Common Criteria EAL4 Evaluation

Check Point Software Technologies Inc.
VPN-1/Firewall-1 Next Generation (Feature Pack 2)
Security Target Issue 1.8 for Nokia

DEVELOPER:
Alex Ragen
Certification Manager
Check Point Software Technologies, Ltd.
3A Jabotinsky Diamond Tower
Ramat Gan 52520
Israel
Email: alex@checkpoint.com
Phone: +972 3 753 4552
Fax: +972 3 753 4748

SPONSOR:
Ed Ingber
Product Manager
Nokia
313 Fairchild Drive
Mountain View, CA 94043
U.S.A.
Email: Ed.Ingber@nokia.com
Phone: 1-650-625-2345
Fax: 1-650-691-2170

Contents

Revision History

Issue	Date	Author	Comments
0.0a	24th Dec 2001	K Elcoate (EDS, Information Assurance Group)	Initial issue for review.
0.0b	14th Mar 2002	P. Taylor (EDS, Information Assurance Group)	Revised to ensure consistency with the final issue of the ITSEC Security Target.
1.0	22nd Mar 2002	P. Taylor	First issue for Check Point review.
1.1	11th Apr 2002	P. Taylor	Revised for formal issue.
1.2	10th May 2002	P. Taylor	Revised to track minor revisions to the ITSEC Security Target requested by CB
1.3	18th June 2002	P. Taylor	Minor rewording for consistency
1.3a	27th Nov 2002	P. Taylor	Draft with CC Part 2 SFRs
1.4	29th Nov 2002	P. Taylor	Issue for Check Point review.
1.4.1	2nd Dec 2002	P Taylor	Formal issue incorporating Check Point comments
1.5	18th Dec 2002	P. Taylor	Revised to address evaluation ORs.
2.0	30th Apr 2003	Ed Ingber	Revised to address VPN-1/FireWall-1 NG (Feature Pack 2), include Nokia IPSO as Operating System
1.8 for Nokia	17th July 2003	Ed Ingber	Revised to accommodate changes between Issue 1.5 and 1.8.

References

[MANAGEMENT] Check Point Management Guide NG FP-2, March 2002

[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

[CP_VPN] Check Point Virtual Private Networks NG FP2, March 2002 Part No: 700350

[GET_START] Check Point Getting Started Guide NG FP2, March 2002 Part No: 700446

[I-ST] Check Point Software Technologies Inc., VPN-1/Firewall-1 Next Generation, ITSEC E3 Certification Security Target, Version 2.1.8, April 2002

[OP_DOC] ITSEC E3 System Generation/Installation Check Point VPN-1/Firewall-1 Next Generation Feature Pack 2 (FP2), Version 2.7, February 2003, Part No: N450941001.

1 ST Introduction

1.1 ST Identification

Title:	Common Criteria EAL4 Evaluation, Check Point Software Technologies Inc. VPN-1/Firewall-1 Next Generation (Feature Pack 2) Security Target.
Target of Evaluation (TOE):	VPN-1/Firewall-1 Next Generation (Feature Pack 2)
Operating System(s):	Windows NT 4 SP6a, Nokia IPSO 3.5, 3.5.1.
Hardware:	Any computer system from the family of Workstations, Servers, and Appliance Platforms that support one of the operating systems listed above (but subject to the constraints noted in paragraph 15).

1 This document serves as the Security Target (ST) for the Common Criteria EAL4 evaluation of Check Point Software Technologies Ltd's (Check Point) firewall and VPN product: VPN-1/Firewall-1 Next Generation (Feature Pack 2), hereafter referred to as 'the product'. It should additionally be noted that when the terms 'Firewall-1' or 'VPN-1' are used (either individually or in combination) they also should be taken as references to 'the product'.

2 It should be noted that the term "VPN-1/Firewall-1 Next Generation (Feature Pack 2)" is not only descriptive, but also identifies the version of the product.

3 For convenience, throughout this document the words 'he', 'his' etc. are intended to represent 'he or she', 'his or hers' etc.

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

5 Some Check Point VPN-1/FireWall-1 or product specific words used in the text are presented in **bold** font.

1.2 ST Overview

1.2.1 Introduction

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

7 Readers are also assumed to be familiar with basic networking, Internet, TCP/IP, UNIX and Windows NT terms and concepts.

1.2.2 Overview

8 The product provides firewall and virtual private network functionality to secure the communications between networks, and the management of the product itself.

9 It supervises the traffic passing between networks physically connected to the product's computer system 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 supervision provided by the product includes the capability to encrypt, authenticate and validate data which travels between selected Internet IP addresses on networks protected by VPN-1/FireWall-1 such that the communication is established with authenticated entities. If such capability is required, the confidentiality of data is maintained preventing unauthorised disclosure and the

integrity of the data is assured through the application of an encrypted message digest covering the contents of each data packet.

