UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P172

Check Point VPN-1/FireWall-1 Next Generation (NG)

Feature Pack 1 (FP1)

Running on specified platforms

Issue 2.0

February 2003

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 144
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

Check Point Software Technologies Limited's VPN-1/FireWall-1 Next Generation (NG) is a software-based firewall application which provides controlled access between physically connected networks by permitting or denying the flow of packets. It also provides IP address translation, IP address hiding and the logging of all attempts to communicate between physically connected networks. In addition, it can operate as a virtual private network which is used to establish a secure communications channel over an unsecured network using 2 installations of the VPN-1/FireWall-1 firewall. The VPN facility is also used to establish a secure communications channel between a VPN-1/FireWall-1 and a VPN-1 SecureClient allowing remote access and secure connectivity for remote and mobile users.

Check Point VPN-1/FireWall-1 Next Generation (NG) with Feature Pack 1 (FP1) has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality when running on the platforms specified in Annex A and in a 'trusted configuration' as defined in the Security Target and summarised in paragraph 11 of this report.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation Certification Scheme
Date authorised	25 February 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AES	Advanced Encryption Standard
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CMT	Cryptographic Module Testing
CMV	Cryptographic Module Verification
CVP	Content Vectoring Protocol
DES	Data Encryption Standard
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
FP	Feature Pack
FTP	File Transfer Protocol
GUI	Graphical User Interface
IKE	Internet Key Exchange
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
NG	Next Generation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
SFR	Security Functional Requirement
SIC	Secure Internal Communications
SMTP	Simple Mail Transfer Protocol
SoF	Strength of Functions
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication
VPN	Virtual Private Network

(This page is intentionally left blank)

REFERENCES

a. Common Criteria EAL4 Evaluation VPN-1/FireWall-1 Next Generation (FP1) Security Target,
Check Point Software Technologies Limited,
Issue 1.8, 24 February 2003.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

f. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Certification Report P166, Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, May 2002.

i. Task LFD/T316 Evaluation Technical Report,
Electronic Data Systems Limited,
P14784/EVAL/R-02/01, Issue 1.0, March 2002.

j. Task LFD/T317 (Phase 1) Evaluation Technical Report,
Electronic Data Systems Limited,
P16759/EVAL/R-02/01, Issue 1.0, May 2002.

k. LFD/T317 (Phase 1) Supplement to Evaluation Technical Report,
Electronic Data Systems Limited,
P16759/EVAL/A-02/02, Issue 1.0, December 2002.

l. LFD/T317 - Re-evaluation of Security Target,
Electronic Data Systems Limited,
P16759/EVAL/A-02/09, 25 February 2003.

m. Certification Report P172, Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2002.

n. UKSP14 Addendum: EAL4 Delta Evaluation,
UK IT Security Evaluation and Certification Scheme,
Issue 2.C, 21 March 2000.

o. ITSEC E3 Secure Delivery - VPN-1/FireWall-1 NG ITSEC E3 Evaluation,
Check Point Software Technologies Limited,
Version 1.0, 19 November 2001.

p. Check Point VPN-1/FireWall-1 NG FP1 System Generation/Installation Guide for ITSEC E3,
Check Point Software Technologies Limited,
Version 1.2, 3 March 2002.

q. Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1) ITSEC E3 Release Notes,
Check Point Software Technologies Limited,
November 2001 (last update - 25 April, 2002).

r. Check Point Getting Started Guide, NG FP1,
Check Point Software Technologies Limited,
Part No. 700360, November 2001.

s. Check Point Desktop Security, NG,
Check Point Software Technologies Limited,
Part No. 700361, November 2001.

t. Check Point FireWall-1 Guide, NG FP1,
Check Point Software Technologies Limited,
Part No. 700349, November 2001.

u. Check Point Management Guide, NG FP1,
Check Point Software Technologies Limited,
Part No. 700348, November 2001.

v. Check Point Reference Guide, NG,
Check Point Software Technologies Limited,
Part No. 700351, November 2001.

w. Check Point User Management, NG,
Check Point Software Technologies Limited,
Part No. 700268, June 2001.

x. Check Point Virtual Private Networks, NG,
Check Point Software Technologies Limited,
Part No. 700350, November 2001.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Check Point VPN-1/FireWall-1 Next Generation (NG) with Feature Pack 1 (FP1) to the Sponsor, Check Point Software Technologies Limited, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

   Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1).

