to refer to packet content, characterised by the following header information for the IP family of protocols and higher level protocols layered over IP, including state information derived from one or more associated IP packets as well as information concerning packet flow in relation to the product's computer system, such as the *direction* and associated *network interface*:

a) source and destination IP addresses

b) IP protocol number

c) source and destination port number

d) TCP ACK bit

e) FTP PORT command

f) *direction*

g) *network interface*.

Internal In the context of networks physically connected to the product, used to refer to the networks for which the product is employed to enforce a degree of protection against the *external* network.

Internet IP Address Any address must be unique if confusion over the correct delivery of messages is to be avoided. This applies to *IP Addresses* as well as more traditional forms of networked communications (e.g. the telephone). In terms of the Internet the legal assignment of *IP* Addresses is performed by a number of InterNIC centres under the control of the Central Internet Address Network Authority.

IP Addresses Internet Protocol (IP) addresses are defined as a 32 bit numbers which are represented, for ease of use, as four decimal numbers corresponding to the decimal value of the four bytes that make up the 32 bit IP address. All addresses consist of a net and host id. The former provides a unique code to the network on which a given connection sits whilst the host id points to a specific connection.

Invalid/Valid IP Address An IP Address which has been approved by an appropriate authority is a valid *Internet IP Address*. An *IP Address* which has NOT been approved by an appropriate authority is an Invalid *Internet IP Address*. Organizations often use *IP Addresses* within an organization which have not been approved for the Internet as this increases flexibility, reduces the cost of *Internet IP Address* registration and means that the addresses of internal machines are *hidden* from *external* networks. In such circumstances address translation must be performed before any connection with an *external* network, including the Internet.

IP Source Routing The process whereby the source host inserts additional information in IP headers in order to specify the route the packet should take.

Log An audit record format which writes the following information to the audit log:

h) IP protocol

i) source IP address

j) destination IP address

k) service or destination TCP/UDP port

l) source TCP/UDP port

m) IP length

n) *FireWall Security Policy rule statement* number

If Address Translation is active, the following additional information:

o) original source IP address

p) original destination IP address

q) original source port (UDP/TCP)

r) original destination port (UDP/TCP).

Message Digesting A condensed representation of text by the means of a string of digits, created using a formula called a one-way hash function.

Network Address Spoofing An attack whereby the attacker sends packets that claim to be from some other, trusted, source.

Network Interface The point of connection of the product's computer system with a physically connected network which constitutes the hardware and software used by IP to communicate with the physical network.

Operation In the context of packet flow through the product, used to refer to one or more of the following Internet services, initiated by subjects on objects, that involve the exchange of one or more associated IP packets whose flow is mediated by the *FireWall Security Policy*:

a) any service which uses only constant, known, port allocations

b) the FTP service

c) the SQL-NET service

d) the echo request/reply service.

Rule Statement

A statement in the FireWall-1 Language (INSPECT) which defines the *action* to be taken on an IP packet which contains *information* meeting certain criteria associated with the statement in accordance with the syntax and semantics of INSPECT. The set of rule statements in an Inspection Script comprise the *FireWall Security Policy*.

Subscriber

A person or service which communicates with another person or service through a firewall module and whose communication is subject to the *FireWall Security Policy*.

VPN enabled client

An external entity that has suitable software to allow it to engage in an IPSec based VPN connection with the product, this will include other instances of the product and entities that incorporate the Check Point Secure Remote software.