11 The product allows Administrators to interact with the VPN/FireWall using VPN-1/FireWall-1's Management GUI. The users of the product in this case, are subscribers who communicate through the firewalls. In the case of the VPN-1 SecureClient, the TOE also allows remote subscribers to communicate through the VPN/FireWall.

12 Note that the CC TOE covers the product's firewall functionality and invocation of the product's VPN functionality. Product cryptographic functionality is covered by a FIPS validation (to the extent that this was addressed by the validation).

1.3 CC Conformance

13 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

2.1 The Trusted Configuration

14 The product has to be used in a 'trusted configuration' (as defined in the next paragraph). Some of the security functionality requires separate but communicating instances of the product to execute on separate Workstations or Servers.

15 A 'trusted configuration' of the product:

a) executes on any computer system from the family of Workstations, Servers, and Appliance Platforms which support one of the following operating systems:

   i. Windows NT4 SP6a

   ii. Nokia IPSO 3.5, 3.5.1

   (subject to the considerations of [GET_START] and [OP_DOC])

b) executes on a computer system which support up to 128 port connections (note that the product uses the concept of managed ports and does not use the traditional firewall terms of *internal* and *external* network)

c) consists of:

   i. a Management Server running on Windows NT4 SP6a which resides on a protected LAN

ii. a Graphical User Interface (GUI) which resides on a separate workstation running Microsoft Windows NT which is part of the same protected LAN as the Management Server

iii. a VPN-1 SecureClient which resides on a remote machine outside of the protected LAN but is part of the corporate network. The VPN-1 SecureClient must reside on a machine running Windows NT

iv. a number of VPN-1/FireWall-1 Modules which may or may not reside on the same protected LAN as the Management Server; the VPN-1/FireWall-1 modules may be configured such that two modules form a High Availability pair, using the Virtual Router Redundancy Protocol (VRRP) implemented in IPSO;

v. a Policy Server installed on a VPN/FireWall machine which resides on the same protected LAN as the Management Server.

d) is configured, controlled and monitored using the Graphical User Interface which communicates with the Management Server; the Management Server then configures the Firewall Modules and via the Policy Server downloads the Desktop Policy to the SecureClient(s)

e) has been installed, configured and started-up, as described in Getting Started with VPN-1/FireWall-1 [GET_START] and [OP_DOC].

16 The product operates in two modes:

a) as a firewall which uses 'Stateful Inspection Technology' to inspect all packets (it supports the complete "IP" family of protocols) passing between networks connected to the product, promptly blocking all unwanted communication attempts;

b) as a virtual private network (VPN) which is used to establish a secure communications channel over an unsecured network (e.g. the Internet) using two Check Point FireWalls or a Check Point Firewall and a SecureClient.

17 These two modes are simultaneous, in that the product can employ both functionalities in respect to different communications and/or at different phases of processing a single communication.

18 The enforcement of the access and communication control aspects of the product is implemented at the VPN-1/FireWall-1 Modules and at the VPN-1 SecureClients. Management and monitoring of the product is supported by the remaining components i.e. the GUI, the Management Server and the Policy Server. In summary, management entails the definition and distribution of appropriate Firewall or Desktop Security Policies to the enforcement modules, whilst monitoring entails the collection and inspection/analysis of logging and status information generated at the enforcement modules. Further discussion of the TOE's functionality is provided in the Summary Specification, section 6.

19 The evaluation of the product includes the following security or security-related features:

a) A Light Directory Access Protocol (LDAP) client interface, which allows a local/remote LDAP compliant directory service to be interrogated for information pertaining to users of protected networks. The directory can be used to store information on the types of connections and services that may be accessed by users of a network protected by a Check Point FireWall.

b) A remote management capability which allows a Management Server to control the firewall flow policies for a number of Check Point FireWalls where the control information is required to traverse secured and unsecured communications links.

c) A Security Server which is used to filter files in selected protocols (http, ftp, smtp), in accordance with rules defined by the administrator, and which is capable of interfacing with third-party products providing further file-analysis services (e.g. virus scanning applications, Universal Resource Locator (URL) filtering etc.).

d) A Secure Internal Communications (SIC) facility which is used to establish trusted secure communication between Check Point Modules, i.e. Management Server, GUI clients and VPN-1/FireWall-1 modules.

e) Invocation of a VPN facility which may be used to establish a secure communications channel between two Check Point FireWalls and also to establish a secure communications channel between a Check Point FireWall and a remote VPN-1 SecureClient allowing VPN remote access and secure connectivity for remote and mobile users.

f) Authentication of end-users which allows an administrator to grant users access privileges to specific client services based on a policy defined for the TOE; evaluation of this feature is to be to the interface level only, the actual authentication mechanism is not included as part of the evaluation.