The Developer was Check Point Software Technologies Limited.

4. The product operates in 2 modes:

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

   b. as a Virtual Private Network (VPN) which is used to establish a secure communications channel over an unsecured network (eg the Internet) using 2 Check Point Firewalls.

The product's firewall functionality and the invocation of the product's VPN functionality are the subject of this evaluation. This functionality, as described in the Security Target [a], is also described in this report as the Target of Evaluation (TOE). The product's cryptographic functionality is outside the scope of this evaluation. (See section "Strength of Function Claims" for details of FIPS testing of the product.)

5. By installing the TOE on a gateway, it can be used as a firewall to supervise all traffic passing between connected networks. It uses Stateful Inspection Technology to inspect packets and ensure that only communications from permitted hosts, accessing services permitted for those hosts, are allowed to pass. A network behind the gateway may thus be protected against attack or unauthorised access originating beyond the gateway.

6. The TOE has four main components:

   a. a Graphical User Interface (GUI);

   b. a Management Server;

   c. one or more Firewall modules; and

d. one or more SecureClients.

7. The product can also operate as a VPN which is used to establish a secure communications channel over an unsecured network (eg the Internet) using 2 installations of the VPN-1/FireWall-1 firewall. The VPN facility is also used to establish a secure communications channel between a VPN-1/FireWall-1 firewall and a remote VPN-1 SecureClient allowing remote access and secure connectivity for remote and mobile users.

8. The product is designed to operate in a distributed configuration, providing centralised management of multiple firewall enforcement points (gateways), as well as centralised management of remote VPN clients.

9. Details of the evaluated version of the TOE and of trusted configurations of the product are contained in the Security Target [a] and summarised in Annex A to this report.

10. An overview of the Product's security architecture can be found in Annex B.

TOE Scope

11. Section 2.1.1.2 of the Security Target [a] defines a 'trusted configuration' of Check Point VPN-1/FireWall-1 NG FP1 as follows:

a. executes on any computer system from the family of workstations and servers which supports one of the following operating systems (subject to the considerations of the Getting Started Guide [r] and the System Generation/Installation Guide [p]. See the section "Platform Issues" in Annex C for further details of the evaluated configuration):

   i. SUN Solaris 8

   ii. Microsoft Windows NT4 SP6a

b. executes on a computer system which supports up to 128 port connections (note that the VPN-1/FireWall-1 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 which resides on a protected LAN;

   ii. a Graphical User Interface which resides on a separate workstation running Microsoft Windows NT which is part of the protected LAN the Management Server is part of;

   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 FireWall Modules which may or may not reside on the protected LAN the Management Server is part of; and

v. a Policy Server installed on a VPN-1/FireWall-1 machine which resides on the protected LAN that the Management Server is part of.

d. is configured, controlled and monitored using the GUI 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 Secure Client(s).

e. has been delivered and installed in accordance with the specific documentation relating to an ITSEC E3-compliant installation [o - q] and is configured and used in accordance with the operations documentation [r - x].