2.2 TOE Exclusions

20 The authentication of end-users which allows an administrator to grant users access privileges to specific client services (please see Section 6.1.2.7 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.

21 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

22 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 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 15, 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 ITSEC E3 or 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 Getting Started with VPN-1/FireWall-1 [GET_START] and VPN-1/FireWall-1 Management and Administration [MANAGEMENT] and [OP_DOC] 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 and the *Desktop Security Policy* for the VPN-1 SecureClients 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 computer system is configured with the minimum of operating system features installed and the minimum of operating system features enabled to permit operation of the product (e.g. networking services, daemons and databases not required are removed).

[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 computer system, workstation or consoles and system devices.

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

[M_AS6] the administrators' use of privileged computer system accounts conforms to the site security policy.

[M_AS7] restrictions imposed by relevant security policies concerning the choice of the computer system password options (e.g. generation and ageing options) are enforced by the computer system configuration.

[M_AS8] guidelines consistent with the site security policy are followed for the computer system controlled ownership and restrictions on access to computer 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 computer system and product to be restored to a secure state after a failure of the computer system or product.

[M_AS10] appropriate use is made of the product'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 computer system 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 computer system, the 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

23 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.

24 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 two hosts each protected by VPN-1/ FireWall-1 firewalls

[T9] undetected attempts to modify the contents of data being transmitted between two hosts each protected by VPN-1/FireWall-1 firewalls

[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 a remote firewall:

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 a remote VPN-1/FireWall-1 firewall and the Management Server

[T14] undetected attempts to modify the contents of data being transmitted between a remote VPN-1/FireWall-1 firewall and the Management Server.

[T15] unauthorized access to one of the physically connected internal networks through a VPN-1 SecureClient machine

3.2 Organisational Security Policies

25 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

26 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 log and generate alerts for all attempts to communicate between physically connected networks

[SO5] invoke a Secure Internal Communications (SIC) facility for communication between Check Point Modules, i.e. Management Server, GUI clients, VPN-1/FireWall-1 modules

[SO6] invoke a Virtual Private Network (VPN) facility for communication between two VPN-1/FireWall-1 firewalls and between a VPN-1/FireWall-1 firewall and a remote VPN-1 SecureClient

[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* or *Desktop Security Policy*

[SO8] provide real-time monitoring of a centrally controlled distributed network of VPN-1/FireWall-1 firewalls.

4.2 Security Objectives for the Environment

27 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 15). (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, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage

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

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

(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 Check Point Modules, i.e. Management Server, GUI Clients, VPN-1/FireWall-1 modules 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 two VPN-1/FireWall-1 firewalls and between a VPN-1/FireWall-1 firewall and a remote VPN-1 SecureClient, 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* or *Desktop Security Policy*

[ESO6] Provide a reliable time stamping mechanism

5 IT Security Requirements

5.1 TOE Security Functional Requirements

28 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)'.

29 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)
FDP_IFC.1 (2)	Subset information flow control (Desktop Security Policy)
FDP_IFF.1 (2)	Simple security attributes (Desktop Security Policy)
FMT_MSA.1 (2)	Management of security attributes (Desktop Security Policy)
FMT_MSA.3 (2)	Static attribute initialization (Desktop Security Policy)
FDP_ACC.1	Subset access control (Policy Server)
FDP_ACF.1	Security attribute based access control (Policy Server)
FMT_MSA.1 (2b)	Management of security attributes (Policy Server)
FMT_MSA.3 (2b)	Static attribute initialization (Policy Server)
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(3)	Management of security attributes (Remote Monitoring)
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1(1)	Audit review (Authorised administrator)
FAU_SAR.1(2)	Audit review (SecureClient remote subscriber)
FAU_SAR.3	Selectable audit review
FMT_MOF.1 (2)	Management of security functions behaviour (Audit)

Table 5-1 TOE Security Functional Requirements

30 The TOE is associated with a number of different flow control and access control policies which regulate access to and through the various components of 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 Firewall Module.
- The DESKTOP-SFP, which controls the flow of network traffic to and from a SecureClient.
- The POLICY-SERVER-SFP, which controls the access of SecureClient components to a Policy Server component, in order to obtain a Desktop Security Policy.
- The SIC-SFP, which ensures that secure (TLS) connections are established between TOE components (apart from the SecureClients) and the Management Server.
- The VPN-SFP, which ensures that secure (IPSec) connections can be established between Firewall Modules and between Firewall Modules and SecureClients.

5.1.1 Flow Control VPN-1/Firewall Module

31 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.1.6b) and FDP_IFF.1.6c). 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 SPFs);

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-SPF 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].

32 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.

33 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.

5.1.2 Flow Control Secure Client

34 This section identifies the SFRs associated with the IP flow control function of the Secure Client components, namely the capability to enforce *Desktop Security Policies* that have been defined at the Management Server. The DESKTOP-SFP is the policy that models this aspect of information flow control. Since the Desktop Security Policies are stored within and downloaded from the Policy Server component of the TOE, the POLICY-SERVER-SFD also has to be defined to complete the model of *Desktop Security Policies*.

5.1.2.1 FDP_IFC.1 (2) Subset information flow control (Desktop Security Policy)

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

a) [subject: remote subscriber associated, via the relevant user group, with the Desktop Security Policy installed on the SecureClient;

b) information: traffic sent and received by the subject;

c) operation: pass information].

5.1.2.2 FDP_IFF.1 (2) Simple security attributes (Desktop Security Policy)

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

a) [subject security attributes: None.

b) information security attributes:

- transport layer protocol;
- TOE interface on which traffic arrives and departs, specifically whether the traffic is inbound or outbound to the workstation;
- 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) [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.]

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

FDP_IFF.1.4 The TSF shall provide the following [None].

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

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

5.1.2.3 FMT_MSA.1 (2) Management of security attributes (Desktop Security Policy)

FMT_MSA.1.1 The TSF shall enforce the [DESKTOP-SFP, POLICY-SERVER-SFP, 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 [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

35 Application Note: The DESKTOP-SFP facilitates the creation, modification and deletion of desktop security policy rules. Also, as a SecureClient obtains its operational Desktop Security Policy from the Policy Server and the POLICY-SERVER-SFP ensures that the policy provided to the SecureClient is that intended by the administrator, the FIREWALL-SFP is providing protection against unauthorised network access to the platform hosting the Policy Server, whilst the SIC-SFP is ensuring protected network access from the Management Server.

5.1.2.4 FMT_MSA.3 (2) Static attribute initialisation (Desktop Security Policy)

FMT_MSA.3.1 The TSF shall enforce the [DESKTOP-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.

36 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 desktop security policy (enforced during booting of the SecureClient and until a customised policy is downloaded from the Policy Server). 'Alternative initial values' refers to a customised desktop security policy.

5.1.2.5 FDP_ACC.1 Subset access control (Policy Server)

FDP_ACC.1.1 The TSF shall enforce the [POLICY-SERVER-SFP] on:

a) [subjects: SecureClient remote subscribers;

b) objects: Desktop Security Policy definition files located at a Policy Server; and

c) operation: validate and when required download remote subscriber Desktop Security Policy file.]

5.1.2.6 FDP_ACF.1 Security attribute based access control (Policy Server)

FDP_ACF.1.1 The TSF shall enforce the [POLICY-SERVER-SFP] to objects based on:

a) [subject security attributes: user credentials associated with the SecureClient remote subscriber,

b) object security attributes: the user group(s) identified in the Desktop Security Policy].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[The Desktop Security Policy definition file resident on the SecureClient will be used to check whether the Desktop Security Policy is valid for the remote subscriber and, when an invalid Desktop Security Policy is identified, the valid file will be downloaded to the SecureClient. This operation will be allowed if:

a) the purported user identity of the subject can be associated with the user group identified in the object; and

b) confirmation of successful authentication of the subject is received from an external authentication service invoked by the TOE.]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rule: [None.]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on [no explicit rules].

5.1.2.7 FMT_MSA.1 (2b) Management of security attributes (Policy Server)

FMT_MSA.1.1 The TSF shall enforce the [POLICY-SERVER-SFP, FIREWALL-SFP and SIC-SFP-] to restrict the ability to [create, modify or delete] the security attributes [Desktop Security Policy definition file objects described in FDP_ACC.1.1] to [the authorized administrator].

37 Application Note: The POLICY-SERVER-SFP facilitates the creation, modification and deletion of user groups. Also, the FIREWALL-SFP is providing protection against unauthorised network access to the platform hosting the Policy Server, whilst the SIC-SFP is ensuring protected network access from the Management Server.

5.1.2.8 FMT_MSA.3 (2b) Static attribute initialisation (Policy Server)

FMT_MSA.3.1 The TSF shall enforce the [SIC-SFP and FIREWALL-SFP] to provide [restrictive] default values for the 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.

38 Application Note: In practice until a Firewall platform has been specifically configured as a Policy Server and desktop security policy files have been installed, the POLICY-SERVER-SFP security attributes are null. These default values are restrictive as, in this situation, FMT_MSA.3 (2) holds. Installation of the desktop security policy files provides the alternative initial values.

5.1.3 Flow Control Secure Internal Communication

39 This section identifies the SFRs associated with the flow control function in relation to the Secure Internal Communication (SIC) between the Management Server and TOE components that directly communicate with the Management Server (i.e. the GUI, VPN-1/FireWall-1 module and Policy Server). 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.