12. The following features and facilities of Check Point VPN-1/FireWall-1, NG FP1 were addressed during the evaluation:

- Network security provided by Firewall and *remote* Desktop (SecureClient) components (note: Desktop SecureClient components that are part of the *local* LAN were outside the scope of the evaluation)
- Remote Management capability, including separate GUI management client
- Security Server functionality (note: the actual services for which the Security Server is used to arbitrate requests were outside the scope of the evaluation)
- LDAP client interface
- CVP interface
- End-user authentication (to interface level only - the actual authentication mechanism was outside the scope of the evaluation)
- Content analysis (to interface level only)
- Auditing

13. The following features and facilities of Check Point VPN-1/FireWall-1 NG FP1 were outside the scope of the evaluation:

- LDAP Server
- Authentication agent
- Secure internal communications
- VPN facility
- Content Verification Server
- Service Servers eg FTP, SMTP
- SYNDefender
- load balancing

14. In addition, all platforms other than those identified in paragraph 11.a above are outside the scope of this evaluation.

Protection Profile Conformance

15. The Security Target [a] did not claim conformance to any protection profile.

Assurance

16. The Security Target [a] specified the assurance requirements for the evaluation. Predefined Evaluation Assurance Level EAL4 was used. Common Criteria Part 3 [d] describes the scale of assurance given by predefined levels EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

17. The minimum Strength of Function (SoF) claimed for the TOE was SoF-Medium. This was not related to any specific security functions.

18. The Cryptographic mechanisms (MD5, AES, SHA, RSA, IKE, Diffie Hellman, DES and Triple DES) are implemented within the product. These mechanisms are used to implement the Secure Internal Communications (SIC) and VPN and are outside the scope of the evaluation.

19. The product has been tested by a NIST NVLAP-accredited Cryptographic Module Testing (CMT) laboratory under the Cryptographic Module Verification (CMV) programme and validated by NIST (Certificate number 234) as complying with the requirements of FIPS 140-1 level 2. The Validation Report states that the TOE contains the FIPS-approved algorithms DES (Cert #142), Triple-DES (Cert #80) and SHA-1 (Cert #69) with RSA (PKCS #1 vendor affirmed) and HMAC-SHA-1 (Cert #69, vendor affirmed). Some mechanisms within the product are non-FIPS-approved.

Security Policy

20. The TOE Security Policy may be deduced from the Security Target [a]. There are no Organisational Security Policies with which the TOE must comply.

Security Claims

21. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and Security Functional Requirements (SFR) and security functions to elaborate the objectives.

22. With the exception of EDT_ITT.1(1) and EDT_ITT.1(2), all of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products. EDT_ITT.1(1) and EDT_ITT.1(2) are fully defined in Section 5.1.3 of the Security Target [a].

23. Security functionality claims are made for IT security functions grouped under the following 5 categories:

- Access Control
- Audit
- Remote Supervision
- Secure Internal Communication
- Data Exchange

Evaluation Conduct

24. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [e, f]. The Scheme has established a Certification Body which is jointly managed by CESG and the Department of Trade and Industry on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

25. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [d] and the Common Evaluation Methodology (CEM) [g].

26. The TOE Security Functions (TSF) and security environment, together with much of the supporting evaluation deliverables, remained largely unchanged from the evaluation of the TOE previously certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 assurance level [h]. For this evaluation of Check Point VPN-1/FireWall-1 Next Generation (NG) with Feature Pack 1 (FP1), the Evaluators addressed every CEM [g] EAL4 work unit but made use (with guidance provided in [n]) of the evaluation results [i] from the ITSEC E3 evaluation where these were valid for the CEM requirements.

27. The Certification Body monitored the evaluation which was carried out by the Electronic Data Systems Limited Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [j] to the Certification Body in May 2002. The Certification Body then produced Issue 1.0 of this Certification Report [m]. As a result of clarification of the Security Target [a], the evaluators issued a supplement to the ETR [k] and confirmed [l] that the previous evaluation results hold with respect to the revised Security Target. The Certification Body then produced this Certification Report.

General Points

28. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

29. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of issue 1.0 of this Certification Report. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should

check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

30. The issue of a Certification Report is not an endorsement of a product.

II. EVALUATION FINDINGS

Introduction

31. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [j] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to consumers of the TOE.

Delivery

32. The secure delivery of the TOE is described in [o] (which can be found on website www.checkpoint.com/techsupport/documentation/certdocs). The delivery instructions are summarised below.