5.1.3.1 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 physically separated TOE components that directly communicate with the Management Server].

40 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 5.4.2.

5.1.4 Flow Control VPN Connectivity

41 This section identifies the SFRs associated with the flow control function in relation to the Virtual Private Network (VPN) connections between the Firewall Module components and Secure Client/Firewall Module components of the TOE. 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.

5.1.4.1 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 between a Firewall Module component and a physically separated Firewall Module or SecureClient components of the TOE.]

42 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 5.4.3.

5.1.5 General Management Facilities

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

5.1.5.1 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 Firewall Module and Firewall Management Server components of the TOE, and indirectly, via the medium Desktop Security Policy validated from the Policy Server, the SecureClient components of the TOE]

to [an authorized administrator].

44 Application Note. The SIC-SFP ensures that access to these components is constrained to an authorized administrator.

5.1.5.2 FMT_MSA.1 (3) 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 a Firewall Module or a Secure Client] to [the authorized administrator.]

5.1.6 Audit

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

5.1.6.1 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].

5.1.6.2 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 be 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 or Desktop Security Policy, which have been specified as giving rise to an alarm.]

5.1.6.3 FAU_SAR.1 (1) Audit review (Authorized administrator)

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data arising from Firewall-1 modules and those audit events specified as alerts for a Secure Client (including reviewing in real time the audit records)] from the audit records.

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

5.1.6.4 FAU_SAR.1 (2) Audit review (SecureClient Remote Subscriber)

FAU_SAR.1.1 The TSF shall provide [a SecureClient Remote Subscriber] with the capability to read [all audit trail data arising from a SecureClient (including reviewing in real time the audit records)] from the audit records.

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

5.1.6.5 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [searches and sorting] of audit data based on:

a) [ranges of dates;

b) ranges of times; and

c) specified actions].

5.1.6.6 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.

b) switching of audit logs.]

to [an authorized administrator].

5.2 TOE Strength of Function Claim

5.2.1 Statement of SOF Claims

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

47 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

48 The security assurance requirements for the TOE comprise the requirements corresponding to the EAL4 level of assurance, as defined in [CC] Part 3. 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

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

5.4 Security Requirements for the IT Environment

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 (3)	Subset information flow control (SIC)
FDP_IFF.1 (3)	Simple security attributes (SIC
FCS_COP.1 (1)	Cryptographic Operation (SIC)
FDP_ITT.1 (2)	Basic internal transfer protection (VPN)
FDP_IFC.1 (4)	Subset information flow control (VPN)
FDP_IFF.1 (4)	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 Flow Control VPN-1/Firewall Module

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

FTP_ITC.1.1 The TSF shall provide a communication channel between itself 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 TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF 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)].

5.4.2 Flow Control Secure Internal Communication

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

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

FDP_ITT.1.1 The TSF 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

5.4.2.2 FDP_IFC.1 (3) Subset information flow control (SIC)

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

a) [subjects: Management Server and TOE components that directly communicate with the Management Server;

b) information traffic sent between the Management Server and another subject; and

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

5.4.2.3 FDP_IFF.1 (3) Simple security attributes (SIC)

FDP_IFF.1.1 The TSF 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 platforms hosting the TOE components.]

b) information security attributes: [none].]

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 can cause information to flow through their respective components of the TOE if based on the subjects certificates a trusted connection can be negotiated between the subjects via the TLS protocol]

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

FDP_IFF.1.4 The TSF shall provide the following [None].

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

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

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

FCS_COP.1.1 The TSF 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].

5.4.3 Flow Control VPN Connectivity

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

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

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

5.4.3.2 FDP_IFC.1 (4) Subset information flow control (VPN)

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

a) [subjects: Check Point Firewall Modules and SecureClient;

b) information: traffic sent between subjects; and

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

5.4.3.3 FDP_IFF.1 (4) Simple security attributes (VPN)

FDP_IFF.1.1 The TSF 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 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 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 establish an encrypted connection between the subjects via the IPSec protocol.]

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

FDP_IFF.1.4 The TSF shall provide the following [None].

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

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

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

FCS_COP.1.1 The TSF 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]

5.4.4 Authentication Services

52 These services are required to support FDP_IFF.1 (1) and FDP_ACF.1.

5.4.4.1 FIA_UAU.5 Multiple Authentication Mechanisms

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

FIA_UAU.5.2 The TSF 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.

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

FTP_ITC.1.1 The TSF shall provide a communication channel between itself 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 TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF 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.]

5.4.5 Audit

5.4.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF 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

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

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

a) Check Point Next Generation Getting Started Guide [GET_START]

b) Check Point Next Generation Management Guide [MANAGEMENT].