33. Check Point ships its products in formal company packaging which clearly indicates the product type and manufacturer. The supplied packaging includes documentation and a media kit.

34. The media kit and user documentation is shrink wrapped both for physical protection and to provide additional assurance that the contents have not been tampered with.

35. As part of the installation procedure of Check Point VPN-1/FireWall-1 it is necessary for the purchaser to enter their licence details. Obtaining licences is described in detail in [r]. Notably the permanent licence required to install the product will only be provided to a purchaser once the product is registered on Check Point's Web Site. Registration will require entry of user details along with a unique Certificate Key which is provided on the CD-ROM case.

Installation and Guidance Documentation

36. Check Point's Getting Started Guide [r] provides procedures for system generation (installation). In addition, Check Point have provided;

a. Release Notes [q] (which contain information on the supported platforms (operating systems) and avoidance of known product limitations and problems); and

b. a System Generation/Installation Guide for ITSEC E3 [p]

specifically to define an ITSEC E3 evaluated configuration which is identical to a CC EAL4 evaluated configuration as the product and method of use are identical in both cases. References [p] and [q], together with the Secure Delivery document [o] are available on the web site www.checkpoint.com/techsupport/documentation/certdocs.

37. The system generation procedures describe the installation pre-conditions (eg removing any services on the VPN-1/FireWall-1 machine that are not required and might be a security risk, confirming that routing and DNS are correctly configured, disabling IP forwarding, etc). They describe the requirements for setting up administrator accounts/permissions, secure internal communications and security policies, removing temporary files, etc.

38. Procedures for secure operation of the TOE are described throughout the product manuals ([r - x]). The Getting Started Guide [r: Chapter 6] provides a tutorial covering aspects of the TOE such as building security policies, use of network address translation, creation of users, defining rule bases and viewing logs.

Strength of Function

39. The SoF claim for the TOE was as given above under "Strength of Function Claims" above. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that the SoF claim of SoF-Medium was therefore upheld.

Vulnerability Analysis

40. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

III. EVALUATION OUTCOME

Certification Result

41. After due consideration of the ETR and Supplement [j, k], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Check Point VPN-1/FireWall-1 Next Generation (NG) with Feature Pack 1 (FP1) meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality when running on the platforms specified in Annex A and in a 'trusted configuration' as defined in the Security Target [a] and summarised in paragraph 11 of this report.

42. The Certification Body has also determined that the TOE meets the minimum SoF claim of SoF-Medium given above under "Strength of Function Claims".

Recommendations

43. Prospective consumers of Check Point VPN-1/FireWall-1 Next Generation (NG) with Feature Pack 1 (FP1) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. In particular, prospective consumers should note that, as stated in paragraph 4 above, the product's cryptographic functionality is outside the scope of this evaluation

44. The Product should be used in accordance with a number of environmental considerations as specified in sections 3.1 and 5.4 of the Security Target. Particular care should be taken that the product is delivered installed and used in accordance with the supporting guidance documentation [o - x].

45. Only a 'trusted configuration' of the TOE should be installed. This is defined in the Security Target [a] and summarised in paragraph 11 above.

46. Consumers of the TOE should note, also, that the underlying operating system and the underlying hardware platform are required to function correctly in order to support the method of use assumptions that contribute to the secure operation of the TOE.

47. Administrators should be aware that the TOE does not counter the threat that a firewall module could be bypassed by connecting the internal network directly to an external network. It is recommended that the TOE is placed in a physically secure environment to which only authorised personnel have access and that internal users are prevented from connecting their workstations or servers to the external network by any link (eg a modem) that does not pass through a firewall module that is part of a trusted configuration of VPN-1/FireWall-1 NG FP1.

48. Consumers should note that the administrators of the TOE are assumed to be trusted individuals who are appropriately vetted and trained. The TOE does not counter threats from careless, negligent or hostile administrators. It is recommended that appropriate measures, including regular, independent audits of the firewall configuration, be taken to counter these threats.

49. Firewall flow policies are complex and they need to be tailored to fit specific requirements. Consumers of the TOE should ensure that administrators are competent to determine the firewall flow policies to be implemented or have access to people who are competent to determine such policies.

50. Administrators should be aware that a firewall does not prevent malicious users on the internal network colluding with hostile attackers on the external network if the user is authorised to access and send the information to external hosts.

51. Administrators are recommended to inspect the TOE's audit trails on a regular basis and, also, to inspect, on a regular basis, the installed FireWall Security Policies and Desktop Security Policies to ensure that they remain correct.

52. Administrators should take particular care to ensure that IP forwarding is enabled in the TOE's computer system only when VPN-1/FireWall-1 is running and is disabled when VPN-1/FireWall-1 is not running, otherwise IP packets may be forwarded by the underlying operating system while the firewall is not running. Administrators should note that this is accomplished differently in NT and in Solaris. Instructions to achieve this are given in [p].

53. Potential consumers of the TOE should be aware that the TOE does not claim to resist all denial-of-service attacks. Whilst the TOE does contain functionality to counter attacks using fragmented or overlapping IP packets, SYN flooding attacks are outside the scope of this evaluation because the SYNDefender functionality was not included in this evaluation.

54. Potential consumers should note that the VPN-1/FireWall-1, in common with similar TOEs, does not counter the threat of Session Hi-jacking (ie an external attacker taking over an authenticated session initiated by another external host) unless using VPN-1 SecureClient for remote access to the protected network. This threat should be considered when defining the internal network security policy.

55. To reduce the potential impact of Session Hi-jacking, it is recommended that the internal network security policy states what executable software is authorised to be received through the firewall from the external network. Corresponding operational procedures to quarantine such software may also be required.

56. To detect whether Session Hi-jacking has affected the firewall, it is recommended that a backup of the firewall in its initial operational configuration is retained and used for comparison at periodic intervals. Operational procedures should state when this comparison is to be made.

57. Potential consumers should be aware that the TOE does not detect viruses. It is recommended that executable programs attached to incoming mail messages should be virus checked. Automatic explosion or execution of MIME-encoded attachments within SMTP messages should also be disabled.

58. Administrators should note that whilst VPN-1/FireWall-1 NG FP1 can coexist within the same network as VPN-1/FireWall-1 Version 4.1 provided each are configured, and their security policies defined, according to their evaluated configurations, the backward compatibility of VPN-1/FireWall-1 NG FP1 to manage VPN-1/FireWall-1 Version 4.1 is not within the scope of

this evaluation and certification. It follows, therefore, that VPN-1/FireWall-1 Version 4.1 cannot be part of an evaluated configuration of VPN-1/FireWall-1 NG FP1.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1)

Note that the scope of the evaluation is described in the section “Evaluated Product” above.

TOE Documentation

2. The supporting guidance documents evaluated were:

- ITSEC E3 Secure Delivery - VPN-1/FireWall-1 NG ITSEC E3 Evaluation [o]
- Check Point VPN-1/FireWall-1 NG FP1 System Generation/Installation Guide for ITSEC E3 [p]
- Check Point VPN-1/FireWall-1 Next Generation (NG) Feature Pack 1 (FP1) ITSEC E3 Release Notes [q]
- Check Point Getting Started Guide, NG FP1 [r]
- Check Point Desktop Security, NG [s]
- Check Point FireWall-1 Guide, NG FP1 [t]
- Check Point Management Guide, NG FP1 [u]
- Check Point Reference Guide, NG [v]
- Check Point User Management, NG [w]
- Check Point Virtual Private Networks, NG [x]

3. Further discussion of the supporting guidance material is given in Section II under the heading “Installation and Guidance Documentation” above.