55 The statements and security functions in this Section are applicable to a product configuration and method of use which conforms to the intended method of use and environment, and associated assumptions, stated earlier in this Security Target.

6.1.2 Access Control

6.1.2.1 Access Control Administration

[AC1] The product shall provide the capability for administrators to:

a) start and stop the product

b) compile and load the *FireWall Security Policy* into the Management Server and then on to the VPN-1/FireWall-1 Module

c) compile and load the *Desktop Security Policy* (including user group definitions) into the Management Server and then on to the Policy Server for the VPN-1 SecureClients

d) apply address translation rules.

These concepts may be described as follows:

Compile means to create a virtual-machine language representation of the *FireWall Security Policy* and the *Desktop Security Policy* for VPN-1 SecureClients from INSPECT code

Load means to create INSPECT code from the text representation of the *FireWall Security Policy* or *Desktop Security Policy*, and transfer it from the Management Server onto the firewall (i.e. onto the VPN-1/FireWall-1 module in the case of the *FireWall Security Policy*, and onto the Policy Server in the case of the *Desktop Security Policy*)

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 or Desktop Security Policy* for the VPN-1 SecureClients

Start means to activate a firewall's security policy and begin *FireWall Security Policy* enforcement and to activate the VPN-1 SecureClient security policy and begin *Desktop 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

6.1.2.2 Traffic Flow Control

[AC2] The product shall enforce the *FireWall Security Policy* and the *Desktop Security Policy* for VPN-1 SecureClients (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 and the Desktop 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* and the *Desktop Security Policy* for VPN-1 SecureClients 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* and the *Desktop Security Policy* for VPN-1 SecureClients 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.

For the *Desktop 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.

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.

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 will 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.

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 the *Desktop Security Policy* for VPN-1 SecureClients 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).

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 to 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).

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*.

56 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].

6.1.2.10 Desktop Policy Server

[AC15] The TOE shall check whether the desktop security policy resident on the SecureClient is valid for the remote subscriber and, when an invalid policy is detected, will attempt to download the valid policy for the subscriber.

6.1.3 Data Exchange

[1] This is a publicly published protocol, see http://www.checkpoint.com/cvpopenspec/index.html

6.1.3.1 Data Confidentiality and Integrity

[VPN1] The product shall invoke establishment of secure and trusted VPN connections between FireWall module and physically-separated FireWall module or Secure Client.

6.1.4 Remote Supervision

[RS1] The product shall allow an administrator to view a representation of the current status of distributed, remote gateways on which FireWalls have been installed and on VPN-1 SecureClients on which Desktop Security Policy have been installed. 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 and a *Desktop Security Policy* on the VPN-1 SecureClient

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

d) the fact that a *Desktop Security Policy* was loaded on the VPN-1 SecureClient (the date the *Desktop Security Policy* was installed can be viewed on the VPN-1 SecureClient)

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

6.1.5 Secure Internal Communication

[SIC1] The product shall allow an administrator to invoke establishment of secure and trusted connections between GUI, FireWall and Management Server.

6.1.6 Audit

6.1.6.1 Audit Data Administration

[AUD1] The product shall provide the capability for administrators to:

a) specify the creation of audit records, logs, on the basis of individual access control *rule statements* of the *FireWall Security Policy* and the *Desktop Security Policy* for VPN-1 SecureClients.

b) specify the generation of audit alerts on the basis of individual access control *rule statements* of the *FireWall Security Policy* and the *Desktop Security Policy* for VPN-1 SecureClients.

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*, including that of VPN-1 SecureClients (audit records generated on the VPN-1 SecureClient can be stored locally or forwarded to the Management Server).

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 [MANAGEMENT] document in the Log Viewer section.

6.1.6.4 Displaying Audit Logs

[AUD4] The product shall provide the capability for an administrator to display on the Management Server, and a user to display on the VPN-1 SecureClient, audit records from the current or a specified audit log file in accordance with one or more of the following selection criteria:

a) audit records being recorded in real time to the current log file

b) audit records with specified *actions*

c) audit records logged after, before or between specified dates and/or times.

Audit records generated on the VPN-1 SecureClient and stored locally can be displayed only locally.

6.1.6.5 Maintaining Audit Log Files

[AUD5] The product shall provide the capability for an administrator to close the current audit log file and switch recording of audit records to a new audit log file on the Management Server, and to specify a policy for doing so on the VPN-1 SecureClient, which will be enforced after the Desktop Policy is loaded to the VPN-1 SecureClient.

6.1.6.6 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

57 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 strength of functionality is required by CC.

6.3 Assurance Measures

6.3.1 Statement of Assurance Measures

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

7 PP Claims

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

8 TOE Rationale

8.1 Security Objectives Rationale

8.1.1 Introduction

60 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.

61 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			
[T15]						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

62 It is asserted that all these assumptions are addressed by the environmental objectives [ES01], [ES02]. 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.

63 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]

64 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]

65 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]

66 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]

67 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]

68 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]

69 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]

70 [SO4] 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] incorporates requirements FAU_SAR.1 that enables monitoring of status of the audit log and FMT_MOF.1(2) that enable policy for closing and switching audit logs to be enforced by the TOE. 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]

71 The threat that unauthorised disclosure of information may occur when being transmitted between two hosts each protected by VPN-1/FireWall-1 firewalls, is addressed by [SO6] and [ESO4]. [SO6] enables the use of [ESO4] cryptographic measures to protect the confidentiality of information transmitted between the instantiations of the firewall components of the product.

8.1.11 [T9]

72 The threat that there could be undetected attempts to modify the contents of data being transmitted between two hosts, each protected by VPN-1/FireWall-1 firewalls, is addressed by [SO6] and [ESO4]. [SO6] enables the use of [ESO4] cryptographic measures to protect the integrity of data transmitted between the instantiations of the firewall components of the product.

8.1.12 [T10]

73 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]

74 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]

75 [SO8] and [ESO2] address the threat that problems with unavailability of a remote firewall 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]

76 [SO5] and [ESO3] address the threat that there could be unauthorised disclosure of information being transmitted between a remote VPN-1/FireWall-1 firewall and the Management Server. [SO5] enables the [ESO3] establishment of a trusted secure communications channel between the product’s modules and this requirement includes the use of cryptographic measures to protect the confidentiality and integrity of information transmitted.

8.1.16 [T14]

77 [SO5] and [ESO3] address the threat that there could be undetected attempts to modify information being transmitted between a remote VPN-1/FireWall-1 firewall and the Management Server. [SO5] enables the [ESO3] establishment of a trusted secure communications channel between the product's components and this requirement includes the use of message digests to detect integrity violations.

8.1.17 [T15]

78 The threat that there could be unauthorised attempts to access one of the physically connected internal networks through a VPN-1 SecureClient machine is addressed by [SO6] which enables [ESO4].

8.2 Security Requirements Rationale

8.2.1 Introduction

79 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

80 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							
FDP_IFC.1 (2)	X							
FDP_IFF.1 (2)	X							
FMT_MSA.1 (2)	X							
FMT_MSA.3 (2)	X							
FDP_ACC.1	X							
FDP_ACF.1	X						X	
FMT_MSA.1 (2b)	X							
FMT_MSA.3 (2b)	X							
EDP_ITT1(1)EXP					X			
EDP_ITT1(2)(EXP)						X		
FMT_MSA.1 (3)								X
FAU_GEN.1				X				
FAU_SAA.1				X				
FAU_SAR.1(1)				X				
FAU_SAR.1(2)				X				

	[SO 1]	[SO2]	[SO3]	[SO4]	[SO5]	[SO6]	[SO7]	[SO8]
FAU_SAR.3				X				
FMT_MOF.1 (2)				X				

Table 8-2 Requirements Rationale Mapping

8.2.3 [SO1]

81 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 and FDP_IFC.1 (2), FDP_IFF.1 (2), FMT_MSA.1 (2), FMT_MSA.3 (2), FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 (2b), FMT_MSA.3 (2b) identify the information flow requirements for the Desktop Security Policies. The Firewall and Desktop Security Policies are directly concerned with the flow control of the IP based packets at the TOE Firewall Modules and Secure Clients, and so address this objective.

8.2.4 [SO2]

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

8.2.5 [SO3]

83 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]

84 FAU_GEN.1, FAU_SAA.1, FAU_SAR.1(1), FAU_SAR.1(2), FAU_SAR.3, FMT_MOF.1 (2) identify the requirement to configure, generate and inspect logs and alerts to meet this objective.

8.2.7 [SO5]

85 EDP_ITT(1)(EXP) identifies the requirement to support trusted channels between the TOE components 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]

86 EDP_ITT.1(2)(EXP) identifies the requirement to support VPN connections, between the TOE Firewall Module and other TOE Firewall Modules or Secure 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]

87 FDP_IFF.1 (1) and FDP_ACF.1 identify the requirement to access to external services supported by the TOE and thereby address this objective.

8.2.10 [SO8]

88 FMT_MSA.1(5) identify the requirement to monitor all the installed product components in real-time and so directly addresses this objective.

8.2.11 IT Environment Functional Requirements Rationale

89 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.

90 Note that environmental objectives [ESO1] and [ESO2] are primarily concerned with physical, procedural and personnel objectives, and relate only indirectly to the IT. These objectives do not therefore map to environmental SFRs.