TOE Configuration

4. The TOE should be configured in accordance with the guidance documents identified in paragraph 2 above.

Environmental Configuration

5. The TOE executes on a wide range of computer systems from the family of workstations and servers which supports one of the following operating systems:

- SUN Solaris 8
- Microsoft Windows NT4 SP6a

6. Chapter 4 of [r] provides guidance on minimum NT and Solaris hardware requirements for the Management Server, FireWall Module and GUI, in terms of disk space, memory and processor speed.

7. The product executes on a computer system which supports up to 128 port connections (note that the VPN-1/FireWall-1 uses the concept of managed ports and does not use the traditional firewall terms of *internal* and *external* network).

8. See, also, the section "Platform Issues" in Annex C for discussion of the issues relating to the hardware platforms.

9. The Developer supplied the following platforms for the Evaluators' functional and penetration testing at the Developer's Cambridge site:

- Two generic Intel machines, each with dual Pentium III processors, 512Mb RAM, hard disk, CD ROM drive, floppy drive and 9 NICs. These machines were each pre-installed with Windows NT4.0 with SP6a.

- One Sun Ultra 10 with 128 Mb RAM, hard disk, CD ROM drive, floppy drive and 8 NICs. This machine was pre-installed with Sun Solaris 8.

- One Dell Latitude laptop with Pentium processor, 128Mb RAM, hard disk, CD ROM drive, floppy drive and 1 NIC. This machine was pre-installed with Windows NT4.0 with SP6a.

10. The above platforms were configured as follows:

- The TOE 'GUI' and 'Management Server' were installed on one generic Intel machine
- The TOE 'Firewall' modules were installed on one generic Intel machine and SUN machine, and configured in a VPN.
- The TOE 'SecureClient' was installed on the Dell laptop and configured in a VPN with a Firewall machine.

11. In addition, initially, the Dell laptop was installed as a separate GUI to enable the evaluation team to observe the operation of the TOE in a fully-distributed configuration.

12. The Developer performed installation and configuration of the TOE on all the above platforms. The Evaluators, as part of their verification of the installation instructions, witnessed installation and configuration on a number of platforms at both Check Point's Ramat Gan and Cambridge offices.

13. In addition, the Evaluators used the following items during penetration testing:

- One Compaq Armada E500 laptop, dual boot, running Windows 2000/Red Hat Linux 7.2
- Two Dell Latitude laptops, dual boot, running Windows 2000/Red Hat Linux 7.2
- Network hubs
- Software Tools: Network Associates Cybercop 5.5
  Nessus 1.1.10
  Nmap 2.54 beta
  wu-ftp server and tftp server.

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the product. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. The product operates in a distributed configuration which consists of:

- A **Management Server** residing on a protected LAN
- A **Graphical User Interface** (GUI) residing on a separate workstation, but on the same protected LAN as the Management Server
- A number of **Firewall modules**, controlled by the Management Server, which may or may not reside on the same protected LAN as the Management Server
- A **Policy Server** residing on a Firewall module machine on the same protected LAN as the Management Server
- A **VPN-1 SecureClient** residing on a remote client outside the protected LAN

Design Subsystems

3. The product is made up of 2 major components:

a. VPN-1/FireWall-1 Firewall; and

b. VPN-1 SecureClient

Note that the evaluation covers the product's firewall functionality and invocation of the product's VPN functionality. The VPN functionality is outside the scope of the evaluation.

4. **VPN-1/FireWall-1 Firewalls** consist of the following components:

a. **GUI** - the graphical interface engaged by the administrator. This is the original point of entry of a Firewall Security Policy and is the interface and terminus for viewing log files and receiving graphical alerts.

b. **Management** - A component on the Management Server which centrally manages one or more firewall modules, each of which may be physically distributed. It receives instructions from a (possibly remote) GUI and distributes these to the firewall machines. It centrally receives and processes log/alerts from the distributed firewalls, and alerts from the VPN-1 SecureClients.

c. **FireWall Kernel** - The main packet filtering/transforming component. Located within the operating system kernel of each firewall gateway, it intercepts packet flows between NICs and IP modules. This component is where filtering and address translation are performed on packets.

d. **VPN Kernel** - The main cryptographic component where encryption operations are performed on packets and VPN aspects of the Security Policy are enforced.

Performs IPSec processing on packets according to the Security Policy and reports auditable events to the FireWall Daemon. (The scope of the TOE only extends to invocation of VPN functionality).

e. **FireWall Daemon** - Exists on every Management Server and every VPN/Firewall machine. On VPN/Firewall machines, receives and installs the Firewall Security Policy on the Kernel, and processes logs, alerts and traps generated by the Kernel. On the Management Server, receives transmitted logs/alerts, writing logs to a file and issuing the alerts, and transmits the Firewall Security Policy to the VPN/Firewall machines.

f. **VPN Daemon** - Negotiates the IPSec Security Association with IKE peers, sends logs to the FireWall Daemon, registers the VPN Kernel to the FireWall Kernel when VPN-1/FireWall-1 is started. Handles requests (traps) from the VPN Kernel for new IPSec Security Associations. (The scope of the TOE only extends to invocation of VPN functionality).

g. **Utilities** - Resides on the Management Server, and is involved in compiling and loading the Firewall Security Policy and Desktop Security Policy. Provides a command-line interface means of engaging Management Server functionality.

h. **Security Server** - Used for user authentication or for when the communication content requires analysis at levels higher than feasible within the Kernel; eg to scan ftp protocol streams for GETs and PUTs. Resides on the VPN/FireWall machine.

i. **Auth Agent** - An agent installed on hosts which provides a means for a VPN/FireWall machine to session-authenticate such hosts. (This functionality is outside the scope of the evaluation.)

j. **Policy Server** - The component that receives the Desktop Security Policies from the Management Server and delivers them to VPN-1 SecureClients, and collects alert data from VPN-1 SecureClients and sends it to the Management Server.

5. **VPN-1 SecureClients** consist of the following components:

a. **SecureClient Kernel** - The main component that enforces the VPN-1 Policy and the Desktop Security Policy. Located within the operating system kernel of each SecureClient, it inspects every incoming and outgoing packet, and decides whether to drop it, accept it, or encrypt/decrypt it.

b. **SecureClient VPN Kernel** - Performs and enforces the VPN and cryptographic aspects of encrypted communication, in much the same way as the VPN Kernel on the VPN-1/FireWall machine. (The scope of the TOE only extends to invocation of VPN functionality).

c. **SecureClient Daemon** - Negotiates the IPSec Security Association with IKE peers, gets Desktop Security Policies from the Policy Server and loads them into the SecureClient Kernel, and collects alerts from the SecureClient Kernel and transfers

them to the Policy Server. (The scope of the TOE only extends to invocation of VPN functionality).

d. **SecureClient VPN Daemon** - Responsible for VPN related tasks and registering the SecureClient VPN Kernel to the SecureClient Kernel when VPN-1 SecureClient is started. (The scope of the TOE only extends to invocation of VPN functionality).

e. **SecureClient GUI** - The graphical interface engaged by the VPN-1 SecureClient user. It is also the interface and terminus for viewing SecureClient log entries and receiving popup alerts.

Hardware and Firmware Dependencies

6. The product relies on the correct operation of the platform's hardware and firmware but otherwise has no security dependencies on the platform's hardware or firmware.

TSF Interfaces

7. The external interfaces for the VPN-1/FireWall-1 are as follows:

a. the GUI, the administrator's graphical point of access (using windowing functionality) for interacting with the product.

b. Command Line Interface - the more expert administrator's means of interacting with the product, using command-line instructions.

c. Interface for packets on the Firewall machines - this is the point within the Firewall Kernel at which packets are intercepted on their normal path between NIC and IP module, and at which packets are returned after inspection/filtering.

d. Interface for interaction with 'users' communicating across the firewall, ie what the user sees as a result of the firewall's mediation (causing connection to be accepted, dropped, rejected), and the interchange for subscriber authentication.