	[ESO 3]	[ESO4]	[ESO5]	[ESO6]
FTP_ITC.1 (1)			X	
FDP_ITT.1 (1)	X			
FDP_IFC.1 (3)	X			
FDP_IFF.1 (3)	X			
FCS_COP.1 (1)	X			
FDP_ITT.1 (2)		X		
FDP_IFC.1 (4)		X		
FDP_IFF.1 (4)		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]

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

8.2.13 [ESO4]

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

8.2.14 [ESO5]

93 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]

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

8.2.16 Security Requirements Dependencies Rationale

95 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 third 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)	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
FDP_IFC.1 (2)	FDP_IFF.1(2)		
FDP_IFF.1 (2)	FDP_IFC.1(2), FMT_MSA.3(2)		
FMT_MSA.1 (2)	FDP_ACC.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3)	FMT_SMR.1	Note 1
FMT_MSA.3 (2)	FMT_MSA.1(2)	FMT_SMR.1	Note 1
FDP_ACC.1	FDP_ACF.1		
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3(2b)		
FMT_MSA.1 (2b)	FDP_ACC.1, FDP_IFC.1(1), FDP_IFC.1(3)	FMT_SMR.1	Note 1
FMT_MSA.3 (2b)	FDP_IFC.1(1), FDP_IFC.1(3), FMT_MSA.1(2b)	FMT_SMR.1	Note 1.
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_SMR.1	Note 1
FMT_MSA.1 (3)	FDP_IFC.1(3)	FMT_SMR.1	Note 1
FAU_GEN.1	FPT_STM.1		
FAU_SAA.1	FAU_GEN.1		
FAU_SAR.1(1)	FAU_GEN.1		
FAU_SAR.1(2)	FAU_GEN.1		
FAU_SAR.3	FAU_SAR.1		
FMT_MOF.1 (2)		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 (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(1)		FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Note 4
FDP_ITT.1(2)	FDP_IFC.1 (4)		
FDP_IFC.1 (4)	FDP_IFF.1 (4)		
FDP_IFF.1 (4)	FDP_IFC.1 (4)	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

96 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 a platform hosting one of the relevant components of the TOE, e.g. the host for the Management GUI, or the Management Server components. 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

97 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

98 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.

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

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

101 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

102 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

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

104 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.
FMT_MSA.3 (1)	AC2	
FDP_IFC.1 (2)	See FDP_IFF.1(2)	
FDP_IFF.1 (2)	AC2, AC3, AC4	The Desktop Security Policy provides a cut down version of the functionality provided by Firewall Modules.
FMT_MSA.1 (2)	AC1	The various SFs associated with the FIREWALL-SFP, POLICY-SERVER-SFP and SIC-SFP also support this functionality.
FMT_MSA.3 (2)	AC2	
FDP_ACC.1	See FDP_ACF.1	
FDP_ACF.1	AC10, AC11, AC15	User authentication serves two purposes in the TOE, the first being to allow access to services external to the TOE that require authentication and the second to authenticate access to the TOE's Policy Server prior to validation/download of a Desktop Security Policy. This security relates to the second case.
FMT_MSA.1 (2b)	AC1	The various SFs associated with the FIREWALL-SFP and SIC-SFP also support this functionality.
FMT_MSA.3 (2b)	AC2	
EDP_ITT.1 (1)	SIC1	
EDP_ITT.1 (2)	VPN1	
FMT_MOF.1 (1)	AC1	
FMT_MSA.1 (3)	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	
FAU_SAR.1(1)	AUD4	

TOE Security Functional Requirements	TOE Security Functions	Comments
FAU_SAR.1(2)	AUD4	
FAU_SAR.3	AUD4	
FMT_MOF.1 (2)	AUD1, AUD2, AUD5	

Table 8-5 TOE Summary Specification Rationale Mapping

8.3.2 Strength of Function Claims are Appropriate

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

8.3.3 TOE Assurance Measures

106 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.
Desktop 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 the VPN-1/FireWall-1 firewall and the VPN-1 SecureClient, located on a physically connected network, yet outside of the protected LAN. The overall Desktop Security Policy will comprise definitions of a number of user groups, to be assigned various access rights, and the component Desktop Security Policies defined for these user groups.
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:

a) IP protocol

b) source IP address

c) destination IP address

d) service or destination TCP/UDP port

e) source TCP/UDP port

f) IP length

g) *FireWall Security Policy rule statement* number

If Address Translation is active, the following additional information:

a) original source IP address

b) original destination IP address

c) original source port (UDP/TCP)

d) 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.
Remote Subscriber	A person or service which communicates remotely (outside of the protected LAN) through a firewall module protecting a physically connected internal network and whose communication is subject to the *Desktop Security Policy*, the *FireWall Security Policy* for VPN-1 SecureClients.
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* or *Desktop 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*.
Symmetric Encryption	Refers to the use of an algorithm to encrypt and decrypt data which requires the same key to encrypt and decrypt the data.