8. The external interfaces for the VPN-1 SecureClient are as follows:

a. the SecureClient GUI, which provides the user's graphical point of access (using windowing functionality) for interacting with the Firewall gateways and policy servers.

b. Interface for packets on SecureClient - the normal point within SecureClient Kernel at which packets are intercepted on their normal path between NIC and IP module, and at which packets are returned after inspection/filtering.

c. Interface for interaction with users communicating across SecureClient, ie what the user sees as a result of the SecureClient's mediation (causing a connection to be accepted, blocked or encrypted).

9. In addition, within the product there are interfaces for communications between the product machines in the distributed configuration and communication with external entities (eg LDAP server).

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Developer supplied test evidence in 2 parts:

    a. Evidence produced specifically for the evaluation, which demonstrated coverage of the security functions and external interfaces.

    b. Evidence extracted from the QA test database which, although aimed at demonstrating security functionality, was used to determine coverage of the subsystems described in the high-level design, as well as coverage of security functions and external interfaces.

2. Coverage of all security functions, subsystems and external interfaces was established from the test evidence supplied.

3. The QA tests supplied were used during the original ITSEC evaluation [i] to demonstrate coverage to the level of basic components (equivalent to 'modules' in the CC low-level design). From this level of test coverage, and knowledge of the product design, the evaluation team also judged that the subsystem internal interfaces had been adequately tested by the supplied test evidence.

4. The test configurations used for all the Developer's tests were in accordance with the evaluated configuration, ie

    a. 'Firewall' and 'Management Server' modules running on Windows NT4.0 SP6a and Solaris 8 operating system platforms; and

    b. 'GUI' and 'SecureClient' modules running on Windows NT4.0 SP6a operating system platforms.

5. The evaluation team witnessed a sample of the Developer's tests, using each of the claimed platforms (NT4.0 SP6a and Solaris 8) for the Management Server and Firewall modules, although only one combination of platforms was used for each test. The Evaluators witnessed tests performed by the Developers both at Check Point's Ramat Gan and Cambridge offices. All relevant Developer's tests were manual, although a number of the tests required the use of general tools.

6. The evaluation team repeated a sample of at least 20% of the Developer's tests. The sample of Developer tests repeated covered TOE operation on both operating system platforms for both the Firewall modules and the Management Server and also covered the SecureClient.

7. The test configuration used for the evaluation team's additional functional tests and penetration tests consisted of one 'Management Server' and one 'GUI' module (each running on Windows NT4.0 SP6a), 2 'Firewall' modules (one running on Windows NT4.0 SP6a, and one running on Solaris 8) and one 'SecureClient' (running on Windows NT4.0 SP6a), as described in paragraphs 9 - 13 of Annex A. The evaluation team devised and ran penetration tests which, where appropriate, were repeated in order to test the 'Firewall' module running on each of the

claimed operating system platforms. These tests were manual, although a number of the tests involved the use of tools, eg commercial and open source vulnerability scanners.

Platform Issues

8. The Security Target claims that the product executes on any computer system from the family of workstations and servers which supports one of the following operating systems:

- SUN Solaris 8
- Microsoft Windows NT4 SP6a

This is subject to the considerations of the Getting Started Guide [r] (which defines minimum hardware requirements) and the System Generation/Installation Guide [p] (which gives guidance on configuration of the evaluated configuration - note that this excludes options such as hardware accelerators).

9. Prospective consumers should note that the Evaluators' independent tests were run on hardware platforms and hardware components representative of the ranges that support the SUN Solaris and Microsoft Windows NT4 SP6a operating systems. Strictly, therefore, the evaluated EAL4 configuration is that running on the hardware platforms identified in Annex A. There is a risk that smaller memory sizes than those tested may introduce performance degradation. No specific problems of this nature were evident in the course of the evaluation.

10. The product relies on the underlying operating system for security-relevant functionality for process separation and time stamping.